January 25, 2023

Via Financial_Data_Rights_SBREFA@cfpb.gov
Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration, dated October 27, 2022

Consumer Reports is pleased to submit these comments in response to the Consumer Financial Protection Bureau's (CFPB's) Outline of Proposals and Alternatives Under Consideration regarding Required Rulemaking on Personal Financial Data Rights, issued October 27, 2022. The CFPB has requested comments on 149 questions as input on the proposals under consideration for making consumer financial information available pursuant to Dodd-Frank Act section 1033. The present comments address a selected number of those questions that we are particularly suited to answer as a consumer advocacy organization.

Permissioned data sharing can help consumers better manage their debt, budget their earnings, and save towards their goals. It can expand access to credit to many creditworthy Americans who are excluded by the credit reporting system's outdated mechanisms. It can facilitate wealth building and enable the behaviors that contribute to financial well-being. The consumers who are likely to benefit most from permissioned data sharing are those who traditionally have been excluded and underserved by the financial system.

In the current environment, any transfer of sensitive data is under relentless attack by those who would seek to exploit or defraud vulnerable individuals. Any situation where consumer financial data is transmitted in the absence of specific rules and protections constitutes a harm to consumers as a group. Protecting the consumer requires equal disclosure and oversight for all consumers of financial products and services, regardless of the size or stature of the provider. All financial data providers in this space should be regulated without exception.

In summary, Consumer Reports' comments address the following topics:

1. Coverage of data providers should be expanded to include Buy Now Pay Later firms and Earned Wage Access programs.
2. Authorization procedures should be modeled on the informed consent protocols prescribed for human subjects research under the Common Rule. These should be specific and tightly enforced.

3. Data should be provided in ways that protect consumers' personal identifying information as well as financial information, and data providers should be prohibited from charging fees for the provision of consumer data.
4. Third parties must observe data minimization requirements, provide a way for consumers to revoke authorization, and permit secondary uses only on an opt-in basis.

These comments are detailed below.

A. Coverage of data providers subject to the proposals under consideration (Questions 5, 8)

We advocate for expansion of the types of data providers that are covered under the proposed regulations. The Proposals describe covering two types of data providers: Regulation E accounts and Regulation Z credit card accounts. We suggest expanding this coverage in three ways.

1. First, all Regulation Z accounts should be covered under the proposed regulation. This will include all lenders, including mortgage lenders. In safeguarding consumers' financial data rights we should ensure those safeguards have broad coverage and not make exceptions that will curtail consumers' ability to access and utilize all of their own financial data. Consider a consumer who wishes to use a personal financial management service but who finds herself unable to include data on her mortgage and other loans. All Regulation Z entities hold important financial data for consumers that consumers should be able to access.

2. Second, other lenders that are not covered under Regulation Z but which occupy an important and growing role in consumers' financial lives should also be covered. These include Buy Now Pay Later lenders and Earned Wage Access programs. As the CFPB has noted, Buy Now Pay Later lending is exploding in popularity and warrants appropriate regulation. Buy Now Pay Later lenders in particular hold financial data the absence of which can lead directly to loan stacking and financial overextension. These services should be included in this rulemaking.

3. Core processors and data aggregators do not hold consumer accounts but they accomplish financial data transfer, payments, and other transactions for entities that do. As such they should be considered data providers under the proposed regulation. This addresses the substantial issue of smaller entities that may be considered for exemption from the present rulemaking. This is a critical financial inclusion and protection issue as the customers of smaller banks and credit unions, MDFIs and CDFIs stand to benefit greatly from the protections under consideration. Where smaller financial institutions might face constraints on their adherence to the present proposals on their own, the core processors and data aggregators that serve them would be able to bridge that gap so that their customers can enjoy the same protections.

B. Authorization Procedures (Questions 12, 13, 17, 18, 20)

The authorization procedures described in the outlined proposals bear a close resemblance to the informed consent procedures required for research with human subjects under the Common Rule (45 CFR part 46). A primary concern is the consent must be meaningful, that consumers must actually

understand that they are giving consent to share their financial data and all of the relevant details. In the context of human subjects research this concern is addressed by close and careful review of the language and protocols of consents, which is accomplished by institutional review boards (IRBs). Who will hold responsibility for this oversight of financial data sharing authorization procedures?

Financial institutions cannot be the arbiters of the adequacy of their own authorization forms and procedures. If the authorization suffers the fate of privacy policies, being quickly scrolled through in search of the "I agree" button, they will be completely ineffective. Some structure should be established to review each authorization disclosure for adherence to the requirements. Usability testing may be useful to ensure that the authorization disclosure and consent form are set up well to be meaningful to consumers.

As suggested in Q18, model forms or clauses provided by the CFPB may be of great assistance in assuring that the language of authorization forms is clear, accessible, and meaningful to users. That will not preclude the need for oversight and enforcement of authorization disclosure requirements because some elements will need to be customized, as detailed below, but it will facilitate the oversight by standardizing parts of the form.

The requirements for authorization disclosures should include:

- A maximum reading level, such as an eighth grade reading level.
- The full authorization disclosure should seek to maximize accessibility. This should include providing paper versions of all documents as an accommodation to consumers who cannot consent by electronic means.
- Key scope terms, including the categories of information to be accessed, the identity of the data provider and the accounts to be accessed, terms related to duration and frequency of access, and how to revoke access.
    - Duration and frequency should be restricted to the minimum necessary to accomplish the intended purpose. For example, for approval of a mortgage, data access should expire upon completion of the mortgage agreement.
    - Duration of data access should not exceed one year, or 365 days. Consent should need to be refreshed annually.
    - The process for revoking access should be easy to use and free of costs or penalties, and a link or instructions for accessing the revocation procedure should be included on the copy of the authorization form that is provided to the consumer.
    - A binding statement that revoking authorization will not affect other features or functions of the third party's services that are not dependent on the data sharing, if any.
    - A binding statement of the data security measures that will be employed by the third party. This may be included in the certification statement, if that is a separate document.
- Key use terms, including the identity of intended data recipients, downstream parties, and data aggregators to whom the data may be disclosed, and the purpose for accessing the information
    - Purposes for accessing the information should be narrowly tailored. Vague language such as "and for other purposes" should be specifically disallowed.

    - Sharing the consumer's data with downstream parties should be permitted only if that sharing is specifically required for the execution of the service for which the consumer is requesting data sharing. Downstream parties with whom the data will be shared should be severely limited and these parties should be named prominently in the authorization disclosure. Vague language such as "other third parties" should be disallowed.
- The disclosure should be provided clearly, conspicuously, and segregated from other material.
- The consent should require the consumer's signature or the electronic equivalent.
- Q20 and Q21: Providing the consumer a copy of their signed consent, either electronically or through the mail, should be required and non-negotiable. Consumers need the ability to refer back to the terms of their consent. The full authorization disclosure, including the third party's certification statement, should be included with the finalized consent provided to the consumer.

C. Making Information Available

- Q26 and Q27: Any measures that can potentially protect consumers from fraud or identity theft are highly important. Personal identifying information transmitted together with an individual's financial data is at high risk of being stolen. The CFPB's proposed confirm/deny approach is preferable to an approach where data providers give consumers' personally identifying information in order to verify an account. Another more secure approach is the tokenized authentication method utilized in the Financial Data Exchange API.

- Q41: Covered data providers should be prohibited from charging fees in connection with the provision of data. Fees would produce disparate impacts where the Americans who need the benefits of data sharing the most will be least able to afford it.

D. Third Party Obligations

- Q88: CFPB proposes a general limitation on data collection, use, and retention beyond what is reasonably necessary to provide the product or service the consumer has requested. Consumer Reports is in support of this data minimization requirement, as without it consumers would be exposed to potential exploitation and fraud.

- Q94: Third parties should be required to provide a simple way for consumers to revoke authorization at any point. This is an important consumer data right.

    - Further, third party authorization should be required to terminate when the consumer deletes or deactivates their account or relationship with the third party, or when the third party terminates the consumer's account for reasons other than fraud or suspicious activity.

- Q99: Secondary uses of consumer-authorized information should be prohibited unless the consumer opts into those uses. Any opt-out scheme disadvantages the consumer and constitutes a dark pattern inducing the consumer to share their data more widely than they otherwise would. Companies should be transparent with consumers (and regulators) about the

uses to which they intend to put the data. They should provide information about those uses in a clear, accessible, prominent, and timely manner along with an opportunity and clear instructions for the consumer to opt in to their choices. Further, companies must provide an accessible and easy-to-use way for the consumer to revoke any permissions they have previously given regarding secondary uses of data.

For further information, please contact:

Noemi Altman
Senior Survey Research Associate
Consumer Reports
Noemi.altman@consumer.org
(914) 378-2216