December 29, 2023

Honorable Rohit Chopra, Director
Consumer Financial Protection Bureau
1700 G St. NW
Washington, DC 20552

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

Dear Director Chopra:

I am writing on behalf of the California and Nevada Credit Union Leagues (Leagues), whose combined strength makes up one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 285 credit unions and their more than 13.6 million members.

In October 2023, the Consumer Financial Protection Bureau (CFPB) proposed a rule to implement personal financial data rights under section 1033 of the Consumer Financial Protection Act of 2010 (CFPA). The proposal would require depository and non-depository entities to make available to consumers and authorized third parties certain data relating to consumers' transactions and accounts; establish obligations for third parties accessing a consumer's data, including important privacy protections for that data; provide basic standards for data access; and promote fair, open, and inclusive industry standards.

The Leagues appreciate the opportunity to comment to the CFPB regarding the proposed rule. As longstanding advocates for consumer financial protection and well-being, credit unions play a crucial role in collecting and managing the personal information of their member-owner consumers in order to tailor products and services to most effectively meet their financial needs. We support a consumer's right to securely access and share their financial data in a transparent manner that affords them control. And while we support the proposal's intent and the overall goals embodied in section 1033, we would like to express concerns regarding various aspects of the proposed rule. Specifically, our concerns revolve around:

1. The potential impact on the ability of credit unions, particularly smaller-sized credit unions, to successfully compete in the financial services marketplace;
2. Privacy and data security;
3. The exclusion of data providers being overly restrictive;
4. The prohibition of fees and the associated costs for compliance;
5. Implementation deadlines; and
6. The absence of a clear assignment of liability among market participants.

We respectfully offer the following comments.

## I. General Comments: *The Credit Union Difference*

We would also like to highlight the distinctive nature of credit unions compared to other financial service providers for the CFPB's consideration. Credit unions are member-owned, democratically governed, not-for-profit cooperatives whose purpose is to promote thrift and improve access to credit for their member-

owners, particularly those of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates. Credit unions exist for the financial benefit of their member-owners, but they are ultimately driven by the philosophy of people-helping-people.

The credit union structure is vastly different than for-profit entities. "Owners" are not proprietors or shareholders in a business whose only goal is that the business maximize individual shareholder profits. Instead, credit union shareholders are member accountholders of a not-for-profit cooperative, with a volunteer board of directors democratically elected by and from among its members. Each member has one vote, regardless of the number of shares (amount of funds) held in the credit union.

We firmly believe that recognizing the unique role of credit unions serves as a vital reminder of their significance within the financial services market and the invaluable contributions they make to their members and the communities they serve.

## II. Specific Comments Pertaining to the Proposed Rule

### 1. There is Competition in the Financial Marketplace

The Leagues wish to emphasize to the CFPB that its ongoing narrative of anti-competitive behavior in the financial marketplace is misguided, given the robust competition evident in the United States banking systems. Consumers enjoy a multitude of choices, contributing to a highly competitive landscape that ultimately benefits consumers. It's essential to recognize that credit unions operate within this competitive framework, facing challenges from traditional banks, online banks, and fintech companies.

Contrary to the suggestion that more competition is unwarranted, credit unions, as the only consumer-owned cooperatives in the financial services sector, provide a valuable and necessary option in this competitive environment. Their mission explicitly includes providing members with credit at competitive rates, and they have a longstanding commitment to safeguarding consumer interests. The Leagues have consistently advocated for appropriate safeguards that strike a balance between ensuring the safety and soundness of credit unions and offering financial opportunities for their members. The significant role credit unions play in promoting competition and consumer well-being within the financial services marketplace cannot be overstated.

With that said, we believe the proposal, as drafted, creates a significant risk of competitive harm. Credit unions would not only have an obligation to share valuable analytic data about their members but would also be required to subsidize third-party access to this data by building and maintaining access infrastructures. Typically, it would take a financial company many years to acquire a historically significant amount of consumer data of the type and quality maintained by credit unions. However, the proposal fails to recognize the upfront investment and resulting value of establishing long-lasting, personalized consumer relationships. The approach of relationship banking, central to credit unions, goes beyond basic transactions, focusing on understanding the unique financial needs and goals of both individual consumers and communities, offering a range of financial products and services, and providing personalized guidance and support.

Considering the ongoing costs of building the infrastructure required by this proposed rule, along with the need for safeguarding sensitive member data, the proposed rule envisions a financial marketplace where fintech competitors can simply extract what they need once granted permission by a consumer. This would place credit unions at a disadvantage as compared to larger or more technologically advanced financial services providers, resulting in unintended consequences contrary to the proposed rule's intent or the intended meaning of section 1033.

## 2. Privacy and Data Security

### A. Privacy

The California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, underwent significant amendments on January 1, 2023, following the passage of California's Proposition 24, also known as the California Privacy Rights Act (CPRA). As the first comprehensive data privacy law in the U.S., the CCPA grants California consumers expanded rights regarding the collection and use of their personal information.

While the proposed rule recognizes comparable requirements in other applicable laws, including the CCPA, the Leagues recommend that the CFPB first conduct a thorough review of state laws like the CCPA in order to mitigate potential conflicts. The Leagues are concerned that adherence to one law might inadvertently lead to a potential violation of another, raising compliance and preemption questions. It's important to note that consumer privacy protection frameworks, especially those related to the CCPA, are continually evolving. Navigating these frameworks already poses significant challenges and complexities for covered entities.

### B. Data Security

- *Cybersecurity Risks*

The CFPB proposes to require in §1033.341(c) that a data provider disclose for its developer interface, in the public and readily identifiable manner described in proposed §1033.341(a), documentation, including metadata, describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface.

We believe the above requirements may inadvertently create new opportunities for hackers and fraudsters to compromise consumer financial data and funds. Cybersecurity fraud incidents have seen a significant increase, particularly for credit unions. As evidenced by data from the National Credit Union Administration (NCUA), since the NCUA's cyber incident reporting rule was implemented in September 2023, the NCUA reports 146 incidents within the initial 30 days, with over 60% attributed to third-party compromises.[1] Consequently, credit unions should anticipate an added layer of cybersecurity risk and associated costs due to the proposed rule's mandate regarding "developer interfaces."

[1] *See* NCUA Cybersecurity Update (October 2023), available at: https://ncua.gov/files/agenda-items/cybersecurity-board-briefing-20231019.pdf.

For credit unions, and especially smaller-sized credit unions, the ongoing cost of safeguarding members' financial data is substantial. This includes the cost of securing the needed infrastructure to support digital and online banking operations, as well as the specific cybersecurity costs that arise from mitigating data breaches and security incidents beyond the confines of regulated financial institutions. Credit unions also bear examination and compliance costs related to data security supervision.

The requirement for data providers to disclose identifying information publicly could expose vulnerabilities that hackers might exploit. We suggest that data providers be expected to furnish this information only after a contract has been signed with a third party allocating responsibilities, liability, and mitigating potential risks.

- *Hold Harmless Considerations*

In today's unpredictable cybersecurity landscape, there is a high likelihood that a third party obtaining data with the consumer's explicit permission could encounter a data breach involving information obtained from a credit union. While the credit union is typically not responsible for the breach, it could still face reputational risks, fraud losses, and expenses to rectify the situation for affected members. Additionally, seeking damages may be challenging for the credit union if other data users and holders are also affected. Resolving these data breach cases can be particularly intricate, time consuming, and costly, within the framework of existing laws.

Therefore, we strongly recommend that the CFPB include “hold harmless” provisions in the final rule. These provisions would help protect credit unions being forced by the rule to grant third-party access to consumer account data by mitigating some of the risks associated with hacking, fraud, identity theft, and data breaches. Such protections are crucial to ensure a fair and equitable regulatory environment for credit unions in the evolving landscape of data security and financial technology.

**3. Excluded Data Providers**

Proposed §1033.111(d) would exempt certain depository institutions that do not provide a consumer interface. Under proposed §1033.131, a “consumer interface” means “an interface that a data provider maintains to receive requests for covered data and make available covered data in an electronic form usable by consumers in response to the requests.” By acknowledging resource limitations for smaller entities, including credit unions, the proposed rule recognizes the challenges in supporting digital banking interfaces like online or mobile banking and aims to exempt them from this compliance obligation.

While we appreciate the CFPB's recognition of the challenges faced by smaller credit unions, we believe that the proposed exemption is overly restrictive. Even smaller sized credit unions offering online or mobile banking may find it challenging to compete without a robust digital interface. The infrastructure costs associated with complying with this rule may force them to choose between taking on the additional costs of compliance at a level that is not sustainable or discontinuing essential services like online and mobile banking.

The potential discontinuation of these services could have severe consequences for credit union members, including limited accessibility, reduced convenience, and time savings, as well as a loss of communication channels. Moreover, this distinction is more likely to disproportionately affect

underserved populations, impeding efforts to enhance financial literacy and empowerment. The decision to discontinue these services could result in a digital divide that would create disparities in access to financial technology and services among different socio-economic groups, which contradicts the CFPB's anti-competitive stance.

We urge the CFPB to reconsider the scope of the exemption to ensure that it does not inadvertently hinder the ability of small credit unions to provide crucial financial services. A more balanced approach is needed to address these concerns while still promoting fair competition and accessibility in the financial services sector.

To address these concerns, we propose a tiered exclusion approach. For data providers that offer no consumer interfaces, the existing exclusion from the rule should remain applicable. For depository institutions that meet the Small Business Administration's (SBA) definition of a small business concern, only the requirement to provide a consumer interface should apply. For depository institutions less than $50 billion in total assets, minimum technical performance specifications should not apply for developer interfaces.

**4. Prohibition of Fees**

The CFPB proposes in §1033.301(c) to prohibit data providers of all sizes from imposing any fees or charges for establishing or maintaining the interfaces required by proposed §1033.301(a) or for receiving requests or making available covered data through the interfaces. The CFPB notes that proposed §1033.301(c) would not prohibit a data provider from charging a fee for specific services, other than access to covered data, through the consumer interface.

While the proposal indicates that the CFPB acknowledges that data providers who do not already have a developer interface would incur some upfront and ongoing costs to establish and maintain one, and data providers in general will incur some cost to maintain the interfaces as well as marginal cost of providing covered data through the interfaces, it preliminarily determined that a data provider charging fees would be inconsistent with the data provider's statutory obligation under section 1033 of CFPA to make covered data available to consumers and to their authorized third party agents.

The Leagues strongly disagree with the CFPB's interpretation of section 1033's requirements and the rationale behind the proposed rule for the following two key reasons:

A. A blanket prohibition on fees is inconsistent with the CFPB's own guidance. In October 2023, the CFPB issued an Advisory Opinion regarding section 1034(c) of the CFPA, requiring large banks and credit union that have total assets of more than $10 billion to comply in a timely manner with consumer requests for information concerning their accounts for consumer financial products and services[2]. The Advisory Opinion asserts that a covered depository institution, including a credit union, would generally not violate section 1034(c) for imposing a fee or charge in limited circumstances such as charging a fee to a consumer who repeatedly requested and received the same information regarding their account. Based on this recent CFPB guidance, we believe it that would be reasonable for data providers to assess fees in cases of repeated requests by the third

[2] *See*, CFPB, Consumer Information Requests to Large Banks and Credit Unions (Oct. 2023), available at: https://www.govinfo.gov/content/pkg/FR-2023-10-16/pdf/2023-22774.pdf.

party where the data provider has already fulfilled its obligation and the information is unlikely to materially change, such as an annual percentage rate or annual percentage yield.

B. The proposed infrastructure requirements, which involve customizing interfaces for each third party, storage management, and maintenance of privacy and data security safeguards, signal that the anticipated costs for credit unions will be substantial. Credit unions predict that their estimated costs of a core processor change, should their current core is incapable of meeting the proposed requirements, will be staggering. The CFPB's position against allowing fees could potentially force credit unions to reconsider participating in an already competitive financial services market or affect their ability to offer affordable products and services to members. As nonprofit financial cooperatives, credit unions credit unions aim to avoid imposing burdensome account maintenance fees or charges on their member-owners. Traditionally, they strive to offer low or no-cost products and services, especially for consumers with modest means. Additionally, because they operate under a unique business model and do not have the same opportunities to raise capital as other data providers in the marketplace, credit unions must expand through retained earnings. While regulators, including the CFPB, focus on limiting sources of fee income, credit unions face challenges in growing their capital and seeking means of return to benefit their members. In light of these considerations, the Leagues firmly believe that credit unions and other data providers should be allowed to charge reasonable fees to third parties and aggregators.

**5. Compliance Dates**

Proposed §1033.121 would stagger the dates by which data providers need to comply with proposed §§1033.201 and 1033.301 (the obligations to make data available and establish interfaces) into four distinct tiers to ensure timely compliance with the rule's requirements. It states:

> "…[A] data provider must comply with §§1033.201 and 1033.301 beginning on:
>
> (a) [Approximately six months after the date of publication of the final rule in the Federal Register], for depository institution data providers that hold at least $500 billion in total assets and nondepository institution data providers that generated at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year.
>
> (b) [Approximately one year after the date of publication of the final rule in the Federal Register], for data providers that are: (1) Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets; or (2) Nondepository institutions that generated less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year.

> (c) [Approximately two and a half years after the date of publication of the final rule in the Federal Register], for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.
>
> (d) [Approximately four years after the date of publication of the final rule in the Federal Register], for depository institutions that hold less than $850 million in total assets."

We believe that the staggered implementation period as currently proposed would not allow sufficient time for credit unions acting as data providers to effectively comply. We have received feedback from multiple credit unions who have indicated they do not have core providers capable of providing the application programming interfaces (APIs) necessary to meet the conditions outlined in this proposed rule. In the absence of an interface platform that meets the required security and development standards, a substantial number of credit unions are faced with the prospect of having to change core platforms in preparation. Not only will this entail significant additional costs, but will impose severe constraints on credit unions, making it challenging for them to meet the proposed implementation deadline. To address this concern, the Leagues recommend dividing the last two cohorts of data providers (i.e., institutions with less than $850 million in total assets and those with assets between $850 million and $50 billion) into two separate groups. This division should include a one-year interval between them to determine compliance deadlines effectively.

Also, as outlined in the proposed rule, many smaller depository data providers will likely depend on core processors and other third-party service providers to establish the interfaces mandated by the rule. Given the potential demand on these providers, smaller entities may face significant wait times. Additionally, if a depository institution data provider opts to construct its own interface without third-party assistance, it may require extra time to do so.

We agree with the CFPB's acknowledgement that smaller data providers will rely on their core processors and other third party service providers to meet the requirements of this substantial proposed rule. Anticipating a potential compliance bottleneck, we believe it would be prudent for the CFPB to phase in compliance for smaller institutions.

**6. Address Liability for Misuse or Fraud**

The proposed rule does not explicitly cover the allocation of liability in cases of fraud, breaches, or stolen credentials among the involved parties. This omission poses challenges for many data providers, such as credit unions, particularly in the areas of error resolution and limitations on consumer liability, as outlined in Regulations E (implementing the Electronic Funds Transfer Act) and Z (implementing the Truth in Lending Act). Consequently, the proposed rule intends for data providers and third parties to collaboratively address the distribution of liability, which naturally places certain smaller entities at a negotiating disadvantage and creates the potential for those who breach the trust of consumers to avoid responsibility.

We strongly believe that the liability should reasonably follow the possession and control over the covered data, and that the CFPB should establish clear parameters in the rule for how this liability is to be allocated. The rule should not permit third parties to avoid responsibility for their own negligence or

misconduct and hold data providers accountable in cases of fraud, breaches, or stolen credentials once that covered data is no longer under the data providers' possession or control.

Furthermore, we strongly recommend that the CFPB establish accountability measures for third parties and data aggregators regarding such liability. For instance, if a third party, such as a fintech, acquires covered data under Regulation E with the consumer's permission from a credit union serving as the data provider, and unauthorized activity occurs under the fintech's control, the fintech should be obligated to conduct the error investigation and, if appropriate, reimburse the consumer in accordance with Regulation E requirements. Moreover, regulators would be expected to enforce these responsibilities as part of their oversight.

Addressing the issue of liability in this manner is essential to ensuring that there is no disparate impact on credit unions in their role as data providers, where they are already expected to shoulder the costs of initial compliance.

## III. Conclusion

We thank you for the opportunity to comment on the proposal and for considering our views. While the Leagues support the CFPB's stated desire to allow consumers the ability to have access to and control their own data, concerns about the practicality and implementation of a proposed rule of this magnitude are significant and require further examination and analysis before implementation.

We strongly encourage the CFPB to delay the proposed rule and allow the opportunity for a more collaborative engagement with a broader range of stakeholders beyond those consulted for this initial proposal. As it stands, the Leagues are concerned that the overwhelming cost and implementation challenges will make it difficult, if not impossible, for many credit unions to effectively compete in the current financial services marketplace, potentially diverting resources and attention away from their primary mission—meeting the financial needs of their members.

A more viable solution that is affordable to all data providers – including mission-focused credit unions – is essential. This solution should not only align with the spirit of section 1033, but also promote an environment where all participants in the financial services market can thrive.

If you have any questions regarding our comments, please do not hesitate to contact me.

Sincerely,

Diana R. Dykstra
President and CEO
California and Nevada Credit Union Leagues