3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

January 25, 2023

Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

RE: **Small Business Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives Under Consideration**

Dear Sir or Madam:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response to the Outline of Proposals and Alternatives Under Consideration (Outline) published by the Consumer Financial Protection Bureau (CFPB or Bureau) that addresses future implementation of section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve 134 million consumers with personal and small business financial service products. NAFCU has serious concerns with the Outline and the CFPB's expansive interpretations of section 1033.

**Executive Summary**

Without revisions to the scope of the Outline and its technical parameters, the proposals under consideration will unfairly burden credit unions with enormous compliance costs and ultimately distort the financial sector's competitive landscape. While the Dodd-Frank Act calls upon the CFPB to promote fair and competitive markets, the plain text of section 1033 does not reflect an intention to reengineer data sharing mechanisms to alter financial sector competition. In the long run, commoditization of financial data driven by the CFPB's goal of "reducing switching costs" could have the opposite of its intended effect: rewarding the largest, most technologically sophisticated companies at the expense of credit unions and other community institutions focused on relationship banking.[1]

Given the significant risks and costs associated with the CFPB's approach, NAFCU supports a more limited interpretation of section 1033 that includes appropriate exemptive relief, scales back the technically prescriptive aspects of the Outline and allows credit unions to exercise appropriate judgment before granting third parties access to member data.

[1] *See* CFPB, Director Chopra's Prepared Remarks at Money 20/20 (October 25, 2022).

In general, section 1033 aims to provide a formal mechanism for making consumer data portable. While data portability can serve as the foundation for more streamlined integration of financial technology, faster account opening, and automation of credit decisioning processes, it can also lead to greater security and privacy risks, particularly when consumers are not able to judge the reputation of third parties seeking data access privileges.

The Outline's conceptualization of open banking rights will likely magnify the potential for consumer harm, particularly in an environment where many financial apps already appear to have a short shelf life relative to traditional consumer deposit accounts.[2] Consumers that are enticed to share information with companies more interested in data monetization strategies than traditional banking services could have profound effects on the security of the financial sector, particular when these entities lack a functional regulator.[3]

The proposals under consideration also risk severe competitive harm. Not only would credit unions have an obligation to share valuable analytic data about members not typically found in periodic statements, but they would also need to subsidize third party access to this data by building and maintaining access portals. Ordinarily it would take a financial company many years to acquire a historically significant amount of customer data of the type and quality that is maintained by credit unions. Yet the Outline assigns little value to the upfront investment of establishing a long-lasting customer relationship and the ongoing costs of safeguarding data, envisioning instead a financial marketplace where fintech competitors are able to extract what they need once granted permission by a consumer.

To offset these risks, the CFPB must proceed cautiously and consider amendments to the Outline prioritizing three areas of focus:

1. To ensure the safety and privacy of sensitive consumer information, third parties should be held to the same information security standards as credit unions and other federally insured depositories.
2. To mitigate the risk of competitive imbalance, the CFPB should reconsider technical aspects of the Outline that are likely to impose unrealistic costs on smaller credit unions, complicate implementation, and grant fintech business models an unfair advantage.
3. To protect consumers, the CFPB should ensure that data providers are able to exercise, at their discretion, appropriate due diligence, and that the duration, scope, and usage of consumer data by third parties is governed by clear disclosures, informed consent, and principles of data minimization.

[2] *See* Apptentitve, Finance Apps: 2022 Mobile Customer Engagement Benchmarks (April 5, 2022), *available at* https://www.apptentive.com/blog/finance-apps-2022-mobile-customer-engagement-benchmarks/.
[3] See CFPB, Prepared Remarks of CFPB Director Rohit Chopra in Great Falls, Montana on Relationship Banking and Customer Service (June 14, 2022) ("[T]he CFPB is working to ensure that algorithmic banking is not being given special treatment and must follow the same set of rules that relationship banks follow.")

**General Comments**

Access to consumer financial data must be governed by rules emphasizing security, transparency, and competitive fairness to meaningfully promote innovation within the financial sector. Whether federally insured credit unions operate as covered data providers or data recipients as those terms are defined in the Outline, all are subject to comprehensive prudential supervision, regular examination, and the information security safeguards prescribed under the Gramm-Leach Bliley Act (GLBA). Comprehensive regulatory oversight supports credit union efforts to engage in safe and secure data exchange with trusted third parties; however, the Outline proposes a radical shift in the way that consumer financial data is handled by allowing companies potentially lacking adequate supervisory oversight to directly access broad categories of consumer data.

Currently, credit unions that provide structured account or transaction data to aggregators or fintech partners engage in rigorous due diligence that may require specific contractual assurance as part of a formal agreement. A formal agreement helps ensure that data exchanging parties meet minimum security and privacy standards, and that the terms of the data sharing agreement are fair to the credit union and its members. Such contracts may even identify specific technical standards (e.g., transmission encryption, storage encryption, adherence to message specifications), and help allocate legal liabilities to different parties in the event of a security incident.

Alternatively, data sharing may occur in the absence of a formal agreement between data exchanging parties. If consumers want to share the data contained in electronic bank statements, for example, they are free to do so, and credit unions routinely provide members with access to periodic statements in an electronic format. However, some types of consumer-directed data exchange are problematic from a security standpoint. Screen-scraping, for example, involves the consumer sharing login credentials with a third party, which is generally regarded as insecure and highly risky.

Different modes of data exchange (company managed versus consumer managed) are largely superseded by the CFPB's Outline, which favors an open-door approach to granting authorized third parties structured access to credit union member information. While the Outline is commendable in certain respects—emphasizing consumer consent to scope, duration, and data usage when granting authorization to a third party—its requirements related to providing portal access and sharing categories of consumer data outside of section 1033's express statutory language will impose major costs on credit unions of all sizes.

Interpreting section 1033 to supersede formal data sharing arrangements also risks impairing the benefits of credit union due diligence, particularly in cases where an authorized third party has unscrupulously obtained a consumer's authorization and consent. To the extent consumers are unable to accurately judge the security or reputation of a data seeking entity, failure to limit data access could expose individuals to elevated risk of fraud or identity theft. For credit unions, the

mishandling of member data by downstream recipients will likely correspond with increased reputational risk as members tend to assert important error resolution rights with their credit union as the primary account holding institution, regardless of where the error originated—a habit NAFCU has observed in the context of P2P disputes.[4]

With respect to the technical scope of the Outline, which envisions credit unions and other data providers supporting third party access through the development of dedicated information portals, similar to application programming interfaces (APIs), the CFPB vastly understates the cost and complexity of such an endeavor. Accordingly, NAFCU urges the CFPB to consider technologically neutral alternatives that focus on the promotion of industry-developed secure data exchange standards, elimination of screen-scraping, and development of core principles to govern authentication of third parties trusted by both the consumer *and* the data provider.

The CFPB's 2017 document addressing "Consumer-Authorized Financial Data Sharing and Aggregation" (2017 Principles) might serve as a starting point for developing an appropriate framework that balances the interests of granting consumers appropriate control over their account related data and allowing credit unions to protect their members.[5] For the principles listed below, NAFCU summarizes its recommendations for improving consumer data portability without imposing disproportionate regulatory burdens on credit unions.

Access

The 2017 Principles provide that consumers should be able, "upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider" and "are generally able to authorize *trusted* third parties" (emphasis added).[6] NAFCU agrees that credit union members should be able to retrieve—on their own, and for their own purposes—data about their accounts, such as periodic statements. However, it would be irresponsible for the Bureau to assume that consumers will be able to accurately judge the security posture and compliance controls of a third party that invites a consumer to share sensitive financial information.

The CFPB should allow credit unions and other data providers to assess the trustworthiness of third parties on a discretionary basis instead of permitting any authorized third party to gain access the moment they obtain the consumer's authorization. The CFPB should also avoid the promulgation of unwieldly and costly technical solutions for facilitating data exchange.

[4] *See* NAFCU, Letter to CFPB re: Agency Information Collection Activities: Comment Request (Regulation E) (Docket No. CFPB-2021-0021) (February 14, 2022), available at https://www.nafcu.org/comment-letter-cfpb-regulation-e-error-resolution-File.
[5] *See* CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (October 18, 2017) [hereinafter 2017 Principles].
[6] *Id* at 3.

It is unlikely that a regulatory specification for data exchange will appropriately match the IT environments of every credit union or keep pace with evolving industry standards for risk management. Federal agencies such as the National Institute of Standards and Technology have generally recognized that there is no one-size-fits-all solution for cybersecurity. The Bureau should heed this advice and avoid issuing a proposal that could either force credit unions to compromise their security or adopt data exchange specifications that primarily benefit large fintech incumbents.

Control and Informed Consent

Third party access to consumer data should be governed by a consent framework that allows consumers to exercise appropriate control over the use and retention of their data.

Credit unions have demonstrated a long history of compliance with the privacy requirements contained in the GLBA and the Bureau's Regulation P. Additionally, the NCUA's implementation of the GLBA's safeguard requirements requires all credit unions to protect their members' data, including member data that is shared with service providers.

In general, when exercising section 1033 rights, consumers should know exactly what data a third party will be requesting on their behalf, for what purpose it is being used, how frequently it will be accessed, how long it will be stored, with whom it might be shared and under what conditions, and any rights they may assert in the event their data is lost or stolen. Additionally, consumers should be given control over how much and what type of data they choose to share.

In general, the Outline meets these objectives by proposing a robust set of disclosure requirements for third party data recipients. While NAFCU sees value in the CFPB's proposed disclosure and consent mechanisms, the CFPB should be careful that consumer control over data access does not impose unreasonable burdens on data providers. For example, complex business logic to effectuate granular limits on the frequency or scope of data sharing will likely inflate the cost of developing third party access portals. Ultimately, the obligation to ensure that consumer data sharing preferences are honored should fall upon the third party recipient rather than the data provider.

Given the heightened risk of fraud in the event that consumers' financial data is compromised, the Bureau should regard disclosures and controls as minimum safeguards for third parties whose data requests are predicated on the rights or privileges recognized under section 1033. Consumers should also be granted the ability to easily revoke third party data access at any time by contacting the third party. The obligation to honor a consumer's request to revoke third party access should fall upon the authorized third party rather than the data provider. Lastly, the CFPB should not grant a presumption of authorization if a consumer has not affirmatively consented to extending their data sharing agreement with a third party beyond its original term.

Security

As discussed in later comments (see p.15), the Bureau should focus its standard setting efforts on establishing minimum data security requirements for third party recipients of consumer information. After a credit union has established a minimum level of trust in an authorized third party to grant a member's request to transfer data, the credit union should also be free to provide additional disclosures to the member to warn of general security risks.

Credit unions should be able to exercise their judgment to conduct discretionary risk assessments of third parties and to suspend access privileges when they reasonably believe that an authorized third party is not able to adequately protect consumer information. When a data provider transmits information directly to a consumer, either because it has been instructed to do so or because it cannot establish trust in a third party, it should not be liable for any action or inaction related to the safekeeping of the information taken by the consumer or a third party recipient that later receives the information from the consumer.

**The CFPB should consider an exemption for small data providers**

The Outline requests comment on whether the CFPB should exempt certain covered data providers from the proposals under consideration and acknowledges that the obligation to make data available through a data portal may be "more burdensome for some covered data providers than others."[7] NAFCU expects that the cost to develop, test, and secure data portals will be significant for most credit unions in their capacity as covered data providers. Accordingly, an exemption from the requirement to provide data access through a portal would be appropriate for credit unions determined to be "small." For the purpose of a future proposal, the starting point for a small entity exemption might reference SBA size standards (i.e., under $750 million in total assets for a depository institution), but an asset-based threshold should be supplemented with an alternative, activity-based measure, such as the number of consumers requesting direct data exports.

The CFPB's alternative approach of tailoring an exemption based on number of accounts offers less compelling relief. The number of accounts held by an institution is not a true measure of activity in terms of what is most relevant to section 1033; one would expect the number of accountholders requesting their data via traditional export methods would be a better proxy for gauging the institution's role as a data provider. Furthermore, an account-based exemption might force small institutions to limit growth to avoid disproportionate compliance costs. Such an outcome would undermine the Bureau's objecting of promoting an inclusive financial services marketplace that does not disproportionately reward the largest incumbents.

[7] CFPB, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights – Outline of Proposals and Alternatives Under Consideration, 13 (October 27, 2022) [hereinafter Outline].

If the CFPB chooses to adopt an exemptive standard for certain covered data providers, it should provide a grace period of at least one year (additional to any initial implementation phase-in following issuance of a final rule) to come into compliance. Regulatory phase-ins are appropriate for credit unions when there is a significant change in compliance expectations. If the CFPB chooses to adopt an activity threshold as an alternative exemption standard, it should also consider a lookback period of at least two preceding calendar years, which would be similar to how loan-volume thresholds are applied under Regulation C's transactional coverage tests.

**If the CFPB exempts certain data providers from the requirement to operate a third party data portal, it should not impose a corresponding obligation to accommodate all screen scraping requests**

The Outline requests comment on whether the CFPB should accommodate screen scraping or designate this method of data exchange as the preferred standard for entities exempt from the third party data portal requirement. The many security risks associated with screen scraping should weigh against any proposal to compel entities to accommodate this method of data exchange—whether they are exempt from the portal requirement or not.[8] Furthermore, for consumers to exercise meaningful control over the a screen scraper's access to data would likely require data providers to adopt tools or controls that would carry their own set of costs, which would undermine the purpose any exemptive relief. Accordingly, NAFCU recommends the CFPB avoid developing a proposal that compels acceptance of screen scraping.

**The CFPB should recognize limits on the information covered data providers are required to make available**

The Outline proposes requiring covered data providers to make available with respect to covered accounts six different categories of data. While some categories clearly correspond with the information expressly listed in section 1033, others do not. Section 1033 covers a relatively narrow band of data that concerns a "consumer product or service" and relates "to any transaction, series of transactions, or to the account including costs, charges and usage data."[9] However, the Outline appears to take an expansive view of what data the statutory language encompasses.

For example, account identity information may not relate primarily to usage of a consumer product or service but to the account holding institution's Bank Secrecy Act (BSA) compliance program. Likewise, a catchall category of "other information," might include security records and analytical insights regarding engagement—categories of data that a consumer would not see or expect to see in connection with a particular account. Any requirement to expose such data would confer little benefit to the consumer as an ordinary user of a financial product or service

[8] *See e.g.,* FINRA, Investor Alert: Know Before You Share: Be Mindful of Data Aggregation Risks, (Mar. 29, 2018), available at https://www.finra.org/investors/alerts/be-mindful-data-aggregation-risks.
[9] 12 U.S.C. § 5533(a).

and grant an unexpected windfall to fintech companies and other competitors of traditional depositories.

NAFCU is aware of strong industry concern that data recipients might reverse engineer business strategies using analytical information gathered from credit unions under section 1033. As described below, this risk is not present for all categories of information; however, for certain types, the risk of unfair competition will likely outweigh the marginal benefit of granting third party access.

1. Periodic statement information for settled transactions and deposits.

Information in this category generally appears on periodic statements that credit union send to their members. NAFCU does not object to sharing such information; however, the CFPB should clearly specify what discrete data elements are included to avoid confusion. Not all periodic statements for "asset accounts" are the same in terms of formatting or content.

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

For this category of information, the Outline offers the example of a pending debit or credit. NAFCU regards this information as difficult to share with third parties and likely to cause confusion for consumers if the systems data providers rely on to share information about pre-settled transaction experience outages.

Data concerning the pre-settlement status of a transaction will not always reside in a centralized system. Furthermore, delays in the transmission of settlement information between data providers and data recipients could give consumers an inaccurate sense of their available funds.

More frequent transmission of settlement data might serve as a workaround to this problem but would pose its own set of challenges. To reduce the potential for delayed transmission of settlement data, third parties may ping data portals more frequently which could result in strains on system bandwidth and higher costs for data providers. As discussed in later comments, NAFCU does not support prescriptive requirements for portal latency. Frequent access by third parties to request real-time updates for pending transactions would undermine principles of minimization and efficient usage of data.

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

For this category of information, the Outline provides the example of data regarding the interbank routing of a transaction. The CFPB also proposes to reveal information about the name and account number of payees, speculating that the availability of such information could aid in

error resolution and help institutions recover funds from fraudulent or unauthorized transactions.

Transmission of routing and account numbers outside of secure payment systems could expose credit unions to 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.

In the context of facilitating consumer payments, sending and receiving institutions generally have access to the necessary information to track down funds that may have been incorrectly or fraudulently transferred. Barriers to recovery that present more practical challenges tend to relate to the speed of fraud detection and financial institution intervention—matters that are far beyond the scope of section 1033 and would, in any case, implicate risk scoring inputs that would fall within section 1033's exempted categories of information.[10]

For third parties that do not offer payment services, providing access to sensitive, backend payments data for the purpose of aiding error resolution is a questionable proposition given that these entities are unlikely to face liability under Regulation E. As NAFCU has noted in past letters, to reduce the risk of payments fraud the CFPB should focus its efforts on improving consumer education and resiliency to fraud.[11] If the CFPB does recognize a right to transfer this data to third parties, then it should also ensure that the recipients are bound to the same Regulation E error resolution obligations that data providers assume with respect to the accounts involved.

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

For this category of information, the Outline provides the example of automatic bill pay and information about a biller with which the consumer has a relationship and information about the consumer's relationship with the biller, such as the consumer's account with the biller. The CFPB speculates that information about future transactions automatically charged to a consumer's account might enhance the ability of authorized third parties to provide just-in-time deposits of credit funds to the consumer's account to prevent overdraft fees.

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. Collectively, these differences

[10] *See* 12 U.S.C. § 5533(b)(2) ("any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct").
[11] See NAFCU, Letter to The Honorable Rohit Chopra, Director, Consumer Financial Protection Bureau re: Regulation E Guidance (August 17, 2022), available at https://www.nafcu.org/letter-cfpb-regulation-e-guidance-File.

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.

NAFCU also questions whether the scope of covered accounts is even sufficient to yield meaningful visibility about automatic payments. Recuring 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.[12] Accordingly, given the limited scoping of the proposals under consideration, covered 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.

5. Account identity information

For this category of information, the Outline lists sixteen elements including date of birth, social security number, race, ethnicity, and marital status. The CFPB recognizes that sharing sensitive identifying information with third parties raises concerns about fraud, privacy, and other consumer protection risks. The CFPB also suggests that these risks could be mitigated through a "confirm/deny" approach where the data holder merely validates but never transmits identifying information.

NAFCU has serious reservations about any proposal that would compel transmission of member identifying information and, like the Bureau itself, questions "the degree of consumer benefit of authorized third-party access to information that a consumer could share with the third party directly, as opposed to through a covered data provider."[13] As described in later comments, the preferred approach for authenticating a consumer's request to share data with an authorized third party would be for the consumer to present the request to the data provider which would then verify the consumer's identity. In no case should a data provider need to transmit identifying information about a consumer to a third party for authentication purposes, particularly when a third party can acquire this information directly from the consumer.

6. Other information

The Outline includes a catchall category of information that includes items such as reports from consumer reporting agencies, fees that the covered data provider assesses in connection with its

[12] *See* Nicole Specter, "35 Percent of Americans Are Enrolled in Auto Pay — and It's News to Them," NBC News (August 29. 2017), available at https://www.nbcnews.com/business/consumer/35-percent-americans-are-enrolled-auto-pay-it-s-news-n797131.

[13] Outline at 23.

covered accounts, bonuses, rewards, discounts, or other incentives that the covered data provider issues to consumers, and information about security breaches. NAFCU regards nearly all of the information contained in this category as not appropriately within the scope of section 1033, the exception being items that would appear on an account statement visible to the consumer (e.g., fees, credits for redeeming rewards).

Security notifications are not typically memorialized as account-specific information, since communications about a cybersecurity incident may reflect risks that are not specific to a consumer financial product or service. Furthermore, member privacy could be undermined if forensic assessments intended only for members include content that is outside the scope of what the member has agreed to share with a third party. Reviewing the content of security related notifications on a case-by-case basis to ensure their conformity with a consumer's data sharing preferences would place an undue burden on data providers that are primarily interested in sending out security notifications as quickly as possible.

Credit unions may also be required to send initial notice to NCUA as a precautionary step in the event of a cyber incident, even as forensic work is ongoing, and the scope of the incident has yet to be fully determined. In these situations, requiring credit unions to share confidential supervisory information with third parties would clearly be excluded by section 1033.[14] A credit union affected by a security incident will generally be the first to notify the member and will be accountable for ensuring accounts are safe thereafter. Unless the Bureau intends to magnify the already heightened risk of reputational injury to a firm engaged in incident response activities, there is little practical benefit to sending breach notifications to third parties.

With respect to reports from consumer reporting agencies, the disclosure of such information could encompass many data elements that are beyond section 1033's intended coverage, such as employment history, online activity and judicial records. Sharing consumer reports with authorized third parties could also expose credit unions and other data providers to increased dispute volume.

Consumers that use data aggregation services to apply for credit products offered by third parties might dispute the accuracy of a credit report provided by a data provider if their application is denied by the third party. However, such disputes may not always implicate a true error and an adverse action notice that names a data provider as a source of information may give a consumer the false impression that the data provider is in a position to amend the third party's credit decision.

Separate from the question of whether consumer reports should be covered data is a related concern—whether the collection of alternative data by a data aggregator makes it a consumer

[14] *See* 12 U.S.C. 5533(b)(3); *see also* NCUA, Cyber Incident Notification Requirements for Federally Insured Credit Unions, 87 Fed. Reg. 45029, 45032 (July 27,2022) ("This notification, and any information provided by a FICU related to the incident, would be subject to the NCUA's confidentiality rules.")

reporting agency under the Fair Credit Reporting Act (FCRA) and whether providing such data renders a data provider a furnisher. These topics are addressed below in the context of promoting data accuracy.

**The CFPB should explore ways to ensure the accuracy of data collected by third parties but should also ensure that any requirement to provide consumer data does not make a credit union a furnisher under the FCRA**

The CFPB should clarify that credit unions that provide data to authorized third parties at the request of a member are not considered data furnishers with respect to that information for the purposes of the FCRA and Regulation V. Credit unions that comply with section 1033 requests to share records would not be furnishing such information by agreement and would not possess knowledge of how the data will be used. Most importantly, the transmission of information would be consumer directed. Regulation V provides an entity is not a furnisher when it is a consumer to whom the information pertains.[15] Given the Bureau's interpretation in the Outline that third parties are "consumers" when they request data in their capacity as agents, it is clear that Regulation V's exclusion applies.

With respect to data accuracy, credit unions are already supervised for compliance with the FCRA's requirements regarding data accuracy and disputes. By contrast, not all data aggregators are held to similar requirements. While the Outline questions how third parties might address data inaccuracies that originate with a data provider, a more fundamental issue is how data aggregators will respond to consumer inquiries about the accuracy of assembled or analytically enriched information.

NAFCU recommends the Bureau clarify in a future proposal what types of data aggregation activities might make a third party a credit reporting agency under the FCRA and Regulation V. If some data aggregators and other recipients of consumer data are not regarded as credit reporting agencies, then the Bureau should clarify what rights consumers may exercise to dispute inaccuracies or errors introduced by these entities. However, the Bureau should not adopt a framework where a third party may redirect disputes regarding data accuracy to a data provider instead of performing its own reasonable investigation of an alleged error.

**The CFPB should defer to a data provider's reasonable judgement about what information may be statutorily excepted from permissioned sharing under section 1033**

Section 1033 contains several exceptions to the general requirement to provide consumers with information about financial products or services they use. In general, the Outline construes these exceptions narrowly. As discussed below, NAFCU recommends a more accommodating approach that allows credit unions to exercise their reasonable judgment to prevent sharing of confidential

[15] *See* 12 CFR § 1022.41(c)(3).

information that might cause competitive harm, endanger consumers, or undermine activities aimed at combatting fraud.

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

NAFCU has 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 section 1033.[16] As the Bureau acknowledges, the phrase also encompasses information covered by other laws, such as the Freedom of Information Act and is even referenced in a related section of the Dodd-Frank Act—section 1034(c)—relating to a covered institution's obligation to respond to consumer requests for information.[17]

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."[18] 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.

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 previously, NAFCU regards 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. 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. NAFCU recommends the Bureau reconsider

[16] See Outline at 24-25.
[17] 12 U.S.C. § 5534(c).
[18] *See Pub. Citizen Health Research Grp. v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983).

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.

For this exception, the Outline regards account information that the covered data provider "is statutorily required to keep confidential from the consumer" as distinct from "information that the covered data provider must keep confidential from persons other than the consumer, but need not keep confidential from the consumer."[19] In general, NAFCU does not object to this approach but suggests 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 section 1033 rights.[20] 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.

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

The Outline offers minimal clarity with respect to how this exception will be interpreted but acknowledges that "the effort required to retrieve the information varies depending on the form and system in which the information is stored."[21] Somewhat related to this exception is the Outline's proposal to define current and historical information that covered 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 section 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

[19] Outline at 26.
[20] For example, the CFPB might clarify how the exception applies to financial institutions subject to business associate agreements under the Health Insurance Portability and Accountability Act and that do not qualify for payment activity related exemptions. *See* 42 U.S. Code § 1320d–8.
[21] Outline at 26-27.

ultimately disadvantage consumers by depriving primary account holding institutions, such as credit unions, of critical analytical insights. Accordingly, NAFCU recommends 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.

**The CFPB should consider appropriate limits on secondary uses of information by authorized third parties**

To better protect consumer privacy and security, the CFPB should consider limits on the secondary use of information by an authorized third party in a future proposal. The Outline's suggestion of categorizing secondary uses by risk level and requiring opt-in by the consumer may offer a sound initial approach; however, the exact parameters of any future restrictions and consent mechanisms will necessarily depend on how the Bureau tailors security standards and oversight for nonbank third parties. Whether a complete prohibition on all secondary uses of data is appropriate may also depend on the exact level of control a consumer is able to exercise with respect to the use and retention of their data. Furthermore, even secondary use of de-identified information could pose significant competitive harm to credit unions if an aggregator is able to leverage information about the credit union's field of membership to draw inferences about the identity of accounts or their location.

**Data Security**

By far the most significant concern for credit unions regarding implementation of section 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."[22]

Regulatory standards to discourage screen scraping can help mitigate fraud and account takeover risks, and NAFCU encourages the development of principles to promote voluntary industry alignment around more secure methods of data exchange. However, the Outline presents a fundamental obstacle to achieving a more secure financial data ecosystem by placing the burden on the consumer to understand which third parties should be trusted with sensitive financial information.

[22] *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-concerning-correlation-cba-warns-against-screen-scraping-20200316-p54am8.html.

The CFPB's implicit trust in consumer judgement at a time when many Americans have demonstrated vulnerability to social engineering scams is counterintuitive—particularly when all federally insured credit unions are required to meet robust security guidelines and perform rigorous due diligence before engaging with third parties.[23]

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.

While some 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, 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 National Credit Union Administration (NCUA)—have developed specialized procedures for assessing the security of regulated institutions. Credit unions receive 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. Furthermore, the Bureau's lack of clear regulatory authority in the domain of data security (i.e., the Safeguards portion of the GLBA) may frustrate efforts to develop common standards for non-supervised entities without significant reliance on the agency's UDAAP authority or the Federal Trade Commission, which lacks the supervisory toolset that would be necessary to address the Outline's security-related risks.

If the CFPB does not require all data recipients to meet the same data security standards—i.e., the Safeguard Guidelines—applicable to credit unions and other insured depositories, nonbank, non-supervised third parties may fail to meet baseline expectations for security and could introduce risks across the broader financial sector.

NAFCU recommends the CFPB adopt the Safeguard Guidelines promulgated by the federal banking agencies and the NCUA as the appropriate standard for data recipients rather than adopt a more general standard "appropriate to a third party's size and complexity."[24] Without the benefit of contractually negotiated terms of data access, variability in data security expectations

[23] *See* Venturebeat, "Report: 84% of U.S. citizens have experienced social engineering attacks," (September 23, 2022), available at https://venturebeat.com/security/report-84-in-us-have-experienced-social-engineering-attacks/ *; see also* 12 CFR Part 748 Appendix A.
[24] See Outline at 46.

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. Surveyed NAFCU members have reported that the share of their operating budgets devoted to cybersecurity has more than doubled in the past five years and expect these costs to rise in the future.[25]

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 Outline 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 section 1033 does not address questions of liability or indemnity.

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 privacy laws, recognize credit unions' existing compliance with the GLBA, preempt state privacy laws, and implement proper guardrails for consumers' protection across the entire data ecosystem rather than just certain sectors.[26] NAFCU encourages the CFPB to support development of a national data security standard before issuing a formal proposal, or else find separate authority to ensure that all data recipients are governed by the same standards that apply to credit unions and other federally insured depositories.

[25] See NAFCU, Report on Credit Unions, 61 (2022)
[26] *See* NAFCU, NAFCU's Principles for a Federal Data Privacy Standard (2022), *available at* https://www.nafcu.org/system/files/files/NAFCU%20Data%20Privacy%20Issue%20Brief%20Dec2019.pdf.

The CFPB could also significantly minimize the harm of unvetted parties mishandling consumer information by allowing data providers to perform discretionary due diligence if a credit union reasonably believes it is necessary.

**The CFPB must ensure that data aggregators and other nonbank data recipients are subject to appropriate supervision before publishing any rule to implement section 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 Outline as entities that support data recipients and data providers in enabling authorized information access, 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 Section 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.

Other fintech firms that meet the Outline's definition of a third-party data recipient 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.[27] Incidentally, these same strategies may be driving demand for enhanced data exchange to accommodate financial product disaggregation.

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.[28]

Implementation of section 1033 without corresponding enhancements to oversight and regulation of nonbank fintechs could magnify the risk of consumer harm. As consumers seek different providers for discrete financial products, the end result could be that only the provider of a core deposit relationship, such as a credit union, is subject to regular supervision and prudential oversight. Disaggregation of payments and credit products without a corresponding update to the Bureau's supervisory framework for nonbank fintechs could expose consumers to

[27] *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* https://files.consumerfinance.gov/f/documents/cfpb_buy-now-pay-later-market-trends-consumer-impacts_report_2022-09.pdf.

[28] *See* CFPB, Proposed Rule re: Registry of Supervised Nonbanks that Use Form Contracts to Impose Terms and Conditions that Seek to Waive or Limit Consumer Legal Protections, 45 (January 11, 2023), *available at* https://files.consumerfinance.gov/f/documents/cfpb_registry-of-supervised-nonbanks_2023-01.pdf.

greater risk by making it more difficult to prevent violations of consumer financial law before they occur.

One action that Bureau can take to improve oversight of data aggregators is to exercise its larger participants authority as requested in a joint letter submitted by NAFCU and other trade associations.[29] Regardless of how the Bureau chooses to implement section 1033, it should fill supervisory gaps that might grant data aggregators preferential treatment and exacerbate consumer privacy risks if left unaddressed. At a minimum, the Bureau should reexamine the scope of its larger participants rule for the consumer reporting market if it has already recognized that "data users may compete for customers with the data holders from which they have obtained data."[30] 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 Outline's proposed mechanisms for third party authentication must accommodate discretionary due diligence but not treat authorized third parties as service providers**

The NCUA requires all federally insured credit unions to exercise due diligence when engaging a service provider and to ensure that service providers adopt controls sufficient to satisfy the information security program requirements described in Appendix A to Part 748 of the NCUA's regulations.[31] While a credit union's relationship with a service provider is distinguishable from its relationship with an authorized third party, which would not typically provide service *directly* to the credit union, older NCUA guidance provides generally that "[c]redit unions should complete a thorough risk assessment as part of their determination to offer account aggregation."[32] General guidance related to evaluating third party relationships is similarly unclear with respect to the status of authorized third parties with whom the credit union has no formal agreement.[33]

The CFPB should coordinate with the NCUA to ensure that a future proposal does not inadvertently create mandatory due diligence requirements for credit unions. Such an

[29] *See* Letter to the Honorable Rohit Chopra, Director, Consumer Financial Protection Bureau, re: Petition for rulemaking defining larger participants of the aggregation services market (August 2, 2022), available at https://www.nafcu.org/joint-petition-cfpb-larger-participant-rulemaking-data-aggregation-services-File
[30] *See* CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71006 (Nov. 6, 2020), available at https://www.federalregister.gov/documents/2020/11/06/2020-23723/consumer-accessto-financial-records. 4 See Taskforce Report
[31] *See* 12 CFR Part 748, Appendix A D.2.
[32] *See* NCUA Letter to Credit Unions, Account Aggregation Services, 02-CU-08 (April 2022), available at https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/account-aggregation-services. In the letter, the NCUA describes account aggregation as a service that "aggregates information from a member's various on-line relationships" such as accounts that would be covered under the Outline and "presents it in a consolidated and centralized manner for review and inquiry."
[33] *See* NCUA Supervisory Letter, Evaluating Third Party Relationships, SL No. 07-01 (October 2007) ("After credit unions have conducted internal risk assessments and due diligence over prospective third parties, they must implement on-going controls over third party *arrangements* to mitigate risks") (emphasis added).

expectation, if applied to potentially numerous third parties requesting data, would be impossible to meet given the time and resources necessary to perform risk assessments. Instead, the CFPB should accommodate a framework where credit unions are permitted to undertake voluntary risk assessments if they have reasonable doubts about the ability of an authorized third party to safeguard data. Reasonable doubts might include information about a data breach or other cybersecurity incident affecting the authorized third party. The CFPB should also allow credit unions, in their capacity as data providers, to include discretionary disclosures indicating whether the security posture of the authorized third party is unknown and how security risks might affect the member.

Without the ability to exercise caution with respect to potential data recipients, credit union data providers would need to trust that third parties are compliant with whatever security standards the CFPB ultimately prescribes for data recipients not already subject to the Safeguard Guidelines.[34] Given the CFPB's limited capacity to supervise every potential data recipient for the purpose of monitoring compliance with data security requirements, a requirement that data providers grant access to authorized third parties without any ability to exercise meaningful control may only serve to increase the probability of consumer harm, particularly when there is no mechanism to deny a consumer's request when there are reasonable doubts about the reputability or security of a third party.

The CFPB could offset this risk by allowing data providers to engage in discretionary risk assessments of authorized third parties to determine whether suspension or denial of access is appropriate. If a risk assessment indicates that the third party has failed to meet minimum security requirements established by the Bureau or other law, then the data provider should not be under any obligation to transfer data directly to the third party and should not be liable to the consumer for failure to do so. Likewise, a data provider should not be penalized for failing to intervene on a discretionary basis—not only due to the practical resource limitations described previously—but because oversight of authorized third parties' data security should be primarily the responsibility of the CFPB.

**The Outline's proposed mechanisms for third party authentication should specify that a consumer must present an authorization request directly to the data provider**

The CFPB acknowledges that "the security of third-party access portals could significantly impact consumer interests related to the privacy and the security of their information" and that "covered data providers have a legitimate interest in the secure handling and storage of their customers' information."[35] NAFCU agrees with both of these statements; however, the CFPB's proposed solution for authenticating a consumer's request to share data with an authorized third party lacks clarity with respect to how data providers should verify a consumer's identity.

[34] See Outline at 46.
[35] *Id*. 35, 38.

The Outline envisions an authentication sequence where a data provider would be required to make information available when it has received "evidence of a third party's authority to access information on behalf of a consumer, information sufficient to identify the scope of the information requested, and information sufficient to authenticate the third party's identity."[36]

To satisfy the first step in this sequence, a third party would need to "provide the consumer an 'authorization disclosure' soliciting the consumer's informed consent to certain disclosed key terms of access, obtain the consumer's express consent, and certify that it will abide by certain obligations."[37] After the covered data provider "receives evidence" that a third party has followed these steps to be authorized, it would then review the scope of information requested, along with information to authenticate the identity of the third party.[38]

The process of authenticating the identity of the third party does not clearly address how the data provider should authenticate the identity of the consumer making the request. NAFCU recommends the CFPB adopt an authentication framework that requires consumers to present their request directly to the data provider to minimize the transfer of personally identifiable information. Once the consumer's identity has been properly authenticated, a data provider could then review the authorization disclosure provided by the third party. If additional identifying information is needed for the consumer to complete the exchange with the authorized third party, the consumer should directly provide that information directly to the third party.

**The Bureau should not promulgate overly prescriptive technical standards regarding the operation of third-party access portals or data exchange specifications**

The Outline contemplates minimum standards for portal uptime, latency, and data caps—among other features that could affect the convenience of third party access. Depending on the size and complexity of the institution operating a portal, achieving certain technical benchmarks may be unrealistic or very costly—particularly for smaller institutions. To account for variability in terms of data portal operators and their available IT infrastructure, NAFCU recommends the CFPB adopt a more general framework that emphasizes making information "available in forms that are readily usable" and in accordance with the principle of data minimization.[39]

Credit unions and other data providers should be able to exercise reasonable judgment to set data caps or limits on requests within a particular period to reflect the capabilities of their systems. It would be unfair to expect a small credit union to purchase an expensive portal

[36] *Id*. at 36.
[37] *Id*. at 36. Notably, the proposed certification does not expressly cover the third party's compliance with minimum data security standards. The CFPB describes the certification statement as covering "use, collection, and retention of the consumer's information." Id at 17.
[38] *Id*.
[39] CFPB, 2017 Principles, 3.

solution to maintain the same capabilities as a very large bank or fintech company while only serving a fraction of the consumers or collecting a much smaller subset of account related data.

The CFPB should also avoid prescribing technical standard for data exchange, either with respect to directly exported files or those exchanged via third party portals. While many credit unions offer bank statements in PDF format to their members, other file types are less common. For consumers, a principle of useability should also recognize that most electronic statements are already machine readable if they can be accessed on a personal computer.

Data exchange specifications that govern information transmitted through third party portals should be developed by industry and the Bureau should avoid imposing its own technical standards. To facilitate voluntary industry adoption of appropriate data formats, the Bureau might emphasize in a future rule that data providers adopt commercially reasonable specifications for the exchange of consumer financial information. A more principled based approach in this domain would also have procompetitive effects insofar as it would encourage further industry innovation and not assign technological preference to specifications advantageous to incumbent business models.

**The proposals under consideration will harm credit unions by distorting market competition and favoring fintech business models**

Granting third parties expansive data privileges will impose unreasonable costs on credit unions that lack the scale and sophistication to accommodate section 1033's open-door conceptualization of data access rights. In addition to absorbing technical costs associated with supporting development or acquisition of a third party portal, credit unions will also face competitive costs.

The Outline grants fintech data recipients an unprecedented opportunity to reverse engineer product and service strategies, and generally devalues credit unions' stewardship of member data. Credit unions make an upfront investment to build a lasting member relationship and this emphasis provides the foundation for acquiring robust datasets and long transaction histories.

The CFPB has stated that implementation of section 1033 may reduce switching costs for consumers that are otherwise trapped with bad companies and reward firms that earn their customers through competitive pricing and high-quality service.[40] Implicit in this view is the erroneous notion that account holding institutions make it difficult for consumers to use alternative financial service providers. Yet the Bureau's own evidence suggests that nearly the opposite is true; citing one source, the CFPB estimates that "the number of consumer and small business accounts accessed by authorized third parties is estimated to be 1.8 billion."[41] With respect to credit unions, which are member owned and democratically controlled cooperatives,

[40] *See* Outline, 4.
[41] *See id*. footnote 8.

the imperative to provide members with access to fintech services is manifest in the multitude of partnerships in existence that facilitate payments, investing, financial planning and many other consumer financial activities.[42] Moreover, as mission-based community financial institutions, credit unions are ultimately answerable to their members. If structured data exchange with third parties is necessary to provide high quality service and meet member demand, natural competitive forces will compel change.

While the CFPB acknowledges the benefits of existing interconnection between account holding institutions and third-party data recipients in the consumer finance marketplace, it asserts without evidence that further enhancements to competition "cannot be guaranteed until disagreements over consumer-authorized information sharing are addressed through rulemaking."[43]

While the CFPB does possess a statutory mandate to promote "fair, transparent, and competitive markets," that mandate is best fulfilled when the Bureau engages in evidence-based rulemaking.[44] The CFPB has not substantively described the disagreements it cites or attempted to quantify their competitive impact. Furthermore, there is no contemporaneous record to show that Congress intended to reengineer existing data sharing mechanisms between financial institutions to promote competition when it passed the Dodd-Frank Act. On its face, the purpose of section 1033 is to provide consumers with convenient access to what is theirs—information about their use of financial products and services.[45] Credit unions already provide members much of the information described in the Outline through account statements that can be accessed physically or electronically.[46]

It is also questionable whether section 1033 contemplates the type of third-party data sharing that is central to the Outline's core set of proposals. The statute provides that covered persons shall make available information "in an electronic form usable by *consumers*" (emphasis added).[47] Nowhere does the statute reference a covered person's obligation to authenticate a consumer's request to share information with an authorized third party. And while the definition of consumer used in section 1033 does encompass an agent, trustee, or representative acting on

[42] See NAFCU Report on Credit Unions, 54-60 (2022).
[43] Outline at 5.
[44] *See* 12 U.S.C. § 5491(a) (The Bureau "shall regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws."); *see also* Dept. of Treasury, Financial Regulatory Reform: A New Foundation 55 (2009) ("For that reason, we propose the creation of a single regulatory agency, a Consumer Financial Protection Agency (CFPA), with the authority and accountability to make sure that consumer protection regulations are written fairly and enforced vigorously.")
[45] See 12 U.S.C. § 5533(a).
[46] The CFPB also acknowledges that most of the information covered in the proposal is already provided by data providers and even exportable in an electronic format. See Outline, 28 ("The CFPB also understands that a substantial portion of the information that covered data providers would be required to make available under the proposals the CFPB is considering […] is currently made available through these online financial account management portals.)
[47] *Id*.

behalf of an individual, the statute does not dictate the creation of a complex framework for authenticating agents or other representatives—procedures that are well outside the intended scope of *consumer* data access rights but seemingly central to the CFPB's plan to reengineer financial sector competition.[48]

It is likely that any future decision to implement section 1033 based on the Outline will alter the competitive landscape for credit unions. NAFCU anticipates that a formal set of rules governing financial data access rights will confer the greatest benefit to entities that are able to serve any consumer from any location, which could have the effect of amplifying the field of membership limitations of credit unions.

Since the passage of the Dodd-Frank Act, the number of credit unions has declined by over 30 percent. 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 section 1033 could have the effect of accelerating consolidation within the credit union industry and reducing access to financial services in underserved or rural communities. This outcome would undermine the Bureau's stated aim of preventing greater centralization of financial services.[49]

Enhanced data access privileges for third parties will likely enhance the viability of business models that leverage wholly digital platforms. Financial companies that operate entirely online, for example, could obtain insights about consumers' financial behaviors without ever needing to be physically present in the communities they wish to serve. Although this model of banking is becoming more commonplace, mass aggregation of consumer data coupled with the ability to render real-time credit decisions (and counteroffers) could have the effect of commoditizing the market for financial products and services in way that makes it challenging for smaller institutions to compete against larger nonbank entities. The displacement of credit unions that lack the necessary scale to compete with fintech marketing strategies could potentially reduce access to affordable credit in communities that have faced historical disenfranchisement.[50] Additionally, the loss of traditional, brick and mortar institutions could exacerbate the digital divide that often exists in underserved and rural communities.[51]

---

[48] *See* 12 U.S. Code § 5481(4); see also CFPB, Prepared Statement of Director Rohit Chopra before the House Committee on Financial Services (December 14, 2022) ("the CFPB is working to proactively create conditions for small firms and start-ups to challenge incumbents"), available at https://www.consumerfinance.gov/about-us/newsroom/prepared-statement-of-director-chopra-before-house-committee-on-financial-services/.

[49] *See* CFPB, Prepared Statement of Director Rohit Chopra before the House Committee on Financial Services (December 14, 2022).

[50] See e.g., Director Chopra's Prepared Remarks on the Release of the CFPB's Buy Now, Pay Later Report (September 15, 2022) (discussing BNPL providers use of paid product placement and the risk of digital "dark patterns"), available at https://www.consumerfinance.gov/about-us/newsroom/director-chopras-prepared-remarks-on-the-release-of-the-cfpbs-buy-now-pay-later-report/.

[51] Pew Research Center, "Digital gap between rural and nonrural America persists," (May 31, 2019), available at https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/.

Implementation of section 1033 could accelerate a general decline in branches by magnifying the competitive dynamics that are driving disaggregation of banking services and growth of purely digital financial services. While NAFCU supports efforts to eliminate barriers to online customer acquisition and service, such as by reforms to rules governing electronic signatures, implementation of the Outline could effectuate a far more radical shift in how banking services are provided, in ways that could potentially devalue the relationship banking model.

While credit unions may see certain benefits from a future section 1033 rule as data recipients, these will likely be tempered by structural limitations. For example, credit unions might be able to enrich their own insights about their members' financial habits with external data to tailor products or services more efficiently. However, these enhancements would be diluted by the reality of limited fields of membership, and it is arguably the marketing value of section 1033 data that will exert the greatest competitive pressure on depository institutions.

Unlike fintech companies that operate nationally, most credit unions with localized fields of membership will find it challenging to leverage data acquisition privileges with the same ease as, for example, a company that can invite anyone to share their financial data in exchange for a promotional rate. Credit unions already face unique barriers in terms of marketing efficiency (incurring greater relative cost to advertise when placements fall outside the boundaries of the credit union's membership) and section 1033 could amplify those disadvantages. Credit unions might be compelled to offer valuable data but would not be capable of taking full advantage of a data rich environment.

Implementation of section 1033 could also compromise credit unions' ability to guard trade secrets insofar as broad access to transactional data might permit third parties to reverse engineer credit decisioning variables. Credit unions devote a significant share of their budgets towards developing analytical tools to derive proprietary insights about financial patterns that can inform development of new products or services. Sometimes these insights are critical to allowing the credit union to compete against other financial companies possessing greater economies of scale. The importance of developing analytical tools and platforms cannot be overstated. Over 94 percent of respondents surveyed in NAFCU's 2020 Report on Credit Unions indicated that information technology was an area that will drive spending over the next three years, and most respondents indicated that within this domain, most investments would flow towards data analytics and marketing. Implementation of section 1033 could undercut the value of these investments and hobble smaller credit unions that already face significant structural limitations.

To offset these competitive risks, NAFCU recommends the Bureau approach implementation of section 1033 with a narrower technical focus. The CFPB might explore regulatory incentives to abandon screen scraping and establish minimum data security standards for third parties; however, the creation of third party access portals will likely correspond with outsize costs for

most credit unions. While there are advantages to structured information sharing via API, the CFPB should not compel data exchange through regulatory dictate, but instead offer clarifying principles designed to encourage voluntary pursuit of such interconnection.

**The CFPB should broaden the scope of covered data providers to ensure fair competition**

The Outline defines data providers as entities that meet either the definition of a financial institution under Regulation E or the definition of card issuer under Regulation Z. The effect of this limited coverage would place the Outline's most onerous requirements on credit unions and other depository institutions while excluding many other types of financial companies, like investment advisors, consumer lenders that are not card issuers under Regulation Z (e.g., BNPL providers), and aggregators—to name only a few.[52] Consequently, many types of fintech companies will enjoy new section 1033 privileges as potential data recipients without any corresponding risk that they will have to share data about their own customers.

It would be naïve for the Bureau to expect that the Outline's lopsided allocation of regulatory burden to financial institutions holding consumer asset accounts will have exclusively procompetitive effects. Data recipients that are able to harvest but not share data about consumers will likely drive further consolidation within the financial services industry while driving greater disaggregation of banking services. For credit unions, such an outcome would pose a significant challenge to the industry's unique, mission-oriented model of relationship banking.

**The CFPB should prioritize coordination and consultation with the NCUA before issuing a notice of proposed rulemaking**

The CFPB's decision to publish the Outline before consulting with the other federal banking agencies or the National Credit Union Administration (NCUA) overlooks the expertise and experience of functional regulators, particularly in matters related to data security and risk management.

As discussed previously, the Outline's lack of discussion regarding the scope of due diligence for service providers versus authorized authorized parties might be addressed by consulting credit unions' functional regulator.[53] As the CFPB moves forward with a future proposal, it should actively engage the NCUA and other federal banking agencies as soon as possible, clearly indicate where it has received agency input, and explain why the approach taken in a future proposal either conforms with or departs from the recommendations of other regulators.

[52] *See* Outline, 12.
[53] *See* 12 CFR Part 748 Appendix A

**The CFPB should provide covered data providers with ample time to implement a future proposal.**

For institutions not eligible for exemptive relief, the CFPB should engage with core providers to understand what realistic implementation timeframes will look like for developing a third party access portal and offer covered data providers ample runway to prepare for any final rule.

At a minimum, data providers should be given at least 36 months to implement any final rule requiring development of a third party data access portal—and possibly longer depending on the scope of a future proposal. Standardization of different categories consumer data in addition to testing new APIs to facilitate third party authentication, data-exchange, and fine-tuned consumer control will likely exceed the technical complexity of HMDA implementation following the CFPB's 2015 final rule amending Regulation C.[54] Depending on the contents of a future rule, which may include an expansive interpretation of "other" information data providers are obliged to share or specific data exchange standards, significantly more time may be needed.

**Conclusion**

NAFCU supports efforts to empower consumers with modern financial tools and believes that regulatory barriers should not prevent financial data from being used in productive ways. To best promote innovation in this domain, the Bureau must consider substantial revisions to the Outline and orient a future rulemaking around core principles of security, transparency, and competitive fairness.

Accommodating industry developed standards for data exchange, clarifying consumer consent and disclosure requirements, and prohibiting insecure methods of data sharing are a step in the right direction. Likewise, parallel efforts to bring data aggregators within the CFPB's supervisory jurisdiction as larger participants would ensure a level playing field exists for all entities subject to a future rulemaking to implement section 1033.

Establishing supervisory parity and emphasizing adherence to the robust information security safeguards applicable to credit unions and insured depository institutions would also help mitigate the significant security risks associated with unvetted information sharing. However, proposals that stray beyond these core objectives will tend to exceed the intended scope of section 1033 by reengineering financial sector competition to suit the Bureau's preferences—the result being significant disruption for credit unions of all sizes and the potential loss of community focused institutions and their relationship banking models. Commodification of consumer data without appropriate guardrails will favor the largest incumbents and drive further consolidation within the financial sector—an outcome that is at odds with the CFPB's desire to promote competition.

[54] See CFPB, Home Mortgage Disclosure (Regulation C), 80 Fed. Reg. 66127 (October 28, 2015).

NAFCU appreciates the chance to submit comments in response to the CFPB's Outline. Should you have any questions or concerns, please do not hesitate to contact me at amorris@nafcu.org or (703) 842-2266.

Sincerely,

Andrew Morris
Senior Counsel for Research and Policy