Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights

March 30, 2023

Table of contents

1. Introduction

Under the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), which amended the Regulatory Flexibility Act (RFA), the Consumer Financial Protection Bureau (Bureau or CFPB) must convene and chair a Small Business Review Panel (Panel) if it is considering a proposed rule that could have a significant economic impact on a substantial number of small entities.[1] The Panel considers the impact of the proposals under consideration by the CFPB and obtains feedback from representatives of the small entities that would likely be subject to the rule. The Panel comprises a representative from the CFPB, the Chief Counsel for Advocacy of the Small Business Administration (Advocacy),[2] and a representative from the Office of Information and Regulatory Affairs (OIRA) in the Office of Management and Budget (OMB).

This Panel Report addresses the CFPB's Required Rulemaking on Personal Financial Data Rights. The CFPB is in the process of writing proposed regulations to implement section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).[3] Section 1033 generally requires a covered person to make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person. On October 27, 2022, the CFPB issued its Outline of Proposals and Alternatives under Consideration (Outline) for this rulemaking.[4]

In accordance with the RFA, the Panel conducts its review at a preliminary stage of the CFPB's rulemaking process. The Panel's findings and discussion here are based on information available at the time the Panel Report was prepared and therefore may not reflect the updated findings of the CFPB in the process of producing a notice of proposed rulemaking (NPRM). As the CFPB proceeds with the rulemaking process, including taking actions responsive to the feedback received from small entity representatives (SERs) and the findings of this Panel, the CFPB may conduct additional analyses and obtain additional information. This Panel Report reflects feedback provided by the SERs and identifies potential ways for the CFPB to shape the proposals under consideration to minimize the burden of the eventual rule on small entities while achieving the purposes of the rulemaking. Options identified by the Panel for reducing the regulatory impact on small entities of the rule may require further consideration, information collection, and analysis by the CFPB to ensure that the options are practicable, enforceable, and consistent with the Dodd-Frank Act and other laws as applicable. Pursuant to the RFA, the CFPB will consider the Panel's findings when preparing the initial regulatory flexibility analysis in the eventual NPRM. This Panel Report will be included in the public record for the CFPB's Required Rulemaking on Personal Financial Data Rights.

---

[1] 5 U.S.C. 609(b).

[2] Advocacy is an independent office within the U.S. Small Business Administration (SBA), so the views expressed by Advocacy do not necessarily reflect the views of the SBA.

[3] Public Law 111-203, section 1021(a), 124 Stat. 1376, 1979 (2010) (codified at 12 U.S.C. 5511(a)).

[4] Bureau of Consumer Fin. Prot., Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

This Panel Report includes the following:

- A description of the proposals that are being considered by the CFPB and that were reviewed by the Panel;
- Background information on small entities that would likely be subject to those proposals and on the particular SERs selected to advise the Panel;
- A discussion of the feedback from and recommendations made by the SERs; and
- A discussion of the findings and recommendations of the Panel.

In particular, the Panel's findings and recommendations address the following:

- A description of and, where feasible, an estimate of the number and type of small entities likely impacted by the proposals under consideration;
- A description of projected compliance requirements of all aspects of the proposals under consideration;
- A description of alternatives to the proposals under consideration that may accomplish the stated objectives of the CFPB's rulemaking and that may reduce the economic impact on small entities of the proposals under consideration; and
- An identification, to the extent practicable, of relevant Federal laws or regulations that may duplicate, overlap, or conflict with the proposals under consideration.

2. Background

2.1 Market background

In modern consumer finance, financial entities hold a great deal of data about their customers and the products and services they offer. Such data have always been valuable to the account-holding entity, but consumers have been less able to benefit from their data for their own purposes. However, as technology has made it possible to store, analyze, and share personal financial data electronically, interest has grown within the financial services industry and among policymakers in the potential benefits of bolstering consumers' rights to access personal financial data and, if they wish, share their data with others, including competing financial services providers.[5]

[5] In the financial services industry, "data aggregation" firms emerged in the 2000s to enable consumer-authorized access to personal financial data. *See, e.g.*, Michael S. Barr *et al.*, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, Univ. of Mich. Ctr. on Fin., L. & Policy, Working Paper No. 1 (Nov. 1, 2019), https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

By accessing their financial data, consumers are better able to manage their financial lives. Today, many financial entities make a great deal of consumers' financial information available to them through online financial account management portals, but consumers may benefit from increased direct access to their financial data, as well as from the ability to share their data with third parties offering them a product or service that complements or relies on data about the products and services they already use.

Data access rights also hold the potential to intensify competition in consumer finance. This can happen in three main ways: by enabling improvements to existing products and services, by fostering competition for existing products and services, and by enabling the development of new types of products and services.[6] If consumers can authorize the transfer of their account data to a competitor, new providers will be able to treat new customers more like customers with longer account relationships, and may have greater ability to provide the better products usually reserved for long-time customers. Customers would not have to "start over," but could transfer the relationship built with an old provider to a new provider, potentially giving them access to higher credit limits or lower account fees. This could enhance competition and drive better service aimed at keeping customers. In addition, as firms use consumer-authorized data to both improve upon and provide greater access to existing products and services, as well as develop new products and services, consumers' motivation to switch providers to get a better deal may grow, making them more likely to abandon providers who treat them poorly. This should incentivize providers to earn their customers through competitive prices and high-quality service. Today, we believe there is evidence that market-driven consumer data access has already produced some of these benefits.[7]

While the CFPB is encouraged by some of the competitive effects of market-driven data access occurring today, it has become clear that these gains cannot be guaranteed until disagreements over consumer-authorized information sharing are addressed through rulemaking. Action is also

---

[6] Bureau of Consumer Fin. Prot., Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 FR 71003 (Nov. 6, 2020).

[7] Many consumers have adopted fintech services that tend to rely on or utilize direct access to consumer-authorized data and have authorized third parties to access their financial data. One trade association estimates that the number of consumers who have utilized a service affected in some way by consumer-authorized data sharing may be as large as 100 million, and that the number of consumer and small business accounts accessed by authorized third parties is estimated to be 1.8 billion. *See* Fin. Data & Tech. Ass'n (FDATA), *Competition Issues in Data Driven Consumer and Small Business Financial Services* 11 (June 2020), https://fdata.global/north-america/wp-content/uploads/sites/3/2020/06/FDATA-US-Anticompetition-White-Paper-FINAL.pdf. Further, the EY Global FinTech Adoption Index shows that in 2019, 46 percent of digitally active U.S. consumers were "fintech adopters," up from 17 percent in 2015 and 33 percent in 2017. EY, *Global FinTech Adoption Index* 6 (2019), https://www.ey.com/en_us/ey-global-fintech-adoption-index. Fintech adopters are consumers who use at least one fintech service from at least two of these five categories: savings and investments; borrowing; insurance; money transfer and payments; and budgeting and financial planning. Many such services, when offered by fintechs, rely on or routinely utilize consumer-authorized data access. To the extent this widespread adoption indicates consumers are voting with their feet, and to the extent such opting for improved offerings is catalyzed by consumer-authorized data access, competition in consumer finance appears to benefit from the ability of consumers to permit third parties to directly access their personal financial data.

needed to ensure that consumer-authorized information shared with third parties is not used for purposes not requested by the consumer or obtained using misleading tactics, particularly by firms whose surveillance revenue models incentivize them to use and abuse consumer data. Such practices have contributed to a lack of trust among market participants, and a growing sense of powerlessness among consumers.

2.2 Statutory authority

Section 1021(a) of the Dodd-Frank Act states that the purpose of the CFPB is "to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[8] Consistent with that purpose, section 1033(a) of the Dodd-Frank Act authorizes the CFPB to prescribe rules requiring

> a covered person [to] make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.[9]

In addition, section 1033(d) states that "[t]he Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section."[10]

By issuing the Outline, convening the Panel, and completing this Panel Report, the CFPB is fulfilling its obligations under SBREFA to assess the impact of its proposals under consideration on directly affected small entities prior to issuing an NPRM regarding section 1033.

2.3 Closely related Federal laws and regulations

Other Federal statutes and regulations that have potentially overlapping or conflicting requirements are described below.

The Equal Credit Opportunity Act (ECOA)[11] and the CFPB's implementing regulation, Regulation B (12 CFR part 1002), prohibit creditors from discriminating in any aspect of a credit transaction, including a business-purpose transaction, on the basis of race, color, religion, national origin, sex, marital status, age (if the applicant is old enough to enter into a contract),

---

[8] Public Law 111-203, section 1021(a), 124 Stat. 1376, 1979 (2010) (codified at 12 U.S.C. 5511(a)).

[9] Dodd-Frank Act section 1033(a), 124 Stat. 2008 (codified at 12 U.S.C. 5533(a)). The full text of section 1033 is included as Appendix A.

[10] Dodd-Frank Act section 1033(d), 124 Stat. 2008 (codified at 12 U.S.C. 5533(d)).

[11] 15 U.S.C. 1691 *et seq*.

receipt of income from any public assistance program, or the exercise in good faith of a right under the Consumer Credit Protection Act.

The Electronic Fund Transfer Act (EFTA)[12] and the CFPB's implementing regulation, Regulation E (12 CFR part 1005), establish a basic framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems. Among other requirements, EFTA and Regulation E prescribe requirements applicable to electronic fund transfers, including disclosures, error resolution, and rules related to unauthorized electronic fund transfers.

The Fair Credit Reporting Act (FCRA)[13] and the CFPB's implementing regulation, Regulation V (12 CFR part 1022), govern the collection, assembly, and use of consumer report information and provide the framework for the credit reporting system in the United States. They also promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. They also include limitations on the use of certain types of consumer information, limitations on the disclosure of such information to third parties, as well as certain requirements related to accuracy and dispute resolution.

The Gramm-Leach-Bliley Act (GLBA)[14] and the CFPB's implementing regulation, Regulation P (12 CFR part 1016), require financial institutions subject to the CFPB's jurisdiction to provide their customers with notices concerning their privacy policies and practices, among other things. They also place certain limitations on the disclosure of nonpublic personal information to nonaffiliated third parties, and on the redisclosure and reuse of such information. Other parts of the GLBA, as implemented by regulations and guidelines of certain other Federal agencies (*e.g.*, the Federal Trade Commission's Safeguards Rule and the prudential regulators' Safeguards Guidelines), set forth standards for administrative, technical, and physical safeguards with respect to financial institutions' customer information. These standards generally apply to the security and confidentiality of customer records and information, anticipated threats or hazards to the security or integrity of such records, and unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

The Truth in Lending Act (TILA)[15] and the CFPB's implementing regulation, Regulation Z (12 CFR part 1026), impose requirements on creditors and include special provisions for credit offered by credit card issuers. Among other requirements, TILA and Regulation Z prescribe requirements applicable to credit cards, including disclosures, error resolution, and rules related to unauthorized credit card use.

The Truth in Savings Act (TISA)[16] and the CFPB's implementing regulation, Regulation DD (12 CFR part 1030), apply to depository institutions; TISA and Part 707 of the National Credit

---

[12] 15 U.S.C. 1693 *et seq.*

[13] 15 U.S.C. 1681 *et seq.*

[14] 15 U.S.C. 6801 *et seq.*

[15] 15 U.S.C. 1601 *et seq.*

[16] 12 U.S.C. 4301 *et seq.*

Union Administration Rules and Regulations apply to credit unions. Among other things, TISA and Regulation DD prescribe requirements applicable to deposit accounts, including disclosure requirements.

The Real Estate Settlement Procedures Act of 1974 (RESPA)[17] and the CFPB's implementing regulation, Regulation X (12 CFR part 1024), include requirements applicable to mortgage servicers that seek to protect borrowers against certain billing and servicing errors.

3. Overview of proposals and alternatives under consideration

This section summarizes the CFPB's proposals and alternatives under consideration as set forth in the Outline. The Outline is attached to this Panel Report as Appendix D.

3.1 Coverage of financial institutions and card issuers

The proposals under consideration would use two existing definitions to establish coverage over data providers: "financial institution" as defined by Regulation E, and "card issuer" as defined by Regulation Z. The data providers that would be directly affected by the proposals under consideration include depository and nondepository financial institutions that provide consumer funds-holding accounts or that otherwise meet the Regulation E definition of financial institution. The data providers that would be directly affected by the proposals under consideration also include depository and nondepository institutions that provide credit cards or otherwise meet the Regulation Z definition of card issuer.[18] Entities that meet the Regulation Z definition of card issuer include persons that issue a credit card and those persons' agents with respect to the card.

3.2 Coverage of asset accounts and credit card accounts

Under the proposals the CFPB is considering, a Regulation E financial institution would be a covered data provider with respect to an "account," as that term is defined in Regulation E § 1005.2(b). Under that regulatory provision, an account is "a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes." The term includes a prepaid account. In the Outline, the CFPB refers to an "account" as that term is defined in § 1005.2(b) as an "asset account."

Also, under the proposals the CFPB is considering, a Regulation Z card issuer would be a covered data provider with respect to a "credit card account under an open-end (not home-secured) consumer credit plan" as that term is defined in Regulation Z § 1026.2(a)(15)(ii). Under that regulatory provision, a credit card account under an open-end (not home-secured) consumer credit plan is "any open-end credit account that is accessed by a credit card." In the Outline, the CFPB refers to such an account as a "credit card account."

---

[17] 12 U.S.C. 2601 *et seq.*

[18] *See* 12 CFR 1026.2(a)(7).

3.3 Potential exemptions for certain covered data providers

The CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers. However, in determining if exemptions would be appropriate, the CFPB is interested in whether there are ways to design the proposals under consideration to reduce impact on covered data providers. The CFPB seeks to ensure that the proposals under consideration appropriately balance benefits provided to consumers with the burden imposed on covered data providers, including smaller covered data providers, in a manner that is consistent with the statutory purposes of the Dodd-Frank Act.

To the extent exemptions would be appropriate, the CFPB is interested in how to define eligibility criteria. The CFPB seeks to strike a balance between benefitting as many consumers as possible by the proposals under consideration and avoiding undue burden on covered data providers. The CFPB also seeks to develop criteria that would allow a covered data provider to easily determine whether it is exempt. If the CFPB were to exempt certain covered data providers from the proposals under consideration, the CFPB is considering whether and how it should address a situation in which a data provider that previously did not meet the criteria for an exemption later meets the criteria, and a data provider that no longer meets the criteria.

3.4 Consumers as recipients of information

Section 1033(a) of the Dodd-Frank Act generally requires data providers to make information available to a "consumer." Section 1002(f) defines a consumer as an "individual."[19] In the Outline, the CFPB refers to covered data providers making information available, upon request, directly to a consumer as "direct access."

The CFPB is considering how its proposals under consideration should address a covered data provider's obligation to make information available directly to a consumer when the account is held by multiple consumers, such as an account held jointly by spouses. The CFPB is not considering any proposal that would affect covered data providers' existing obligations to provide information directly to consumers under other Federal consumer financial laws, such as the Electronic Fund Transfer Act (EFTA), the Truth in Lending Act (TILA), and the Truth in Savings Act (TISA), and their implementing regulations. Those regulations generally permit covered data providers to satisfy the relevant information disclosure requirements by providing the information to any one of the consumers on the account.[20] Here, the CFPB is considering proposing that a covered data provider would satisfy its obligation to make information available directly to a consumer by making the information available to the consumer who requested the information or all the consumers on a jointly held account.

[19] *See* 12 U.S.C. 5481(4).

[20] *See* 12 CFR 1005.4(c), 1030.3(d), 1026.5(d).

3.5 Authorized third parties as recipients of information

Section 1033(a) of the Dodd-Frank Act generally requires data providers to make information available to a "consumer," which includes an agent, trustee, or representative acting on behalf of an individual consumer.[21] In the Outline, the CFPB uses "third-party access" to refer to covered data providers making information available, upon request, to authorized third parties.

The CFPB is considering proposals related to authorization procedures for third parties to access consumer information on consumers' behalf. These proposals seek to ensure that such third parties are acting on behalf of the consumer. The proposals under consideration would include a requirement that, in order to access consumer information under the rule, the third party accessing the information would need to: (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information (certification statement).

3.6 Section 1033(a)—making information available

Section 1033(a) of the Dodd-Frank Act authorizes the CFPB to require a data provider to make available information in the control or possession of the data provider that concerns the consumer financial product or service that the consumer obtained from the data provider. The Outline discusses the proposals under consideration that address the information a covered data provider would be required to make available to a consumer or an authorized third party concerning the consumer financial product or service that the consumer obtained from the covered data provider. The proposals under consideration would not affect covered data providers' obligations under existing statutes and regulations—*i.e.*, statutes and regulations other than Dodd-Frank Act section 1033—to make available to consumers the information specified in those existing statutes and regulations.

The following subparts set forth six categories of information the CFPB is considering requiring covered data providers to make available with respect to covered accounts. The categories are intended to reflect the type and range of information the CFPB is considering. The specific data elements set forth within each of the six categories should not be taken as exhaustive but as representative of the data elements the CFPB is considering.

1. Periodic statement information for settled transactions and deposits (Outline part III.C.1.i);
2. Information regarding prior transactions and deposits that have not yet settled (Outline part III.C.1.ii);
3. Other information about prior transactions not typically shown on periodic statements or portals (Outline part III.C.1.iii);
4. Online banking transactions that the consumer has set up but that have not yet occurred (Outline part III.C.1.iv);

[21] *See* 12 U.S.C. 5481(4).

5. Account identity information (Outline part III.C.1.v); and
6. Other information (Outline part III.C.1.vi).

3.7 Section 1033(b)—statutory exceptions to making data available

Dodd-Frank Act section 1033(b) sets forth four exceptions to the general section 1033(a) requirement to make information available. Specifically, section 1033(b) states that a data provider may not be required by section 1033 to make available—

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

The CFPB is considering how to interpret these exceptions and how they should affect the CFPB's proposals under consideration regarding the types of information that covered data providers would be required to make available.

3.8 Section 1033(c)—no duty to retain records (current and historical information)

The CFPB is considering proposals with respect to defining the scope of current and historical information that covered data providers would be required to make available to consumers or authorized third parties, depending on what type of information is requested. The CFPB is considering proposing that a covered data provider would need to make available the most current information that the covered data provider has in its control or possession at the time of a request for current information.

With respect to historical information that may be requested, Dodd-Frank Act section 1033(c) states that section 1033 shall not be construed to impose a duty on a data provider to maintain or keep any information about a consumer. In light of section 1033(c), the CFPB is considering proposals under which a covered data provider would be required only to make available information going as far back in time as that covered data provider makes transaction history available directly to consumers, such as, but not limited to, through the covered data provider's online financial account management portal.

3.9 How and when information must be made available to consumers

With respect to requests for direct access, the CFPB is considering proposing that a covered data provider would be required to make available information if it has enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested. The CFPB is also considering proposing that covered data providers would need to make available all the information that would be covered by the proposals under consideration

through online financial account management portals and allow consumers to export the information covered by the proposals under consideration in both human and machine readable formats.

3.10 How and when information must be made available to third parties

The CFPB is considering proposing that covered data providers would be required, upon request, to make information available to third parties authorized to access information on a consumer's behalf. The CFPB is considering proposing that covered data providers would be required to establish and maintain a third-party access portal that does not require the authorized third party to possess or retain consumer credentials.

The CFPB is considering various proposals related to the availability of information obtained through such third-party access portals, the security of such portals, and the impacts of such portals on the accuracy of information accessed through them.

The CFPB is also considering proposing that a covered data provider would be required to make information available to a third party, upon request, when the covered data provider 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. The CFPB is seeking to ensure that third parties that do not meet these conditions are prevented from obtaining access to the information. The CFPB is considering how to address circumstances in which third parties could be prevented from getting access to information where they do not satisfy the conditions.

The CFPB is considering whether covered data providers should be required to make information available to third parties when the covered data provider knows the information requested is inaccurate.

Regarding other covered data provider disclosures, the CFPB is considering whether it should require covered data providers to disclose to consumers or authorized third parties the reason information is not available pursuant to the section 1033(b) exceptions. In addition, the CFPB is considering whether covered data providers should be required to disclose to consumers or third parties why access is prevented for reasons other than the section 1033(b) exceptions.

3.11 Limiting the collection, use, and retention of consumer-authorized data

The CFPB is considering proposals under which third parties accessing consumer-authorized information would have to limit their collection, use, and retention of that information. The proposals under consideration would include collection limitations related to the duration and frequency of information accessed pursuant to consumer authorization, including requiring that authorized third parties provide consumers a simple way to revoke access. The proposals under consideration would also include limitations on uses of consumer-authorized information. Finally, the proposals under consideration would also include deletion requirements and limitations on retention of consumer-authorized information.

3.12 Third party commitments on data security

The CFPB is considering a proposal to require authorized third parties to implement data security standards to prevent authorized third parties from exposing consumers to harms arising from inadequate data security. Although the CFPB believes that authorized third parties that seek to access consumer-authorized information are also likely subject to the GLBA safeguards framework, the CFPB is considering whether it should impose specific data security standards on authorized third parties under the rule.

3.13 Third party commitments on data accuracy and dispute resolution

The CFPB is considering a proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the information that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers.

3.14 Disclosures related to third party commitments

The CFPB is considering proposals related to disclosure requirements applicable to authorized third parties to enable consumers to make informed decisions about ongoing collection, use, and retention of consumer-authorized information. The CFPB is also considering proposing that authorized third parties would need to provide consumers with a mechanism to request information about the extent and purposes of the authorized third party's access.

3.15 Record retention obligations

The CFPB is considering proposing record retention requirements for covered data providers and authorized third parties to demonstrate compliance with certain requirements of the rule.

3.16 Implementation period

The CFPB seeks to ensure that consumers have the benefit of a final rule within a short timeframe, while also seeking to ensure that covered data providers and authorized third parties have sufficient time to implement the rule. As such, the CFPB is considering the proper implementation period for complying with the rule. The CFPB is also considering whether certain covered data providers should not be subject to the third-party access portal requirement on the rule's compliance date and instead should be given additional time to build a compliant third-party access portal.

3.17 Potential impacts on small entities

3.17.1 CFPB review of implementation processes and costs to data providers

For covered data providers, the proposals under consideration would lead to one-time and ongoing costs. The CFPB expects that the largest costs would involve building and maintaining a third-party access portal. The CFPB expects that small entities would comply with the proposals under consideration by either contracting with a vendor to implement a third-party access portal, or by developing a third-party access portal in-house.

Lacking direct data on costs associated with building or maintaining a compliant third-party access portal, the CFPB conducted market research and spoke with industry participants. In the Outline, the CFPB estimated a monthly ongoing cost for covered data providers that contract with a vendor to implement a third-party access portal ranging from several hundred dollars to as high as $50,000, with limited additional upfront or ongoing costs. For covered data providers that build a third-party access portal fully in-house, the CFPB estimated a total upfront staffing cost ranging from $216,000 to $432,000 and ongoing staffing costs of $42,000 to $83,000.

Covered data providers would incur additional costs to comply with the direct access requirements of the proposals under consideration. Assuming all covered data providers have an online financial account management portal, the added costs would stem from making additional required information available that is not currently provided through the portal. Covered data providers who contract a vendor to provide their online financial account management portal would likely rely on their vendor to add the additional information, with potentially limited added costs. For covered data providers who maintain their portal in-house, the CFPB estimates a one-time cost of $21,000 to $42,000 to do so. Finally, to comply with the proposals under consideration, covered data providers would need to develop or update their standard disclosures and record retention policies and procedures and review compliance with the proposals as a whole. In the Outline, the CFPB estimated an upfront cost of roughly $5,500 to $11,700 for developing and implementing compliant procedures.

3.17.2 CFPB review of implementation processes and costs to third parties

For third parties, the proposals under consideration may require modifications to existing systems or procedures to meet the conditions required for authorized data access, such as providing the authorization disclosure and certification statement; implementing the limitations on data collection, use, and retention; mechanisms for revocation of authorization and deletion; potentially providing ongoing disclosures and opportunities to reauthorize access; and record retention requirements.

The CFPB is considering proposals that would require third parties to build and maintain systems that could receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revocation or authorization lapses. These systems would also need to retain records as required by the proposals under consideration. In the Outline, the CFPB estimated that building and maintaining an appropriate data system would cost up to $75,000. In addition, the CFPB estimated that building systems to provide the authorization disclosure and certification statement would cost $83,000, but that costs may only need to be incurred by third parties that are data aggregators.

To implement the proposals under consideration, third parties would need to develop and maintain policies and procedures in several distinct areas. These include (1) a comprehensive written data security program appropriate to their size and complexity, (2) reasonable policies and procedures to ensure the accuracy of the data that they collect, (3) policies governing the limits on collection, use, and retention of consumer-permissioned data, and (4) record retention requirements for third parties to demonstrate adherence to certain requirements of the eventual rule. In the Outline, the CFPB estimated an upfront cost of roughly $8,200 for developing and implementing compliant necessary procedures and expects limited ongoing costs.

3.17.3 Impacts of proposals under consideration on data providers

The proposals under consideration would lead to increased integration of data and communications systems between covered data providers and third parties. The CFPB expects that most existing consumer-permissioned data access that occurs through screen scraping would transition to new third-party access portals, and additional consumer-permissioned data sharing may be facilitated if the proposals under consideration lower the barriers to establishing third party connections. However, some existing consumer-permissioned data access may require modifications if the requirements and conditions on data collection, use, and retention for third parties make certain business models or use cases unprofitable. These indirect effects of the proposals under consideration may include both costs and benefits for small data providers, depending on the specifics of their institution and their desire to provide authorized data access.

The CFPB anticipates that the proposals under consideration would reduce the set of negotiable terms in agreements between a data provider and a data aggregator or data recipient on the terms of consumer-authorized data access, as these terms would be largely determined by the proposals. Depending on the data providers' desired terms of access, these changes may reflect an indirect benefit or cost of the proposals under consideration.

Some third-party products and services derived from consumer-permissioned data sharing can be complementary to the services offered by data providers, while other uses compete with data providers' internal products and services.

Some of the proposals under consideration may require data providers to make available additional data fields relative to the status quo, while others may reduce the data fields available to third parties. This may either enable new third-party products or use cases or reduce the profitability of existing products. This may represent an indirect cost or benefit of the proposals under consideration.

The CFPB understands that consumer-permissioned data access that occurs through third-party access portals may involve substantially lower traffic loads per instance than screen scraping. The transition to third-party access portals is therefore likely to reduce total traffic. Similarly, proposals under consideration related to the collection, use, and retention limitation standard are likely to reduce total traffic, particularly for use cases which do not require large data fields such as detailed transaction information.

The transition away from credential-based authorized data access to tokenized access would likely reduce the risk of data breaches and resulting potential costs for data providers.

3.17.4 Impacts of proposals under consideration on third parties

Some of the proposals under consideration would create conditions for third parties that place limits on the uses and retention of consumer financial data. These conditions could impede certain products or business models that third parties use to generate revenue, such as the required deletion of consumer's financial data when authorization lapses or is revoked. If third parties rely on such data to develop new products or services, the proposals under consideration could hinder these use cases.

Recipient-not-present personal financial management services rely on frequent monitoring of balances and transactions. These services may become more limited if the CFPB requires periodic reauthorization, as third parties will be unable to collect account data if a consumer fails to reauthorize its access. However, these services may be improved by increasing the availability of relevant data elements.

The CFPB anticipates that the proposals under consideration will enable third parties to obtain more data elements from covered data providers relative to the status quo. The CFPB is also considering proposals that would regulate the availability of these data elements and may make them available more often by creating requirements for third-party access portals' uptime, latency, planned outages, error response, and access caps. These changes may improve the quality of services offered by third parties, and these services may better compete with (or complement) data providers' own services. This may be particularly salient when the data provider's product makes use of data that was not shared with third parties prior to the rulemaking, but under the rulemaking will be required to be shared.

4. Applicable small entity definitions

A "small entity" may be a small business, small nonprofit organization, or small government jurisdiction. The NAICS classifies business types and the SBA establishes size standards for a "small business." To assess the impacts of the proposals under consideration, the Panel met with small entities that may be impacted by those proposals. Any small entity that falls within the eventual rule's definition of a data provider that meets the definition of "financial institution" set forth in Regulation E or "card issuer" set forth in Regulation Z could potentially be affected. However, as previously discussed, the CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers. Additionally, any small entity that falls within the eventual rule's definitions of a data recipient and data aggregator could also be affected. In this instance, the CFPB sought feedback from depository institutions, as well as nondepository financial institutions and entities outside of the financial industry that may fall within the eventual rule's definitions of data providers, data recipients, or data aggregators.

5. Small entities that may be subject to the proposals under consideration

The Panel is required to collect advice and recommendations from SERs that are likely to be subject to the regulation that the CFPB is considering proposing. For this purpose, the RFA defines "small entities" as small businesses, small organizations, and small governmental jurisdictions. The term "small business" has the same meaning as "small business concern" under section 3 of the Small Business Act (SB Act);[22] the term "small organization" is defined as any not-for-profit enterprise which is independently owned and operated and is not dominant in its field; and the term "small governmental jurisdiction" is defined as the governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of

[22] Public Law 85-536, section 2, 72 Stat. 384 (1958) (codified at 15 U.S.C. 631).

less than 50,000.[23] Thus, to determine whether a business is a small entity, the CFPB looks to the SBA's size standards.[24]

Small entities likely to be affected by the proposals under consideration are those that meet the definitions of covered data providers,[25] data recipients, or data aggregators. Covered data providers include depository institutions and nondepository institutions.

Nondepository financial institutions and entities outside of the financial industry may also be affected, though it is important to note that entities within these industries would only be subject to the proposals under consideration if they meet the definitions of covered data provider, data recipient, or data aggregator. The CFPB expects that thousands of these small nondepositories likely meet the definition of data recipient, and a smaller number likely meet the definitions of covered data provider or data aggregator. Examples of potentially affected small data recipients include entities using consumer-authorized information to underwrite loans, offer budgeting or personal financial management services, or facilitate payments. These examples are not intended to cover all potential third parties or uses of consumer-authorized information.

The Panel has identified 17 categories of small businesses that are likely to represent most small entities that may be subject to the eventual rule, together with the maximum asset size or average annual receipts to be considered a small business under each NAICS code.[26]

---

[23] *See* 5 U.S.C. 601(3) through (6).

[24] *See* Small Bus. Admin., *Table of Small Business Size Standards Matched to North American Industry Classification System Codes* (effective Dec. 19, 2022), https://www.sba.gov/sites/default/files/2022-12/Table%20of%20Size%20Standards_Effective%20December%2019%2C%202022_508%20%281%29_0.pdf (SBA Size Standards).

[25] As explained above, the proposals under consideration would use two existing definitions to establish coverage over data providers: "financial institution" as defined by Regulation E, and "card issuer" as defined by Regulation Z. In this Outline, the CFPB refers to financial institutions and card issuers collectively as "covered data providers."

[26] The SBA regularly updates its size thresholds to account for inflation and other factors. The SBA Size Standards described here reflect the thresholds and NAICS codes in effect at the publication date of this report. *See* Small Bus. Admin., *Table of Small Business Size Standards Matched to North American Industry Classification System Codes* (effective Dec. 19, 2022), https://www.sba.gov/sites/default/files/2022-12/Table%20of%20Size%20Standards_Effective%20December%2019%2C%202022_508%20%281%29_0.pdf.

Table 1: SBA size standards for businesses that may be subject to the proposals under consideration, by NAICS industry

Code Description	NAICS CODE	SBA Size Standard to Be Considered Small
Software Publishers	513210	$47 million in receipts
Computing Infrastructure Providers, Data Processing, Web Hosting, and Related Services	518210	$40 million in receipts
Commercial Banking	522110	$850 million in assets
Credit Unions	522130	$850 million in assets
Savings Institutions and Other Depository Credit Intermediation	522180	$850 million in assets
Credit Card Issuing	522210	$850 million in assets
Sales Financing	522220	$47 million in receipts
Consumer Lending	522291	$47 million in receipts
Real Estate Credit	522292	$47 million in receipts
Financial Transactions Processing, Reserve, and Clearinghouse Activities	522320	$47 million in receipts
Other Activities Related to Credit Intermediation	522390	$28.5 million in receipts
Investment Banking and Securities Intermediation	523150	$47 million in receipts
Commodities Contracts Intermediation	523160	$47 million in receipts
Financial Transactions Processing, Reserve, and Clearinghouse Activities	522320	$47 million in receipts
Payroll Services	541214	$39 million in receipts
Custom Computer Programming Services	541511	$34 million in receipts
Credit Bureaus	561450	$41 million in receipts

In addition, as discussed above, a "small organization" is any not-for-profit enterprise which is independently owned and operated and is not dominant in its field, and "small governmental jurisdictions" are the governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than 50,000.[27]

6. Summary of small entity outreach

6.1 Summary of the Panel's outreach meetings with small entity representatives

The CFPB convened the Panel on February 1, 2023, and held two Panel Outreach Meetings on February 1 and 2, 2023.

In preparation for the Panel Outreach Meetings and to facilitate an informed and detailed discussion of the proposals under consideration, discussion questions for the SERs were included throughout the CFPB's Outline; several of these questions also appeared in a shorter High-Level Summary and Discussion Guide (see Appendix E).

In advance of the Panel Outreach Meetings, the CFPB, Advocacy, and OIRA held a total of three WebEx video conferences with the SERs in December 2022 and January 2023 (pre-Panel video conferences) to describe the SBREFA process, obtain important background information about each SER's current business practices, and begin discussions on selected portions of the proposals under consideration.

Representatives from 18 small businesses were selected as SERs for this SBREFA process and participated in the Panel Outreach Meetings. Representatives from the CFPB, Advocacy, and OIRA provided introductory remarks. The meetings were then organized around discussions led by the CFPB's Office of Regulations, Office of Markets, and Office of Research about each aspect of the proposals under consideration and the potential impact on small businesses. The presentation slides framing this discussion are attached at Appendix F. The CFPB also provided the SERs with an opportunity to submit written feedback by February 15, 2023. Seven of the 18 SERs provided written feedback, copies of which are attached at Appendix B.

6.2 Other outreach efforts, including to small entities

In addition to the SBREFA process, the CFPB has conducted extensive outreach efforts to stakeholders, including consumer and community-based groups, industry and trade groups, and other Federal and State agencies.

As part of its market monitoring process, the CFPB is engaged in ongoing discussions with data providers, data recipients, and data aggregators regarding the consumer-authorized financial data ecosystem. The CFPB plans to continue to conduct outreach to stakeholders, including to consumer groups, community advocates, and industry participants of a range of sizes.

[27] 5 U.S.C. 601(3) through (6).

7. List of small entity representatives

The following 18 SERs were selected to participate in the Panel's Small Business Review process.

Table 2: List of SERs

Name & Title	Business Name, City, and State	Business Type
Adam Roseman Co-Founder & President	Steady Atlanta, GA	Income verification and personal financial management for gig workers
Anthony Patti Executive Vice President & Chief Financial Officer	Reading Cooperative Bank Reading, MA	Bank
Bryan Garcia Chief Technology Officer	Finlocker St. Louis, MO	Mortgage underwriting
Christopher Petersen Executive Vice President, Chief Financial Officer & Chief Information Officer	St. Paul Federal Credit Union St. Paul, MN	Credit union
Dominik Mjartan President & Chief Executive Officer	Optus Bank Columbia, SC	Bank and Minority Depository Institution
Jason (Gross) Rosen Co-Founder & Chief Executive Officer	Petal Atlanta, GA	Non-bank credit card lender
Jeff Jacobson Compliance Officer	New Market Bank New Market, MN	Bank
Jim Morrell President & Chief Executive Officer	Peninsula Community Federal Credit Union Shelton, WA	Credit union
Joyce Chen Product & Regulatory Counsel	Nova Credit San Francisco, CA	Alternative credit underwriting
Kahlil Lalji Chief Executive Officer	Ivella Santa Monica, CA	Neobank
Leigh Phillips President & Chief Executive Officer	SaverLife San Francisco, CA	Financial wellness and personal financial management
Lori Frederick Head of Banking & Payments	Ninth Wave New York, NY	Data aggregator

Name & Title	Business Name, City, and State	Business Type
Melanie Kennedy Chief Executive Officer	Southwest Financial Federal Credit Union Farmer's Branch, TX	Credit union
Michelle Corson Founder & Chief Executive Officer	On the Road Lending Irving, TX	Deep subprime auto loans and personal financial management
Monica Davis Senior Vice President – Risk Management	Union Square Credit Union Wichita Falls, TX	Credit union
Parag Shah Founder & Chief Technology Officer	Vemos Sao Palo, CA	Non-bank mobile payments
Pietro Grandinetti President & Chief Technology Officer	Pentadata Burlingame, CA	Data aggregator
Rob Curtis Co-Founder & Chief Executive Officer	Daylight West Hollywood, CA	Neobank

8. Summary of feedback from small entity representatives

Through the SBREFA process, the Panel solicited feedback from small entities early in the rulemaking proceeding and prior to the CFPB's development of an NPRM. To obtain specific information about the costs of complying with a potential rulemaking, the CFPB provided SERs with a list of questions to consider about the impacts of the proposals under consideration and to assist the CFPB in refining them. These discussion questions, which were part of the Outline (Appendix C), formed the basis of the Panel Outreach Meetings and the subsequent written feedback. Several of these discussion questions also appear in the High-Level Summary and Discussion Guide (Appendix E).

During the Panel Outreach Meetings, as well as during the pre-Panel video conferences and in written feedback submitted by SERs following the Panel Outreach Meetings, the SERs provided feedback on most aspects of the proposals under consideration. The SERs provided information to the Panel about their business operations and how the CFPB's proposals under consideration could impact their businesses. The Panel appreciates the meaningful feedback and data that SERs provided and for the time they spent assisting the Panel. This section summarizes SER feedback on the various parts of the Outline. Written feedback provided by SERs is included in Appendix B.

The section below describes the SERs as either data providers or third parties. As explained in the Outline, a "data provider" means a covered person with control or possession of consumer financial data. In the Outline, the CFPB refers to data recipients and data aggregators, generally, as "third parties." A "data recipient" means a third party that uses consumer-authorized

information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer. A "data aggregator" means an entity that supports data recipients and data providers in enabling authorized information access. Depending on the context and its activities, a particular entity might meet several of these definitions. In preparing this Report, the Panel has attempted to characterize the SERs based on the inferred capacity in which they provided feedback.

8.1 General feedback from SERs

Multiple SERs agreed that consumer-authorized data sharing and consumer control over their data can increase competition and improve financial well-being. One third party SER explained that open finance can bring in new entrants and better products and services, particularly for underserved consumers. This SER stated that consumer-authorized data sharing enables consumers to increase savings behavior, provide insights into the lives of low-income consumers, and measure the impacts of social policies on households. This SER also stated that an open data ecosystem can create a more competitive marketplace, but that equity must be a priority.

Some SERs, including data providers and third parties, also believed that consumer-authorized data sharing enables the development of new products and services, including those that can better serve low-income and other underserved consumers. One third party SER stated that data sharing helps consumers manage complex financial decisions, particularly when consumers have multiple accounts at multiple institutions and if they have disparate income and expense streams. Another third party SER stated that underwriting based on consumer-authorized data can expand access to credit for underserved consumers and is more accurate and timely than credit bureau data.

Third party SERs believed, however, that the state of the market with respect to consumer-authorized data sharing presents barriers for consumers and fintechs alike. One third party SER stated that consumer data access is becoming foundational for access to credit, but its potential depends on the reliability of that access. This SER further stated that industry has done what it can to implement consumers' right to data access, but that progress has been inconsistent.

Two third party SERs also stated that consumers should be placed at the center of the financial data ecosystem. One third party SER stated that the current state of the industry creates risks that could be overcome by an orientation toward financial inclusion and financial health. Another third party SER stated that data rights confer property rights, and the rule should respect consumers' fundamental property rights, including by letting consumers share their property however they choose.

One third party SER stated that robust consumer protections are critical. This SER also stated that all consumers deserve access rights, and low-to-moderate income consumers, in particular, deserve robust consumer protections against unlawful discrimination and unfair, deceptive, and abusive acts or practices generally. In addition, this SER stated that the promise of data access is matched by the risks, so the CFPB must issue strong protections while ensuring high-quality data access. Furthermore, several SERs, including data providers and third parties, stated that data

access should not further entrench a two-tiered financial system that fails to adequately serve low-income consumers or minority communities.

Many SERs also stated that the CFPB must ensure that its rule does not unintentionally undermine its stated goal of increasing competition. Several SERs, including data providers and one third party, stated that requiring covered data providers to adopt a third-party access portal could be burdensome for small providers, potentially forcing consumers to move to larger financial institutions, thereby reducing competition. One such data provider SER stated that small entities will be disproportionately affected and may even cease doing business when faced with this burden. Other data provider SERs added that the CFPB's goals cannot be achieved unless the CFPB accounts for the potential impact on small institutions, and that the CFPB must not create a free rider problem.

Several SERs, including data providers and one third party, stated that fractured data privacy laws in the United States create complications. One data provider SER suggested that the CFPB request that Congress pass a data privacy law to simplify implementation.

8.2 SER feedback related to coverage of financial institutions, card issuers, asset accounts, and credit card accounts

General feedback. One data provider SER believed that proposals under consideration to cover Regulation E "financial institutions" and Regulation Z "card issuers" were well-defined. However, many third party SERs believed that coverage should be broader. Several third party SERs stated that the coverage proposals under consideration would limit the ability of data recipients to develop products for underserved and thin-file consumers and the ability of consumer to demonstrate creditworthiness, or that the proposals generally would reduce financial inclusion by not supporting products or services that rely on access to a broader picture of consumers' financial lives (*e.g.*, debt management and cash-flow underwriting). One of these SERs added that if the CFPB does not expand the scope, it should clarify that the rule's coverage is not exhaustive or otherwise would be intended to limit the applicability of section 1033, and that a regulation issued pursuant to section 1033 is not necessary for enforcement of the statutory requirement. This SER further stated that the CFPB should explicitly reserve its rights to expand the rule's coverage in the future. Two third party SERs stated that consumers should be able to access their data regardless of where they bank, including all accounts owned by any covered provider, and that covering a broader set of data will ensure that millions of Americans have the highest level of protections, insights, access, and ultimately, choice, over their data and financial lives. One third party SER added that expanding coverage would benefit small business owners, who increasingly rely on third party services to manage their business finances.

Specific suggestions. A few third party SERs had specific suggestions for covering a wider range of covered persons, as that term is defined in the Dodd-Frank Act, including providers of mortgages, student loans, car loans, personal loans, or certain closed-loop prepaid card issuers. Several third party SERs suggested expanding coverage to include government benefit accounts, such as Electronic Benefit Transfer (EBT) accounts used to distribute needs-based government benefits, including benefits under the Supplemental Nutrition Assistance Program (SNAP). One third party SER argued that failure to include public benefits would prevent users of such benefits from taking advantage of modern financial products and services to manage their

financial lives, including the potential advantages afforded by cash-flow underwriting. Another third party SER stated that, at present, the marketplace for consumers who access public benefits is defined by limited competition, poor service, and vendors that experience little-to-no pressure to improve their offerings.

Several third party SERs suggested covering payroll providers. One third party SER explained that covering payroll providers would reduce costs to consumers seeking access to their payroll data, which is currently expensive to access. Two third party SERs suggested covering providers of non-standard income data, and another third party SER suggested covering providers of billing data. One third party SER stated that failure to include mortgage servicing would prevent the future development of consumer products or services that use information from a consumer's current mortgage to evaluate available refinance or purchase options. One third party SER suggested that the CFPB clarify whether investment firms would be covered, and another third party SER asked about coverage of non-bank account providers.

8.3 SER feedback related to potential exemptions for certain covered data providers

Support for exemptions. Many SERs, including data providers and third parties, generally supported potential exemptions or other flexibilities for smaller data providers. Several data provider SERs stated that small entities face disproportionately greater burden than larger entities because of challenges related to managing costs, and that without exemptions, costs would be passed on to consumers. A few SERs stated that a requirement to establish and maintain a third-party access portal would be costly for small entities, in particular for credit unions and community banks. Several data provider SERs discussed the challenges of having multiple core service providers and other information technology systems that store consumer data, as discussed in section 8.5 below. One data provider SER stated that a small entity exemption would be needed to promote competition by small entities that also support financial inclusion goals, and that small data providers that are exempt from the rule would still have market incentives to provide access to third parties. Another data provider SER stated that, without a small entity exemption, smaller entities serving minority populations could be left behind, resulting in an uneven playing field.

Opposition to exemptions. In contrast, several third party SERs generally opposed potential exemptions. A few stated that an exemption would create unfair competitive dynamics and would disadvantage consumers based on where they have account relationships. One third party SER stated that covering small institutions would incentivize the market to build necessary technologies to support consumer data access and would be necessary to ensure both competition among financial institutions and the long-term survival of smaller banks and credit unions. This SER added that Congress had already determined that offering consumers fulsome and reliable electronic access to financial data should be a requirement of entities that seek to provide consumer products and services in this country. A few third party SERs and one data provider SER stated that the CFPB should first consider how to reduce costs for small entities complying with the rule, such as by providing flexibility or establishing clear data-sharing standards.

Thresholds for exemptions. Several SERs provided feedback the threshold for a potential exemption. One data provider SER stated that the CFPB should consider an exemption threshold

for complying with a third-party access portal requirement, such as the $10 billion asset threshold for direct supervision of the CFPB or the $750 million asset threshold of the SBA. Another data provider SER also suggested that the CFPB consider using its $10 billion asset threshold for direct supervision, but suggested it might not be an appropriate threshold. This SER also suggested utilizing the number of accounts along with the asset size of a covered entity. Another data provider SER suggested that the CFPB consider an exemption based on the size of an entity's credit card program, such as fewer than 5,000 or 10,000 active accounts. A couple of data provider SERs suggested basing an exemption on whether an entity was a community development financial institution (CDFI) because they use the CDFI Fund specifically to promote the goal of financial inclusion.

8.4 SER feedback related to recipients of information

Third party authorization procedures in general. One third party SER stated that the CFPB's proposals under consideration related to third party authorization procedures were reasonable and that clear guidelines on authorization would be welcomed. Other third party SERs raised questions about the mechanics of the authorization procedures. One suggested that the CFPB consider whether third parties would need to provide an authorization disclosure whenever they need information to provide a product or service that differs from what a consumer might have originally sought from the third party. A few third party SERs stated that the rule should clarify which third party would be responsible for providing the authorization disclosure and obtaining the consumer's consent. A few third party and data provider SERs stated that the data recipient should be responsible for those steps. One third party SER pointed out that data recipients that rely on data aggregators have little control over the authorization process a data aggregator uses when obtaining consent. Another third party SER stated that it would be burdensome for the consumer to go through the same authorization procedures for multiple parties.

Two data provider SERs provided feedback on authorization procedures where a covered account is held by more than one consumer. One stated that joint holders of an account should not be permitted to authorize the sharing of another's information, as doing so could result in substantial harm to the account holder who has not consented. The other SER stated that CFPB precedent and current financial institution practices require that only one consumer authorize action on a joint account. This SER further stated that restricting the ability for joint account holders to individually authorize data sharing would unduly burden applicants relying on spousal or household income, presenting significant barriers to consumers' ability to access credit and potentially posing fair lending concerns.

Authorization disclosure content. Several SERs commented on the content of the authorization disclosure. In general, one third party SER stated that the proposal under consideration to require the disclosure of key scope and use terms seemed reasonable. A few data provider SERs and a third party SER stated that the terms should be specific and detailed, so consumers know exactly what information they are authorizing a third party to access. Regarding key scope terms, one data provider SER stated that the authorization disclosure should clearly and conspicuously describe the identity of the data provider, the terms related to frequency and duration of access, and the information to be accessed. Regarding the key use terms, a few data provider SERs stated that the consumer should be made aware of any identities the third party

may utilize, including "doing business as" or other assumed names, both when the authorization takes place and if this information changes. One data provider SER stated that the authorization disclosure should identify any additional downstream parties, including any affiliates with whom the data recipient may share the consumer's information. In contrast, one third party SER stated that disclosing downstream parties could be challenging because the data recipient may not know their identity ahead of time. One data provider SER said the authorization disclosure should describe what the third party can and cannot do with the consumer's information. A few data provider SERs stated that the authorization disclosure should provide clear and convenient procedures for revocation of authorization. One data provider SER suggested that the authorization disclosure contain contact information for responding to consumer inquiries.

Authorization disclosure format. Several third party and data provider SERs stated that the authorization disclosure should be clear, specific, user-friendly, and in plain language to ensure actual consumer consent. Some data provider SERs suggested that the CFPB consider developing a model form for the authorization disclosure that clearly identifies the relevant elements of the disclosure to ensure that third parties comply. One third party SER stated that displaying the authorization disclosure along with the data provider's terms and conditions would provide a better user experience.

Certification statement. One data provider SER stated that the third party should certify to the consumer that it will abide by certain obligations regarding the use, collection, and retention of the consumer's information, including the GLBA, the record retention requirements in Regulation B and ECOA, Regulation E and EFTA, and Regulation Z and TILA, the FCRA, and other consumer protection regulations.

8.5 SER feedback related to data types covered under Section 1033(a)

General feedback. In general, SERs believed that the six categories of information described in the Outline that a covered data provider would be required to make available were either too narrow or too broad. Most data provider SERs believed that the proposals under consideration were too broad. They stated that requiring covered data providers to make available a broad scope of information would be expensive for small entities because information is stored on in-house systems and multiple vendor systems (*e.g.*, core service provider systems) that charge for data access. Some data provider SERs estimated that they might rely on three to eight different information technology systems. A few other data provider SERs explained that information might also be displayed on different types of online financial account management portals (*e.g.*, mobile and online banking platforms) that might require separate third-party access portals. They further explained that information-retrieval costs would depend on which financial account management platforms are used, whether the data for those platforms are maintained by a vendor, and how much the vendor charges to retrieve the data. A few third party SERs believed the six categories of information described in the Outline were too narrow. They stated that covered data providers should be required to make available all covered information in their control or possession because a wide range of information would support a broad array of beneficial use cases and promote financial inclusion and competition.

Feedback on specific categories of information. Many of the data provider SERs who thought the proposals under consideration were too broad believed the CFPB should consider requiring

covered data providers to make available only the information in the first category (periodic statement information for settled transactions and deposits). Several of the data provider SERs stated that they already make this information available on their financial account management platforms (online and mobile), and that the information in the other categories is not generally readily available. They also explained that the benefits of making it available are unclear. However, one data provider SER stated that it does make available the second category of information (prior transactions and deposits that have not yet settled). One data provider SER stated that the transaction data elements currently on the periodic statement should be sufficient for data recipients' purposes.

Several SERs, including data providers and third parties, stated that providing some of the data elements included in the other categories of information could raise privacy, fraud, or discrimination risks, or compliance risks with respect to other laws. For example, regarding the third category of information (other data about prior transactions not typically shown on periodic statements or portals), one data provider SER stated that the data elements proposed would infringe on other consumers' privacy rights relating to consumers seeking to exercise their rights in cases of erroneous or fraudulent transactions. This SER also stated that its organization is limited by rules governing payee/payor information, such as Nacha or card network rules. With respect to the fourth category of information (online banking transactions that the consumer has set up but that have not yet occurred), this SER stated that information about payees could raise privacy or compliance risks with respect to other laws, such as the Health Insurance Portability and Accountability Act of 1996.

Regarding the fifth category of information (account identify information), several SERs, including data providers and third parties, stated that the proposal under consideration may be at odds with other regulatory requirements and creates privacy risks for consumers and reputational risks for both data providers and data recipients. For example, a few data provider SERs pointed out that Regulation B precludes them from obtaining and retaining certain information, such as age, gender, race, ethnicity, as that information may relate to protected classes. These SERs also stated that other laws, such as ECOA/Regulation B, HMDA/Regulation C, and TILA/Regulation Z, limit the collection, use, and retention of demographic information. One data provider SER stated that consumers can provide this information to data recipients directly.

On the other hand, some third party SERs had different views about whether the CFPB should require the availability of information in the fifth category. One third party SER stated that de-identified demographic data could be important for fair lending self-testing. Another third party SER stated that identity information could be important to reduce fraud risk (*e.g.*, if a non-account-holding individual tries to use the account-holder's identity to obtain another product or service). Another third party SER stated that permissioned identification information is used today for identity and account verification and for identifying and reporting suspicious activity.

For the sixth category of information (other categories of data and specific data elements), one data provider SER questioned whether this category fell within the scope of section 1033(a). Several data provider SERs stated that sharing consumer reports may risk financial institutions violating FCRA or at least raise compliance questions. They also stated that credit bureaus restrict the use of consumer reports or impose additional charges with regard to providing the information to the consumer.

Suggestions for reducing burden. Several SERs offered suggestions that may reduce burden on small entities. One data provider SER suggested that the CFPB provide clarity on the types of information under consideration. The SER explained that this would help determine the costs and time associated with implementation, including a clear accounting of the data elements within the periodic statement information category that are consistent with existing regulatory requirements (*e.g.*, Regulations DD, E, and Z). This SER also stated that, if the CFPB requires the third category of information (other data about prior transactions not typically shown on periodic statements or portals), it should significantly limit the scope. Another data provider SER suggested that, if the CFPB requires that all six categories of information be made available, the CFPB should consider a "phase-in" approach for implementation, as substantial work with core service providers and other vendors would be required to incorporate certain data elements for direct and third-party access. One third party SER stated that the CFPB should establish normalization standards to make data interpretation by authorized third parties easier and to reduce development costs for data providers. This SER also suggested referring to Nacha, as it has been instrumental in creating common ACH standards for financial institutions and also suggested making metadata (such as merchant location) available for broader use by third parties.

8.6 SER feedback related to Section 1033(b)—statutory exceptions to making data available

Regarding the statutory exceptions to making data available under section 1033, one third party SER stated that none of the data elements described in the Outline should fall within the exceptions because the more information that can be made available to third parties, the more they can make use of that information for consumer-facing products. With respect to the exception about confidential commercial information in section 1033(b)(1), one data provider SER suggested that the CFPB interpret the exception to apply to contracts to prevent reverse engineering of models and algorithms. Regarding the statutory exception about information that cannot be retrieved in the ordinary course of business in section 1033(b)(1), one data provider SER suggested that the CFPB interpret the exception to apply to information held in vendor systems, information that requires manual extraction, and information that cannot be extracted.

8.7 SER feedback related to Section 1033(c)—no duty to retain records

A few third party and data provider SERs generally supported making information available going as far back in time as the covered data provider makes historical information available to consumers in an online financial account management portal. Two third party SERs stated that historical information would maximize the variety of use cases, including use cases for low-income borrowers.

In contrast, several third party and data provider SERs opposed limiting historical information to what is available on an online financial account management portal and instead suggested that the CFPB establish a set timeframe. Two third party SERs stated that the time periods of historical information provided today are inconsistent and range from three to 24 months. One of these third party SERs explained that, without a more comprehensive backfill of information that is defined by technical—rather than business—considerations, consumers will continue to

receive reduced benefits from data access, such as fewer product features. One third party SER stated that historical information should include any information in the "control or possession" of the covered data provider, which typically covers more than 24 months of data. This SER also pointed out that data providers covered by the Bank Secrecy Act retain a minimum of five years of consumer deposit data. Another third party SER stated that a longer period would help consumers who have been impacted by external events, like the COVID-19 pandemic, that affect account histories. Two third party SERs stated that two to three years should cover most use cases. One third party SER suggested a period of at least seven years based on underwriting practices, which would create a level playing field between consumer reporting agency (CRA) and non-CRA data. This SER explained that, to realize the full potential of cash-flow underwriting, historical information parity with CRA data is necessary.

Several data provider SERs expressed concern about long timeframes for historical information. One data provider SER stated that ten years of history would put undue stress on credit unions and small community banks because they would need to buy additional storage and archiving tools to house that much history. Another data provider SER mentioned that increased storage requirements would increase the possibility and severity of a data breach. A couple of data provider SERs mentioned that legacy platforms can make provision of historical information challenging. Another data provider SER stated that many data providers do not have information available going back two to three years.

8.8 SER feedback related to how and when information must be made available to consumers

One third party SER believed that the proposals under consideration for information to be available on an online financial account management portal was consistent with platforms developed by many data providers. However, a data provider SER recommended that the CFPB clarify whether its proposals would apply to mobile or non-mobile financial account management platforms. One third party SER indicated that, at least with respect to its online financial account management portal, consumer access to information is tied to the consumer's participation in credit reporting.

8.9 SER feedback related to how and when information must be made available to third parties

Third-party access generally. Feedback from SERs highlighted several types of impacts that data providers and third parties would face from a third-party access portal requirement. As described above, SERs explained that small data providers, or the financial institutions they partner with, often rely on multiple third parties to store consumer information. They believed reliance on vendors generally would make implementing a third-party access portal relatively more costly for them than for larger data providers with more integrated information technology systems. For example, SERs explained data providers would incur fees to access and make information available to third parties. Two data provider SERs also explained that core service providers might impose restrictions on the types of third parties that can access information and have their own technical standards for information sharing.

SERs also highlighted potential costs to third parties. Two third party SERs explained that third parties will incur costs to integrate into a third-party access portal. One of these SERs explained that a small number of large data aggregators have integrations with large banks and some smaller banks, and that these aggregators might not wish to integrate with small data recipients. Two SERs explained that if access to small data providers (facilitated through data aggregators) cost more than for larger data providers, data recipients would be less able to serve consumers with information held at small data providers.

Data portal requirements generally. Overall, at least one third party and several data provider SERs believed that developing a consistent set of standards for third-party sharing would reduce costs for small data providers and third parties and promote competition by reducing integration costs across the market. For example, one data provider SER explained that a single set of standards would reduce fragmentation caused by multiple portal standards developed separately by core service providers.

SERs, including data providers and third parties, offered different suggestions for how standards could factor into the CFPB's third party data sharing rules. One data provider SER believed that the CFPB should establish a safe harbor for compliance for data providers operating under existing industry standards. Another data provider SER stated the CFPB should develop a single set of standards that are consistent with industry standards. Another data provider SER recommended that the CFPB, rather than data providers, establish a third-party access portal that would be mandatory for the market and that could be maintained either by the CFPB or data providers.

Types of data portal requirements. In providing feedback on the third-party access portal under consideration, a few SERs, including data providers and one third party, identified types of standards that would benefit from consistency: account connectivity and reliability of data access, data format and transmission, data security (including authentication for those accessing the data), and consumer disclosures. Feedback related to third party obligations under consideration, including obligations related to data security and consumer disclosures are described further below.

With respect to account connectivity and reliability, one third party SER explained that standards should address problems arising from data providers that terminate, disrupt, slow, or otherwise inhibit data access, which can create high rates of disconnection with a third party product or service.

With respect to information format and transmission, one data provider SER explained that standards should address descriptions of data types to be made available, the length of data fields, whether information provided should be provided in alpha or numeric formats, and the order in which information should be provided.

With respect to the security of a third-party access portal, several SERs, including data providers and third parties, stated that the CFPB should establish authentication standards for the portal. One data provider SER stated the CFPB should provide data providers with a list or database of verified third parties that are deemed qualified and authenticated by the CFPB, similar to what is done for Nacha third-party payments portal. The SER recommended that the rule provide a safe

harbor for data providers relying on this information to authenticate third parties. Another data provider SER recommended that the CFPB prescribe data security standards for third-party access portals, including requiring security tokens and multi-factor authentication.

Data accuracy issues. Several SERs commented on the accuracy of information transmitted through a portal. Two data provider and third party SERs stated that data providers' records are generally accurate because data providers have strong incentives to maintain accurate records (including through rigorous audits). Several data provider SERs explained, however, that data providers might only be able to identify and correct inaccurate information after it is posted to a consumer's account. Another data provider SER explained that whether information is inaccurate might be subjective. This SER explained, for example, that the name a consumer uses to apply for third party product or service might not correspond to the name appearing in a data provider's records.

Two SERs stated that omission-based inaccuracies are most often due to connectivity issues. One third party SER explained that its most frequent customer complaint is that information is missing, which often occurs because the connection to the data provider was disrupted. This SER added that sometimes the data provider may disrupt the connection on purpose, but other times connections just break. One third party SER explained that the regular reauthorization of credentials would make the correction of data more difficult.

SERs had different views on whether data providers should take special steps to ensure the accuracy of information transmitted through a portal. One third party SER recommended that if inaccurate information is shared, data providers should send corrected information to authorized third parties to ensure third parties do not make a decision based on inaccurate information. However, data provider SERs explained that rules around accuracy of information would create operational challenges for data providers, inconvenience consumers, and create additional liability risk where a data recipient makes a decision based on information later discovered to be inaccurate. One data provider SER stated that, because consumer-authorized information is query-based, most accuracy issues result from information that might not have been recently updated. This SER further stated that, if the information were "web-hook"-based (*i.e.*, in which a data provider would need to transmit data as it is updated), data accuracy problems would be solved, but it would also impose more burden on the data provider. Another data provider SER suggested that third parties should have some responsibility for reducing consumer confusion by ensuring they convey to consumers the same information held in data provider records.

Fees for portal access. Several SERs, including data providers and third parties, recognized that data providers will incur costs to establish and maintain a third-party access portal and believed that data providers would either need to charge fees to third parties or their consumers to defray those costs. One of these data provider SERs stated that passing costs on to consumers would likely cause it to discontinue its no-monthly-fee or low-fee deposit accounts. Some data provider SERs believed it would be inequitable for data providers to incur all of the costs to establish and maintain a third-party access portal in which a financial benefit accrues to third parties. One SER explained that data providers do not charge consumers in the direct access context, but that third parties almost always have to pay, either because they have to build custom connections or pay a data aggregator for the connection.

Several data provider SERs recommended that data providers be permitted to charge fees to third parties for accessing data through the third-party access portal. SERs offered different suggestions for how data providers should be permitted to charge third parties. One third party SER suggested that a data provider should be permitted to charge a data aggregator for the costs of integrating with a data provider's portal, but not be permitted to charge fees for specific transactions. Another third party SER suggested that data providers charge based on the value of the data recipient's specific use of the data so that data access remains affordable to low-revenue uses.

When a data provider would need to make information available. SERs provided feedback on the conditions that would trigger a data provider's obligation to make information available through a third-party access portal. SERs had different views about the extent to which data providers should be responsible for managing third-party authorization. A data provider and third party SER stated that the data provider should be able to verify the consumer's consent before making the information available to the third party. However, another data provider SER stated that data providers are best positioned to authenticate consumers and that their core service providers might have difficulty tracking consent and revoking access when consent is originally obtained by a third party.

SERs, including data providers and third parties, explained that data providers likely would need to implement systems, such as tokenized access systems, to manage authorizations and authentications. While some data provider SERs agreed that data providers should authenticate consumers and third parties, they expressed concern about the burden and liability risks associated with doing so for multiple third parties. These SERs recommended that the CFPB develop standards for authentication, such as those developed by Nacha or the Federal Reserve System. A third party SER also stated that standardizing authentication requirements would reduce burdens on third parties. Data provider SERs also recommended that the CFPB develop a safe harbor method of authentication for data providers. For example, one data provider SER recommended that the CFPB maintain a registry of authenticated third parties for data providers to validate a third party's authenticity.

A few data provider SERs expressed support for data providers having a role in revocation of third-party access. Third party SERs highlighted the burdens associated with consumers having to authenticate themselves with multiple entities or to re-authorize third parties when authorization ends. These SERs believed that this friction would reduce consumers' interest in completing the process to obtain a third party product or service. Some data provider SERs believed the CFPB should permit data providers to terminate a third party's access in cases of suspected fraud or other wrongdoing, or security breaches at third parties. One data provider SER also believed third parties, in addition to data providers, should be responsible for terminating access to prevent bad actors from accessing consumer data.

Screen scraping as alternative to a third-party access portal. SERs, including data providers and third parties, provided substantial feedback on credential-based screen scraping as an alternative to a third-party access portal. Several third party SERs believed that screen scraping should be permitted to continue for a limited time because it is a vital source of data in the absence of a data portal integration. One third party SER explained that approximately 80 percent of its customers bank at one of just 30 financial institutions, with the remaining

20 percent banking at one of 3,600 financial institutions, and that these customers are likely to lose access to the SER's products or services if a data portal cannot be established on the same timeline as the rest of the market.

One third party SER recommended that data recipients be permitted to access data through screen scraping from entities outside the scope of a CFPB rule but within the scope of section 1033. Third party SERs also expressed support for screen scraping to be a means of accessing data from data providers covered by the rule before a portal is established or when a portal becomes temporarily unavailable.

Although credential-based screen scraping would not require the type of implementation costs as a third-party access portal, data provider and third party SERs identified other costs. SERs, including data providers and third parties, explained that credential-based screen scraping creates significant data security, fraud, and liability risks for data providers, particularly because their online financial account management portals allow consumers to engage in transactions and move funds. Some data provider SERs expressed concern that many third parties are not subject to the same data security requirements as depository institutions. These data provider SERs also noted that screen scraping results in inaccurate or unreliable information transfers. Third party SERs explained that screen scraping creates inaccurate information, does not allow for high-quality data analysis, and does not provide the depth of information that could be available from a portal. One third party SER explained that it is harder to audit the trail of screen scraping than using a clear application programming interface. This SER stated that screen scraping should be considered a "last resort." Data provider and third party SERs also explained that screen scraping creates operational challenges due to changes to the data provider's online financial account management portal or, in the case of credential-based screen scraping, changes in the consumer's credentials. One data provider SER advised against an approach that could result in a two-tier banking system in which certain groups would use screen scraping and others could use an application programming interface (API) standard.

One data provider SER stated that the CFPB should discourage or prohibit screen scraping and harvesting credentials due to the risks associated with unauthorized access. This SER further stated that third parties are not required to comply with security frameworks, such as those developed by the payments industry, the Federal Reserve System, or other federal regulators. Another data provider SER stated that screen scraping exposes data providers to liability because of risks presented to account funds. One third party SER stated that reducing reliance on the receipt of a consumer's credentials could help reduce a data provider's liability risk.

Liability for covered data providers. Most data provider SERs expressed concern about increased liability risk for covered data providers. These SERs stated that third parties should be subject to the same regulations and remedies as data providers (*e.g.*, GLBA and EFTA/Regulation E) to safeguard the consumer's data and ensure the consumer is reimbursed when their data are lost or misused. One data provider SER stated that data providers should not be financially responsible for reimbursement of the losses to a consumer due to the failure of a data recipient's security. Other data provider SERs stated that, if third parties are not held liable, community banks will be unjustly held financially liable for losses due to the negligence of others. Another data provider SER stated that, without shielding the data provider from liability, there could be reluctance to share information.

Most data provider SERs stated that third-party access would increase liability and fraud losses for covered data providers. Three data provider SERs stated that insurance costs would increase because of liability and risks related to this access. One data provider SER stated that security breaches at third parties would create reputational risks for data providers. Other data provider SERs stated that it was unclear which party would be liable in the event of a breach.

One data provider SER stated that the requirement to make data available shifts the liability to the data providers to authenticate each third party. This SER also stated that this approach would leave financial institutions with an enormous obligation and no safe harbor in which to operate. This and several other data provider SERs further stated that credit unions would be disadvantaged due to limited resources and staff with the expertise to perform these technological functions. These SERs also expressed concerns about resources and staff limitations at small data providers.

8.10 SER feedback related to limiting the collection, use, and retention of consumer data by third parties

General approach to limits on collection, use, and retention. Third party SERs generally requested flexibility in how third parties collect, use, and retain information. Several third party SERs explained that giving third parties flexibility would enable them to develop new products and services and use information to inform research and public policy. Some third party SERs explained that the CFPB should allow consumers to manage their own information-sharing, rather than impose a general limitation standard on third parties. These SERs believed that the general limitation standard described in the Outline would be too restrictive, vague, and would not achieve the CFPB's stated goals of promoting competition and innovation. One SER stated that the general limitation standard would not readily support cash flow underwriting. This SER recommended that the CFPB generally require consumers to opt in to different use cases after a third party provides clear, user-friendly, plain-language disclosures. However, several third party SERs cautioned that requiring granular consumer consent would introduce friction into the enrollment process and would not benefit consumers or the public generally. In addition to these observations about the proposals under consideration, two SERs believed that a Federal privacy law was needed to address privacy risks effectively.

As specifically related to the use of information, two third party SERs expressed concerns with defining the limitation standard in terms of what is reasonably necessary to provide the product or service the consumer requested. These SERs believed such a definition would place too much emphasis on consumer understanding of how their data would be used and would be too limited for third parties. A data provider SER believed the CFPB should consider defining a use limitation standard in terms of what was disclosed and agreed to by the consumer, and for compliance with other laws and regulations.

Limits on collection. SERs offered a range of views with respect to whether there should be a maximum limit to duration of third-party access. One third party SER supported a maximum limit of one year for collecting consumer-authorized information, before or after the consumer could reauthorize continued access. However, other SERs offered opposing views. One third party SER explained that requiring reauthorization after a maximum duration period ends would result in loss of services. This SER offered, as an example, data indicating that approximately

thirty-two percent of consumers reauthorize access after the third party's initial authorization ended. Other third party SERs explained that limits on duration would frustrate consumer intent and that consumers should have greater control in selecting the duration of third-party access.

A wide range of SERs supported a general consumer right to revoke third-party access. One third party SER stated, however, that a requirement for data providers to inform consumers how their information was accessed, as consumer reporting agencies do in the context of consumer reporting, would be preferable to any standard related to revocation.

Several SERs, however, cautioned that revocation could impose costs on industry and consumers. One third party SER explained that third parties will face costs in implementing and tracking the data elements necessary to revoke access. A data provider SER stated that the CFPB would need to clarify how revocation would work with respect to data providers. Several SERs supported a consumer's right to revoke access through either a third party or a data provider. However, some data provider SERs believed third parties should have obligations to notify data providers that a consumer has revoked third party authorization. One of these SERs stated that the CFPB's rule should ensure that data providers would not be held responsible if a revocation request were not communicated to the data provider at all or in a timely manner.

A third party SER explained that available technological solutions—specifically, access tokens—could be adapted to set maximum limits on duration of various lengths and enable consumers to revoke access. The SER explained that access tokens can be established as specific module within online banking where consumers can see what they have permissioned, which third parties are using those accounts, and revoke access. The SER explained that smaller institutions can achieve this through software providers, intermediaries, or core service providers.

Limits on use. SERs provided feedback on how the CFPB was considering defining a use limitation standard, the options it was considering for restricting uses falling outside that standard (referred to as "secondary uses"), and how the rule should address specific uses of data. One third party SER also made a general observation that applying secondary use restrictions to data recipients and not data providers would put third party recipients at a competitive disadvantage and would disadvantage consumers.

With respect to the options the CFPB was considering for restricting secondary use, one data provider SER believed secondary uses should be prohibited. Another third party SER cautioned against an approach to prohibiting high-risk secondary uses without clearly defining high-risk uses, explaining that the European Union's standard for defining high-risk uses was ineffective because it was overly broad. Some SERs indicated that opt-in or opt-out approaches to secondary uses were preferred options. However, one SER cautioned against placing too many restrictions on consumers' ability to permission uses, such that information could not be used for needed purposes, like research. This and another SER suggested that anonymized information should be treated differently from information that directly identifies consumers. At least one SER believed the sale of information should be subject to an opt-in requirement.

SERs also offered views on how specific uses of information should be treated. Data provider SERs believed data recipients should be able to use information for product maintenance,

improvement, and development if such uses were disclosed. SERs stated that research-based use should be permitted. One data provider SER believed the sale of consumer information should be permitted if a consumer consents. Another third party SER believed it should never be permitted.

Limits on retention. SERs offered a range of views on limits on a third party's retention of consumer-authorized information. Two third party SERs generally supported limits on retention. One of these SERs supported consumers being able to request deletion of their information. The other SER supported a general limitation that would allow for data recipients to retain a year's worth of historical information for troubleshooting purposes.

Other SERs expressed caution for limits on retention. Several SERs, including data providers and third parties, explained that retention limits were generally expensive and time-consuming to implement and would impose additional costs in light of regulatory and other legal record retention requirements, the need to evaluate consumers for future eligibility of products or services, and future product development. One data provider SER explained that consumers could be confused if data providers and third parties retained information for different periods. Another third party SER was generally opposed to a retention limitation on third parties because it would favor data providers and undermine competition.

De-identified data. Several SERs provided feedback on how a CFPB rule should treat de-identified information. Third party SERs stated that de-identified and aggregated information is used for many purposes that benefit consumers, including consumer research, product development, and fraud mitigation, and that permitting the retention of de-identified information would be less burdensome for third parties than complying with a deletion request. One third party SER offered views on how the CFPB should consider defining de-identified information. This SER stated that the generally accepted definition of de-identification is information with the personally identifiable information removed. This SER also stated that de-identified information that is linkable to a consumer (which the SER described as pseudonymized) is valuable for responding to consumer disputes and product development.

Screen scraping. Several SERs provided feedback on the extent to which third parties engaged in screen scraping would be able to comply with the CFPB's proposals under consideration related to the collection and retention of information. Several SERs, including data providers and third parties, explained that it is difficult to limit the collection of information through screen scraping. One third party SER explained that it is difficult for data providers to distinguish consumers from third parties or only make information available consistent with a use case-specific collection limitation standard. For this reason, the SER explained, any collection limitation would need to be implemented by third parties. However, the SER explained that it would still be difficult for third parties to understand and process all the information being scraped and comply with a collection limitation standard.

8.11 SER feedback related to third party obligations on data security

Several data provider SERs stated that data providers ultimately would become liable for fraud and data security incidents occurring on a third party's systems, and that this risk would increase to the extent third parties were not subject to the same data security requirements as data

providers, as they believed is the case with some third parties. Several SERs, including data providers and third parties, believed third parties should be held to the same data security standards as data providers, such as the GLBA safeguards framework. A third party SER stated that any data security standards should be sufficiently detailed to enable the development of compliance programs. This and a data provider SER believed that some kind of auditing or supervision would be necessary to ensure that third parties are complying with data privacy requirements.

8.12 SER feedback related to third party obligations on data accuracy and dispute resolution

As discussed above in section 8.9, third party SERs believed many data accuracy problems involved in a third party's use of consumer-authorized information are caused by data providers' failure to share information or by latency issues caused by the manner in which a third party accesses a data provider's systems. Another third party SER noted that frequent reauthorizing of credentials would make correcting inaccuracies harder because it would interrupt the flow of information from data providers. SERs, including data providers and third parties, explained that consumers typically seek to resolve errors at the data provider rather than the third party and that third parties would not know about or be able to resolve inaccuracies, except to the extent the third party modifies the information. To address inaccuracies, one data provider SER explained that it relies on contractual agreements with third parties and audits to ensure accuracy. Another third party SER suggested that the FCRA should serve as a model for dispute resolution. Two third party SERs suggested that accuracy issues could be resolved by requiring data providers to alert third parties about inaccurate information or were required to affirmatively update the information.

8.13 SER feedback related to certain third party disclosure obligations

Several SERs supported disclosure requirements that would enable consumers to make informed decisions over the course of their relationship with a third party about the collection, use, and retention of consumer-authorized information, but had recommendations related to content and delivery requirements.[28] With respect to disclosures that remind consumers of a third party's access, including a potential revocation reminder, a third party SER believed consumers should be able to review which third parties are authorized to access their information. However, another third party SER believed it would be confusing for third parties to disclose that a data aggregator had received their information because consumers generally are not aware of data aggregators. Other SERs, including data providers and third parties, explained that, to be effective, such disclosures would need to be disclosed in a manner that ensures they are read by the consumer. One data provider SER also stated the CFPB should provide more guidance about what must be disclosed and how it must be disclosed. One third party SER believed data providers should make information available to consumers about how their information was accessed, including information about data types, authorized third parties, and access history.

[28] SER feedback related to the authorization disclosure, provided when authorization is originally sought, appears in section 8.4.

8.14 SER feedback related to record retention obligations

SERs explained that covered data providers and some third parties are already subject to record retention requirements under Federal law, State law, or industry standards. SERs raised concerns about customer confusion regarding information that data providers can revoke access to or delete, as opposed to information that institutions must preserve by law. They also raised concerns about data breaches if consumer information is stored in multiple places to comply with myriad retention requirements and urged that the rule address how to segregate consumer information for compliance purposes. Finally, data provider SERs raised concerns about the compliance burden of responding to customer requests for information if they are required to retain records while third parties are not. SERs expressed general support for basing any retention requirements in the section 1033 context on existing law and industry standards.

8.15 SER feedback related to the implementation period

SERs explained that the primary driver of the implementation period would be the time needed to develop a third-party access portal. As described above in section 8.9, SERs explained that small data providers, including credit unions and small banks, might not have the in-house technical resources to implement on their own, might have multiple systems from which information would have to be pulled, and might have to rely on core service providers to develop a portal. SERs' estimates for data providers' timelines to implement the proposals under consideration generally ranged from one and one half to three years, with one data provider SER estimating four to seven years. One data provider SER mentioned the establishment of the FedNow payment system as an example in which financial institutions have integrated with a technological system of similar complexity; the SER explained that rollout was estimated to take over three years.

SERs, including data providers and third parties, expressed specific concerns that the timeline could be stretched out by bottlenecks as data providers without portals seek out the same core service providers to develop portals and integrate them with the data providers' systems. Data provider SERs explained that there are not many core service providers, and that they will need to scale for every institution coming into compliance at the same time, which will take additional time. One data provider SER explained that data providers cannot easily switch core service providers to come into compliance, stating that core conversions can take two to three years.

Two 1data provider SERs and a third party SER also explained that the complexity and length of implementation would depend on the information covered by the rule, especially to the extent the rule covered information for which data elements are not already defined and programmed. Another data provider SER explained that only requiring account periodic statement information would significantly shorten implementation time, while requiring investment information, for example, would lengthen it. This SER explained that clarity on the dataset would be helpful because core service providers will not begin to develop solutions until a dataset is specified in the rule.

SERs explained that data recipients would also need time to integrate into data providers' portals. One third party SER explained that implementation would need to occur in stages,

starting with data providers developing a portal, integrating with aggregators, and aggregators integrating with data recipients. Several third party SERs estimated that data recipients could come into compliance in two to three months, including the time needed to transition from screen scraping to portal integration. Another third party SER estimated that developing a revocation solution could take seven to eight months, whereas another estimated that it could develop a revocation solution in two to four weeks.

8.16 SER feedback related to implementation processes and costs

Covered data providers—direct access. Data provider SERs explained that they generally had a online financial account management portal of some kind available through a website or mobile application. These SERs expressed that while information on periodic statements and transaction histories were available through such a portal, many of the other categories of data the CFPB is considering are not. As a result, they believed they would incur costs to provide those data. These SERs stated that depository data providers typically provide their online financial account portal through a core service provider. The costs of providing these portals ranged from $200,000 per year plus $2,000 to $3,000 per month for maintenance to $280,000 per year in total costs.

Covered data providers—third party access. Most data provider SERs stated that they do not currently have a third-party access portal or comparable system in place, and thus would have to build new systems, modify systems, or contract with a vendor to acquire a compliant third-party access portal.

Several SERs noted that depository data providers would likely have to rely on core service providers to help provide a portal, and that their current core service providers do not offer a third-party access portal that would satisfy the proposals under consideration. Further, they noted that switching core service providers is costly. Depending on the scale and complexity of systems being converted, the upfront costs at the new core service provider can range from $50,000 to $350,000, with additional decommissioning costs to retrieve information from the old core service provider of up to $200,000.

Data provider SERs noted that even if depository data providers did not have to switch core service providers, building a compliant portal would require building multiple internal APIs because several of the categories of information under consideration are stored on between three and eight separate information technology systems, most of which are not currently connected to their core banking system. These SERs expressed that each of these APIs could cost approximately $60,000 in upfront staffing costs and $20,000 in technology costs. The staffing costs include hiring outside contractors with database and software engineering expertise that might not be available in-house. One data provider SER that had just implemented an API to streamline its systems explained that it and its vendors invested approximately 50-60 hours preparing, 50-60 hours creating the database, 80 hours prototyping for optimization and security, and 40 hours for testing and documenting, with additional hardware and cloud hosting expenses.

In cases where the externally-facing part of the third-party access portal, such as the authorization system, is hosted by a core service provider, SERs stated that core service providers are likely to charge data providers a per-account, per-month fee for use of the portal.

SERs noted this was similar to pricing for providing online financial account management portals. One data provider SER expressed that these costs could be as high as $2 per account per month. Data provider SERs also noted that more generally, ongoing contracts with core service providers might require monthly maintenance fees of $2,000 to $5,000. One data provider SER noted that any integrations built with fintechs was likely to cost it more than $100,000. One data provider SER estimated the cost to provide data access at more than $2 or $3 a month per unit or per customer.

In discussing costs not reflected in the Outline, SERs noted that depository data providers have extensive costs related to preventing fraud and unauthorized transactions, and reimbursing consumers when such fraud occurs. One data provider SER noted that preventing fraud required three full-time employees and that they suffered approximately $85,000 in losses due to fraud in 2022. Another data provider SER noted that debit card fraud losses totaled $36,000 last year, a large total relative to their net revenues of $128,000. These SERs noted that data providers also pay premiums for insurance against catastrophic fraud losses, with plans typically covering losses in excess of $25,000 with certain restrictions. Several data provider SERs noted that if access to information is increased, these costs could increase as well.

Overall, SERs expressed that the CFPB's cost estimates for depository data providers were too low. Given the number of systems that would need to be connected to provide all information categories under consideration, one data provider SER estimated that total costs could be over $500,000, notwithstanding the existence of a consumer-facing online or mobile banking platform. This SER stated that costs could be so great that they could cause the sale or closure of rural community banks that might not have the capital to absorb the costs. One SER expressed concerns that adverse effects of high costs could worsen the divide in the financial industry and reduce numbers of institutions serving vulnerable communities. Another SER indicated that its business model would require that its customers bear unrecovered costs regardless of whether they sought to share information with a third party.

Some SERs expressed that implementation would potentially be less difficult for non-depository data providers because they do not have as many vendors and information technology systems that would need to be connected, and the implementation could be built in-house. One data provider SER expressed that an internal staff member had built an API over the course of a summer, and another data provider SER expressed that it would expect it to take eight to 12 weeks of work by internal staff to comply with the proposals under consideration.

Third parties. One SER explained that costs to integrate with a third-party access portal can be significant, and that its aggregator costs (for income verification purposes) represent its single largest budgetary line item (approximately 10 percent of monthly spend), and the largest contributor to its costs of goods sold. Third party SERs provided more feedback on the costs related to the potential obligations applicable to third parties. SERs generally expressed the view that handling information deletion requirements would be straightforward for data recipients. Several provided estimates. At the low end, one third party SER that had implemented de-identification and deletion systems stated that it took its team two to four weeks. Another third party SER estimated that building a system for information deletion would take 1,000 hours. Another third party SER explained that, as an organization of less than 50 people, complying with a single deletion request could require a month's worth of time from approximately three

data analysts, data scientists, and data engineers. Another third party SER stated that they developed a system to comply with the California Consumer Privacy Act (CCPA) in about a month with approximately three full-time employees. According to one third party SER, it is possible to buy "widgets" for revocation and deletion at reasonable cost. These estimates are based on CCPA compliance. For CCPA-compliant data recipients, the incremental burden is likely to be smaller.

Most SERs did not distinguish between costs third parties would face with respect to deletion requirements and retention limitations. However, one third party SER stated that small entities would face significant technical, legal, and compliance burdens in separating data elements collected through data aggregation into relevant buckets for retention.

Two third party SERs explained that their third-party audit program cost about $40,000 per year.

Data recipients may already provide disclosures for compliance with CCPA or the European Union General Data Protection Regulation. One third party SER stated that any modifications due to the proposed rule were unlikely to be burdensome. Another data provider SER stated that disclosures provided in-app, or wherever the consumer is using the product, might reduce burden.

Several SERs, including data providers and third parties, expressed concern about reauthorization requirements for data recipients, describing them as frustrating for consumers and potentially costly. Two of these SERs suggested in-app reauthorizations as a way to reduce this burden on data recipients.

8.17 SER feedback related to additional impacts

Data providers. Some third party SERs expressed concern that credit unions and smaller financial institutions might find it challenging to compete with larger data providers as they have more restrictive data access policies. These SERs explained that providers with internal APIs would find it easier to comply than those that rely on core service providers. They explained that it would be more feasible for smaller data providers to limit the list of required data elements to include only the data elements available in the online banking portal.

Third parties. Two third party SERs expressed that an information retention policy that limits the length of retention or requires immediate deletion would limit research and development uses by third parties, and that an exception should be made for de-identified information. One third party SER expressed that it would be unfair for third parties to face restrictions on secondary uses of consumer information if these restrictions were not imposed on data holders as well.

One third party SER expressed that restrictions on secondary uses, or data availability limitations, would harm product innovation by third parties. For example, a requirement that information be de-identified for secondary uses would "destroy" cash-flow underwriting systems, as personally identifiable information is required to link transaction data with credit bureau data. Other limitations on historic information may further affect the development of credit models and risk management strategies.

Two third party SERs suggested that periodic reauthorization requirements on third parties could lead to reduced customer retention, with one SER stating that this would "frustrate" consumers, and another stating that only approximately 0.32 percent of users prompted to reconnect to their bank account ever did so.

Three third party SERs expressed that the potential for screen scraping to be turned off "all at once" would limit data accessibility for some data fields and products offered by third parties (*e.g.*, mortgages, student loans). They hoped screen scraping could be allowed in the interim or that screen scraping limitations would have varied implementation periods.

8.18 SER feedback on the cost and availability of credit to small entities

SERs did not provide feedback on this topic.

9. Panel findings and recommendations

9.1 Findings regarding number and types of small entities affected

For the purposes of assessing the impacts of the proposals under consideration on small entities, "small entities" are defined in the RFA to include small businesses, small nonprofit organizations, and small government jurisdictions. A "small business" is defined by the SBA's Office of Size Standards for all industries in the NAICS. The CFPB has identified several categories of small entities that may be subject to the proposals under consideration. Within the financial industry, these include depository institutions (such as commercial banks, savings associations, and credit unions), credit card issuing nondepositories, sales financing companies, consumer lending companies, real estate credit companies, firms that engage in financial transactions processing, reserve, and clearinghouse activities, firms that engage in other activities related to credit intermediation, investment banking and securities dealing companies, securities brokerage companies, and commodities contracts brokerage companies. Outside of the financial industry, potentially affected small entities include software publishers, firms that provide data processing and hosting services, firms that provide payroll services, firms that provide custom computer programming services, and credit bureaus.

According to the SBA's Office of Size Standards, depository institutions are small if they have less than $850 million in assets. Nondepository firms that may be subject to the proposals under consideration have a maximum size of $47 million in receipts, but the threshold is lower for some NAICS categories as shown in Table 1.[29] Table 3 shows the number of small businesses that may be subject to the proposals under consideration based on December 2022 credit union and bank Call Report data and 2017 Economic Census data from the U.S. Census Bureau. Entity

[29] SBA regularly updates its size thresholds to account for inflation and other factors. The SBA Size Standards described here reflect the thresholds in effect at the publication date of this report. The NAICS codes listed in Table 1 reflect the industry category definitions in the SBA Size Standards effective in December 2022, which differ in some cases from the codes used in the 2017 Economic Census data, which are listed in Table 3. The 2017 Economic Census data are the most recently available data with entity counts by annual revenue. *See* Small Bus. Admin., *SBA Size Standards* (effective July 14, 2022), https://www.sba.gov/sites/default/files/2022-07/Table%20of%20Size%20Standards_Effective%20July%2014%202022_Final-508.pdf.

counts are not provided for the specific revenue amounts that the SBA uses to define small entities and are instead usually provided at multiples of five or ten million dollars. Table 3 includes the closest upper and lower estimates for each revenue limit (*e.g.*, a NAICS category with a maximum size of $47 million in receipts has both the count of entities with less than $50 million in revenue and the count of entities with less than $40 million in revenue).

Not all small entities within each included NAICS category would be subject to the proposals under consideration. The CFPB is not able to estimate with precision the share of entities that would be affected by the rule, but it anticipates that most small depository institutions would be covered data providers subject to the rule, while only a limited share of small nondepository institutions would be covered data providers, data aggregators, or data recipients subject to the rule.

Table 3: Number of small businesses that may be subject to the proposals under consideration, by NAICS industry

	Number of Entities	Percent of Entities
A. Small Depository Firms		
Commercial Banking (522110) and Savings Institutions (522120)	4,706	
< $850M (Assets)	3,566	75.8%
Credit Unions (522130)	4,861	
< $850M (Assets)	4,365	89.8%
B. Small Nondepository Firms		
Software Publishers (511210)	10,014	
< $40M (Revenue)	9,395	93.8%
< $50M (Revenue)	9,461	94.5%
Data Processing, Hosting, and Related Services (518210)	10,860	
< $40M (Revenue)	9,930	91.4%
Sales Financing (522220)	2,367	
< $40M (Revenue)	2,112	89.2%
< $50M (Revenue)	2,124	89.7%
Consumer Lending (522291)	3,037	
< $40M (Revenue)	2,905	95.7%
< $50M (Revenue)	2,915	96.0%
Real Estate Credit (522292)	3,289	
< $40M (Revenue)	2,872	87.3%
< $50M (Revenue)	2,904	88.3%
Financial Transactions Processing, Reserve, and Clearinghouse Activities (522320)	3,068	
< $40M (Revenue)	2,916	95.0%
< $50M (Revenue)	2,928	95.4%
Other Activities Related to Credit Intermediation (522390)	3,772	

< $25M (Revenue)	3,610	95.7%
< $30M (Revenue)	3,621	96.0%
Investment Banking and Securities Dealing (523110)	2,394	
< $40M (Revenue)	2,214	92.5%
< $50M (Revenue)	2,227	93.0%
Securities Brokerage (523120)	6,919	
< $40M (Revenue)	6,703	96.9%
< $50M (Revenue)	6,717	97.1%
Commodities Contracts Brokerage (523140)	856	
< $40M (Revenue)	825	96.4%
< $50M (Revenue)	829	96.8%
Payroll Services (541214)	4,328	
< $35M (Revenue)	4,111	95.0%
< $40M (Revenue)	4,116	95.1%
Custom Computer Programming Services (541511)	62,205	
< $30M (Revenue)	60,959	98.0%
< $35M (Revenue)	61,088	98.2%
Credit Bureaus (561450)	307	
< $35M (Revenue)	279	90.9%
< $75M (Revenue)	283	92.2%

9.2 Findings and recommendations regarding related Federal laws and regulations

The CFPB in its Outline identified Federal statutes and related regulations that have potentially duplicative, overlapping, or conflicting requirements with section 1033. Specifically, the CFPB identified the Electronic Fund Transfer Act (EFTA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Truth in Lending Act (TILA), the Truth in Savings Act (TISA), the Real Estate Settlement Procedures Act of 1974 (RESPA), and the CFPB's implementing regulations of those statutes.

The Panel recommends that the CFPB continue to evaluate the extent to which these and other Federal laws and regulations, including regulations issued by the prudential regulators and FinCEN, have potentially duplicative, overlapping, or conflicting requirements with section 1033, and that the CFPB continue to coordinate with the other Federal agencies responsible for relevant laws and rules.

The Panel recommends also that the CFPB consider how the rule would interact with the GLBA's privacy provisions and Regulation P, including with respect to consent and revocation procedures, and the FCRA and Regulation V.

9.3 Compliance burden and potential alternative approaches

Based on the oral and written feedback from SERs on the CFPB's proposals under consideration, as summarized in section 8 above, the Panel has the following recommendations.

9.3.1 General recommendations

The Panel recommends that the CFPB further consider how to reduce additional sources of liability and financial risk for covered data providers and consumers resulting from the rule, such as fraud and unauthorized access to a consumer's account.

The Panel also recommends that the CFPB issue implementation and guidance materials (including a small entity compliance guide as required by the RFA, as well as other materials), specifically to assist small entities in complying with the eventual rule.

9.3.2 Recommendations regarding data provider and product coverage

The Panel recommends that the CFPB continue to explore whether exemptions from the proposals under consideration would be appropriate for any data provider that would otherwise be covered. For example, the CFPB should further consider whether to create complete or partial exemptions for data providers, or whether to delay implementation for certain covered data providers for certain aspects of the rule, such as a requirement to establish a third-party access portal. The Panel also recommends that the CFPB seek comment on how to define potential exemption eligibility requirements or implementation tiers, such as by establishing a threshold based on asset size or activity level, or by exempting data providers based on entity type. The Panel also recommends that the CFPB further clarify the types of accounts that would be covered accounts under the rule.

9.3.3 Recommendations regarding authorization procedures for third parties

The Panel recommends that the CFPB consider how to design authorization procedures that minimize costs on third parties while still achieving the CFPB's objective of helping to ensure that consumers provide informed consent when authorizing third parties to access their information. The Panel also recommends that the CFPB further consider how it can reduce compliance costs for third parties in providing the authorization disclosure by further specifying the content and formatting principles of the disclosure. In addition, the Panel recommends that the CFPB consider how the third party authorization procedures interact with data providers' obligations to make information available. The Panel also recommends that the CFPB further consider how the authorization procedures would work in the context of accounts with multiple owners.

9.3.4 Recommendations regarding the types of information that would be covered

The Panel recommends that the CFPB further consider whether the rule should require covered data providers to make available all six categories of information set forth in the Outline. In considering the types of information that data providers would need to make available, the Panel recommends that the CFPB consider the SERs' feedback on costs to small data providers with respect to the following: accessing data stored with multiple vendors or under the control of other third parties; restrictions on data providers' ability to share information; and whether sharing certain information could expose data providers and data recipients to legal liability or reputational risk. With respect to the statutory exceptions to making information available, the Panel recommends that the CFPB continue to seek feedback on how to interpret these

exceptions, and further consider whether there are specific data elements that should be covered under any of these exceptions.

9.3.5 Recommendations regarding direct access (in general)

The Panel recommends that the CFPB clarify whether the online financial account management portal that the CFPB is considering with respect to direct access includes a data provider's mobile banking portal in addition to its online banking portal.

9.3.6 Recommendations regarding a third-party access portal (in general)

The Panel recommends that the CFPB evaluate options for promoting greater consistency in standards related to the "availability" of information (as defined in part III.D.2 of the Outline), the format and transmission of information made available to third parties, and data security of the portal (including authentication standards). The Panel recommends that the CFPB consider to what extent existing industry standards for data sharing should inform the CFPB's rule, as well as the potential costs to small entities associated with core service providers building and maintaining a third-party access portal. The Panel also recommends that the CFPB consider how data providers would need to defray the costs associated with developing and maintaining a third-party access portal. In addition, the Panel recommends that the CFPB consider how it can develop proposals applicable to data providers' third-party access portals that would facilitate small data recipients' ability to integrate with such portals.

9.3.7 Recommendations regarding when a data provider would have to make data available to a third party

The Panel recommends that the CFPB further clarify the circumstances under which data providers would be required to make information available to third parties. The Panel also recommends that the CFPB continue to evaluate options that would allow data providers to take reasonable steps to reduce security and fraud risks (such as authenticating the consumer themselves), while still ensuring that consumers are able to exercise their rights under the rule. The Panel also recommends that the CFPB evaluate options that would reduce additional costs on data providers and third parties in authenticating a third party or verifying a third party's authorization, such as providing data providers with a list of third parties that make available information relevant to their authentication. The Panel also recommends that the CFPB consult with other Federal agencies responsible for administering data security requirements applicable to data providers to discuss the feasibility of developing a safe harbor for authenticating third parties.

9.3.8 Recommendations regarding alternatives to a third-party access portal

The Panel recommends that the CFPB further consider whether screen scraping should be an alternative to a third-party access portal as a means of sharing data in some circumstances. The Panel recommends that the CFPB consider whether there are forms of screen scraping that would reduce impacts of third-party portal service interruptions on third parties and minimize costs to data providers and third parties while ensuring data quality and security. The Panel also recommends that the CFPB seek comment on how to reduce impacts on third parties that rely on

consumer-authorized data from data providers that would not be covered by the CFPB's rule, or that offer a mix of covered and non-covered products.

9.3.9 Recommendations regarding limits on collection of data by third parties

The Panel recommends that the CFPB consider options to limit duration and frequency of third-party collection of consumer data that do not unnecessarily restrict third parties' ability to provide products or services requested by consumers. For example, the CFPB should consider the option of limiting third-party collection to the duration and frequency necessary based on the product or service requested by consumers, options for reauthorization requirements after the expiration of any durational limitations, and options that enable consumers to revoke third-party access with third parties and data providers. The Panel recommends that the CFPB clarify the kind of revocation mechanisms third parties would be required to provide to consumers. The Panel also recommends that the CFPB continue to consider how revocation requirements could be designed to reduce impacts on third parties and data providers.

9.3.10 Recommendations regarding secondary use limits on third parties

The Panel recommends that the CFPB consider how the secondary use limitation that the CFPB is considering would apply in certain use cases and with respect to certain business activities. For example, the Panel recommends that the CFPB consider options that would permit uses of data (including de-identified or anonymized data, as discussed in the recommendation below) for product maintenance or improvement, if appropriate consumer protections can be put in place. The Panel recommends that the CFPB consider where it can give flexibility to third parties while still achieving its consumer protection objectives.

9.3.11 Recommendations regarding data retention limits on third parties

The Panel recommends that the CFPB consider how retention limits would apply with respect to certain business activities, like troubleshooting, product improvement, and product development, and that the CFPB consider existing standards, including existing legal requirements (*e.g.*, record retention requirements), when developing any proposed retention limits. The Panel recommends that the CFPB consider the impacts of retention limits on competition among data providers and third parties, and where it can give flexibility to third parties while still achieving its consumer protection objectives.

9.3.12 Recommendations regarding requirements applicable to de-identified data

The Panel recommends that the CFPB consider how the rule would apply to de-identified data and whether it would be appropriate to align the treatment of de-identified data with other statutes and regulations, such as the CFPB's Regulation P (GLBA). The Panel also recommends that the CFPB consider whether different use or retention standards should apply to de-identified data.

9.3.13 Recommendations regarding third party data security requirements

The Panel recommends that the CFPB consider options for ensuring that consistent minimum data security standards apply to third parties and data providers, and consider approaches for

ensuring compliance with security standards that minimize impacts on small entities while ensuring consumers' information is secure.

9.3.14 Recommendations regarding third party data accuracy and dispute resolution requirements

The Panel recommends that the CFPB consider ways to facilitate compliance by designing any requirements to be consistent with existing accuracy and dispute resolution requirements to the extent practicable.

9.3.15 Recommendations regarding certain third party disclosure obligations

Regarding potential disclosures that would enable consumers to decide whether to revoke third-party access, the Panel recommends that the CFPB clarify what information must be disclosed and how it must be disclosed. The Panel also recommends that the CFPB design its disclosure requirements to reduce the risk of consumer confusion when engaging with third party products and services. The Panel also recommends that the CFPB consider how to facilitate compliance with existing disclosure requirements, such as disclosures required by Regulation P of the GLBA.

9.3.16 Recommendations regarding record retention requirements

The Panel recommends that the CFPB assess options that reduce impacts on small entities by evaluating whether any record retention requirements are consistent with other existing requirements and do not create unnecessary data security risks.

9.3.17 Recommendations regarding implementation period

The Panel recommends that the CFPB seek comment on ways to facilitate implementation for small entities. The Panel also recommends that the CFPB continue to study the time needed for vendors to establish a data portal on behalf of data providers; the time needed by data providers, data aggregators, and data recipients to integrate into data portals at the scale envisioned by the proposal; and the time needed to develop other systems needed to comply, such as revocation and data retention mechanisms. The Panel recommends that the CFPB seek comment on implementation options that reduce impacts on small entities, including by staging implementation based on categories of data to be made available, entity size, or other factors.

9.3.18 Recommendations regarding impact on small entities

The Panel recommends that the CFPB incorporate feedback from SERs in its estimation of costs in the regulatory impact section of the NPRM. The Panel recommends that the CFPB consider incorporating one-time and ongoing cost estimates from SERs into the CFPB's estimation of the rule's costs and benefits in the NPRM, and to seek comment in the NPRM on its estimation of the costs of implementing the eventual rule.

APPENDIX A: SECTION 1033 OF THE DODD-FRANK ACT

12 USC 5533.

SEC. 1033. CONSUMER RIGHTS TO ACCESS INFORMATION.

(a) IN GENERAL.—Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

(b) EXCEPTIONS.—A covered person may not be required by this section to make available to the consumer—

(1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;

(2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;

(3) any information required to be kept confidential by any other provision of law; or

(4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

(c) NO DUTY TO MAINTAIN RECORDS.—Nothing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer.

(d) STANDARDIZED FORMATS FOR DATA.—The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.

(e) CONSULTATION.—The Bureau shall, when prescribing any rule under this section, consult with the Federal banking agencies and the Federal Trade Commission to ensure, to the extent appropriate, that the rules—

(1) impose substantively similar requirements on covered persons;

(2) take into account conditions under which covered persons do business both in the United States and in other countries; and

(3) do not require or promote the use of any particular technology in order to develop systems for compliance.

APPENDIX B: WRITTEN FEEDBACK SUBMITTED BY SMALL ENTITY REPRESENTATIVES

Written feedback submitted by the following SERs is attached:

- Michelle Corson, On the Road Lending
- Monica Davis, Union Square Credit Union
- Jeff Jacobson, New Market Bank
- Jim Morell, Peninsula Community Federal Credit Union
- Leigh Phillips, SaverLife
- Adam Roseman, Steady
- Jason (Gross) Rosen, Petal

SER Comments to PFDR Rulemaking Proposal

Michelle Corson
Founder/CEO – On the Road Companies

Background

We make low-cost car loans for working families so that they can avoid use of predatory lenders (such as "buy here, pay here" car lots, which often provide punitive loans on poor quality vehicles). Our lending entity is a non-depository financial institution and certified as a Community Development Finance Institution ("CDFI"). We are a small enterprise with about $35 million in assets. We are based in Dallas, Texas, but we serve ten states. Our clients are transportation-challenged, so we do not operate in a retail manner. There are no bricks & mortar locations. We do our work remotely through various technological systems.

We do not provide any individual customer information to any third parties, with the exception of credit reporting. Our borrowers are primarily credit-challenged consumers who want us to report credit to help them build their scores/files. We are required to report to funders on outcomes and impact metrics, but all information is provided on an aggregate, anonymized basis. The statements are similar to: "Our customers' credit scores increase, on average, by 157 points over the life of their loans;" "As of December 2022, our 31+ delinquency rate was 3.14%;" or "Approximately 63% of our borrowers meet the definition of LMI of being at or below 80% of median household income for their family composition and state of residence at the time of the loan."

Because of the nature of our work and how we are funded, we are required to report on information that may not be captured by traditional lenders, such as demographic or social characteristics of our borrowers, whether they are survivors of abuse, or whether they have a disability, for example. We are also required to report long-term trends. To accomplish this reporting, we use a robust, custom-built Salesforce CRM system. Developing and maintaining this system is expensive for a small organization like ours, as is the cost to collect data. Being required to invest in other technical systems or to adhere to regulations regarding the capture and retention of this data could be cost-prohibitive or burdensome for an enterprise such as ours.

Our borrowers receive financial coaching and education, as well as support in making the decision about purchasing a vehicle. We obtain their consent to gather personal financial data, such as read-only access to bank accounts/statements, credit reports, and verification of income, for example. These tools are used for underwriting, establishing a baseline for gains in economic mobility, and financial coaching.

CDFIs as a "covered person" or an "authorized third-party"

In some cases, our entity generates personal financial data, such as on-time payment history. This information is shared with authorized third parties – primarily credit bureaus – for the express purpose of helping our clients/borrowers to build credit.

We do have a customer-facing portal that our borrowers can use to access their loan information, check their balance, and make their payments. It is not difficult for us to provide information to our borrowers who request a history of their payments. However, if consumers were allowed to opt out of credit reporting, it would be difficult for us to administer. We hope to upgrade our loan servicing platform in the future. Additional reporting could be incorporated in that system, if not cost-prohibitive.

Data Aggregators

We have begun to work with loan aggregators. There are few lenders in our credit strata (average FICO score of about 510). Our character-based lending approach does not allow for instantaneous decisioning on loan applications, so it is harder for us to work with aggregators, but some have no other lenders available. While we receive applications through these aggregators and we provide a response to them, we are generally not providing any confidential data to them.

We do report to Experian, Equifax, and TransUnion on behalf of our clients in their efforts to build their credit profile.

Retention of Data

Because our investors/funders require us to report on economic mobility trends for low-income borrowers, we retain information for a longer horizon than a lender ordinarily would. Our loans are typically five years in duration and many of our borrowers come back to us for additional loans in the future. Being able to report on their improved credit scores, gains in income, and better financial-decision-making, are metrics that many of our funders want to see as they support our work. It would be problematic for us to lose data that illuminates longer-term outcomes.

Affordability for our Organization

We already have in place a customer-facing portal. To the extent that any additional regulatory requirements could be incorporated within that system, we think we could manage the costs and have no recommendations for alternatives at this time.

Credit Union

February 14, 2023

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

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

Dear Sir or Madam:

Union Square Credit Union is a $684 million, four-branch community credit union in Wichita Falls, TX serving 38,000 members and 15 North Texas/Southern Oklahoma counties. Credit unions are member-owned financial institutions. We typically offer lower loan rates and fewer fees than a traditional bank. We meet the needs of our members with a motto of "Not for Profit, Not for Charity, But for Service." On behalf of our membership, we are writing the Consumer Financial Protection Bureau regarding the proposed Consumer Access to Financial Records rule. We encourage the CFPB to require a regulatory framework for electronic access and data security for all parties to this proposed rule. We also charge the CFPB to consider the enormous expenses and unbalanced compliance responsibilities placed on financial institutions concerning the data recipients under the proposed rule.

1. **Credit Union Data**. Credit unions must comply with regulatory requirements, such as the Gramm-Leach-Bliley Act (GLBA) implemented by NCUA's Part 748, as a holder of member nonpublic information. We are required to secure the data, protect against anticipated threats or unauthorized access, and be subject to compliance examinations by a state or federal regulatory agency. The Federal Reserve describes any institution providing data processing, storage, and transmission as a financial institution, which would include a data recipient under the proposed rule. European models for open banking systems incorporate a regulatory framework known as a payment Service Directive (PSD2) for electronic payments systems that rely on application programming interfaces (APIs) to share information. This framework includes regulating payment initiative services that enable online banking and payments, regulating account information services that collect and store consumer disparate account information and provide aggregated data on their finances, and establishing strong consumer authentication-including multifactor authentication (MFA) for certain types of transactions, setting requirements on what types of MFA are acceptable, and allowing exemptions for certain types of transactions, such as recurring payments or low-value and low-risk transactions.

   Additionally, European companies are subject to the General Data Protection Regulation (GDPR) and face large fines if a breach of personal data occurs. By allowing access to the consumer's nonpublic information, the CFPB is ultimately increasing the surface area of risks to security and intrusion at each financial institution. As such, and under this proposed rule, the CFPB must ensure the GLBA regulates

1401 HOLLIDAY, WICHITA FALLS, TX 76301 | P: (940) 720-8000 | F: (940) 720-8070 | WWW.UNIONSQUARE.ORG

data aggregators and data recipients in the same manner as financial institutions. The failure to do so would potentially harm the consumers the CFPB protects.

The credit union uses various tools to detect, investigate, and report external cyber threats to our security framework. The tools currently identify over 1 billion cyber events and 11 thousand cyber threat detection alerts monthly. Each event or alert requires additional attention to determine malicious intent or false triggering. Each malicious event identified requires an incident case to assess the severity of the threat. Credit unions fight the security battle daily to ensure our members' information is secure. Data recipients and aggregators are prime targets when left to regulate their security, with our members and credit union paying the ultimate price. We invest in layers of protection and experts to ensure we stay compliant and secure from the 70 million cyber events seen daily. The CFPB must establish a regulation that subjects unaffiliated, unregulated third parties to the full scope of the GLBA upon implementing this proposed rule.

2. **Unauthorized Access and Identity Theft**. The Electonic Funds Transfer Act (EFTA) regulates the consumer's liability for unauthorized transactions. Typically, the consumer is not responsible for unauthorized transactions on their accounts when they report them to the financial institution. The financial institution reimburses the consumer for the amount of loss and pursues the unauthorized charge with the merchant or third party. The merchant and the financial institution do not share the liability equally. The credit union bears the heaviest financial burden in providing consumers with lost funds. The credit union submits a case to recover the funds; however, either the merchant refuses to grant the credit, or the amount of the charge is less than the costs to attempt recovery of the funds. The credit union takes the loss in income and possibly incurs increased premiums for any amounts filed with the insurance company. Also, any breach of nonpublic consumer information increases the risk of identity theft. The Federal Trade Commission (FTC) reported data showing more than a 70% increase in consumer losses to fraud between 2020-2021. The credit union has a dedicated team of three full-time employees to combat possible fraud. In 2022, the credit union saw potential losses of over $674,000 in fraudulent transactions, and amounts surpassed $84,000 in actual losses. These amounts are substantial losses to credit unions and their members. Suppose a data recipient is breached, and an unauthorized transaction occurs on a consumer account. The consumer is contacting and expecting the credit union to reimburse them for their losses, not the third parties. We incur losses due to our members falling victim to scams, fraud, and other factors while complying with security requirements. A third-party with no obligation to comply with a security framework derives significant benefits with minimal costs while positioning financial institutions to incur more significant losses. The CFPB must proportionally distribute the monetary burden and responsibility for losses by holding data recipients to the same regulations and remedies when consumer data is lost or misused.

3. **Disparate Costs**. The credit union recently set up an API to streamline our systems. We were able to utilize some skilled staff employed at the credit union and partner with a third party for the needed expertise. The credit union and third-party invested approximately 50-60 hours preparing, 50-60 hours creating a database with an expert in databases, 80 hours prototyping for optimization and security, and 40 hours testing and documenting, with additional hardware and cloud hosting expenses. These expenses do not include necessary maintenance and care needed after the API is deployed into a production environment. The approximate costs in personnel hours are $60,000, with another $20,000 for hosting the API. This estimate demonstrates the costs associated with one API. Our credit union is similar to other financial institutions in that we operate several systems to supply the information required in the proposed rule. Each system would need an API to aggregate the data into one system. This cost is projected to be enormous for most credit unions and community banks. The data recipient is not sharing any of these costs but gaining all the rewards. The costs rest solely on the data provider, which in this

case, is the credit union. As mentioned previously, credit unions are not-for-profit organizations focused on member service in the field of memberships they serve. This cost is crippling to our bottom line for a credit union our size.

CFPB Outline of Proposed Rule

1. *Statutes or regulations duplicate, overlap, or conflict with the proposals under consideration*. The GLBA, EFTA, Equal Opportunity Act (ECOA), Fair Lending Act, and Fair Credit Reporting Act (FCRA) potentially conflict with the proposed rule.
    a. The GLBA requires the application of standards for administrative, technical, and physical safeguards to the security and confidentiality of consumer records and information. The CFPB must require coverage and regulatory oversight of data recipients under the GLBA or similar privacy security regulation with a security framework as recipients and holders of consumer information. Additionally, the CFPB must require data recipients to inform consumers upon knowledge of a breach or suspected unauthorized access to their information.
    b. The EFTA applies to unauthorized transfers due to loss, theft, or breach of consumer information. The CFPB must hold data recipients accountable for consumer losses due to unauthorized access or use of consumer information. Financial institutions should not be financially responsible for reimbursement of the losses to a consumer due to the failure of a data recipient's security.
    c. The ECOA and Fair Lending Act prohibit discrimination in credit transactions. Regulatory agencies govern financial institutions under these Acts to protect consumers from discrimination based on specific characteristics. Under the proposed rule, data recipients will have access to personally identifiable data points, possibly provide them to downstream third parties not governed by these Acts, and potentially increase consumer harm as a result of discriminatory acts and practices.
    d. The FCRA governs the collection, assembly, limitations, and use of credit reports and the disclosure of information to third parties. Financial institutions, as furnishers and users of credit reports, are not allowed to share the report with the consumer and third parties based on contractual obligations with credit reporting agencies (CRAs). The FCRA and the requirements do not clearly define the extent of disclosing information on a credit report, and sharing a copy of the report with the data recipient could place financial institutions in breach of contract with the CRAs. Another issue is the destruction of the data. We are required to render data unrecoverable after being used for the intended purposes. One example of a contract with a CRA states the following;
        i. Prohibits installing peer-to-peer file-sharing software on systems used to access, transmit, or store CRA data.
        ii. Only allows access to credit report information for permissible purposes of the credit union in decisioning applications.
        iii. Information used that is no longer needed must be rendered unrecoverable.
        iv. Requires immediate notification for any data believed to have been compromised.
        v. The FACTA Disposal Rules require companies to implement appropriate measures to dispose of sensitive information related to credit reports that will protect against unauthorized access or use of that information.
2. *Factors disproportionately affecting small entities and exemption considerations*. Small entities such as credit unions and community banks would incur considerable expenses to establish, maintain, and ensure security on an API solution. As discussed above, <u>one</u> API could cost upwards of $80,000 to install, with

additional annual costs for maintenance and security (i.e., patches, upgrades, etc.). Most financial institutions do not have all the proposed data points in one system. The credit union has approximately five systems holding member information which would require creating an API for each system, establishing a data aggregator, and building an API for third-party access. This process is affected by the size, scope, number of users and vendors, hardware, software, and staffing necessary to complete each API. The data recipient is incurring little to no costs under this proposed rule and gaining all the advantages to increase competition with the financial institutions for consumer business. Credit unions are not-for-profit organizations restricted to their established field of membership. This restriction puts credit unions at a disadvantage compared to banks with an unlimited customer market base.

Moreover, the credit union consistently reviews vendors and core providers for possible efficiency gains and improved services. The credit union would incur the costs associated with establishing API access anytime we convert to a new loan origination system, card processor, or core provider. The consequences of the added expenses for rebuilding APIs would result in less core provider competition and a less equitable market. Credit unions and small communities unable to meet the requirements in the proposed rule would become fewer in number, and big banks with deep pockets would have a clear advantage to force them out of the financial industry market. The CFPB should consider an exemption threshold for complying with this proposed rule, such as the $10 billion asset threshold for direct supervision of the CFPB or the $750 million asset threshold for the Small Business Association (SBA).

3. *Accounts held by multiple consumers*. The credit union generally applies the "disclosure to one is disclosure to all" position to satisfy joint owners on an account when permissible. However, under this proposed rule, the CFPB should require disclosure to each account owner before releasing the potential data points. The GLBA requires disclosure notices about the credit union's privacy policies and practices and the conditions under which the credit union may disclose nonpublic personal information to nonaffiliated third parties. The credit union maintains these disclosures and the opt-out options at the person level. In our opinion, one consumer should not be able to consent to a vast amount of nonpublic information on someone else's behalf. The implications of allowing joint owners to permit another owner's information could result in substantial harm to the unconsenting owner. One example is a parent-owner and child-joint account in which the child signs up for a third-party budgeting application, and the third party has access to the parent's nonpublic information without their knowledge. While the account activity information should be shared, the CFPB should permit the sharing of personal data points only when the individual consumer to which the personal data consents.

4. *Authorization procedures*. The CFPB must require data recipients to provide authorizations that clearly and conspicuously include the identity of the data recipient and data provider, the terms for frequency and duration of access, contain a clear opt-out and revocation option, describes the information to be received, identifies any additional downstream third-party who the data recipient may share the consumer's information, received by the consumer before the data provider provides access, and in a prescribed format (such as the model Privacy Policy),. We believe the CFPB must create a model template for authorizations to ensure data recipients comply. The data recipient must provide authorization and receive explicit consent from each consumer. The data provider should be able to confirm authorization before submitting the information to the data recipient. Additionally, the data provider must be allowed to revoke access in cases of suspected fraud or security breaches.

5. *Types of information available*. The CFPB is considering nonpublic information inaccessible on one financial system and overly reaching to provide to a nonaffiliated unregulated third party under the proposed rule.

    a. Account Identity Information. The consumer should be required to provide the account identity information to the third party. The consumer is requesting a relationship with the third party to access valuable information from a banking platform and should have some responsibility to provide the personal data information contained in those data points. The credit union does not collect information regarding gender, marital status, number of dependents, race, ethnicity, citizenship or immigration status, or veteran status to avoid any implications of violating the ECOA or Fair Lending Act. These data points are exceptionally personal in nature, and the consumer should be required to provide them directly to the third party if necessary. Older adults, retired military, and minority groups could be targets for scams, frauds, and lenders with less integrity or regulatory supervision, such as payday lenders. The credit union works diligently to protect our members and recover funds from these types of targeted attacks with required reporting to Adult Protective Services, law enforcement, and regulatory agencies. If granted access to these data elements, the CFPB should enforce the same reporting requirements for third parties who observe these types of illegal activity. The proposed rule should be narrowed, requiring data providers to provide only the remaining account identity data elements and items pertaining to the periodic statement and activity of the account historically stored on the online banking platform.

    b. Other Information About Prior Transactions Not Typically Shown on the Periodic Statements or Portals. The CFPB proposes access to transaction-specific data, including card networks, ATM networks, ACH networks, check-collection networks, and real-time payment networks. The credit union considers the transaction data elements currently on the periodic statement to be sufficient for the purposes of the data recipient. The data elements proposed would infringe on other consumers' privacy rights relating to consumers seeking their rights in cases of erroneous or fraudulent transactions. We strongly support all efforts to deter fraud and identify malicious actors in fraudulent situations. The consumer or account information at another institution involved in a fraudulent or erroneous transaction is typically not the initiator of the transaction and is usually also a victim of the fraud. A fraudulent actor will not identify themselves at an account level in a financial institution. They will move the money through multiple victims' accounts while stripping away layers of the funds by instructing accountholders to purchase gift cards, send wire transfers, or initiate cash applications (instant electronic transfers). The CFPB could inadvertently harm another consumer by requiring the identity and account information in an erroneous or fraudulent transaction. Furthermore, the credit union is limited by rules governing payee/payor information, such as NACHA or Mastercard Rules. The final rule should not include the payee's name and account information through these channels with unregulated third parties.

    c. Other Information. CRAs do not contractually allow the credit union to provide the credit report to the consumer. While the FCRA is not clear on what defines information on a credit report and what type of sharing with a consumer is allowed, this ambiguity could put financial institutions in a position to violate the FCRA or possibly breach the contracts with CRAs. The consumer can provide a copy of their credit report to the data recipient with the tools provided for consumer

reports, such as www.annualcreditreport.com. The CFPB should not require financial institutions to act outside the permissible use of credit reports allowed under FCRA and existing contracts.

6. *Third-party Access*.

   a. Liability. The CFPB outlines the requirements of covered data providers, including making information available to third parties when the consumer has authorized access. Data recipients are required under the proposal to provide an authorization disclosure, obtain the consumer's consent, and certify they will abide by this proposed rule considering the collection, use, storage, and retention of the consumer's information. This requirement can allow multiple third parties to request access to consumer information from all different sources and shift the liability to the data providers to authenticate each third party. This approach leaves financial institutions with an enormous obligation and no safe harbor in which to operate. Credit unions are disadvantaged due to limited resources and staff with the expertise to perform these functions. Due to credit unions' field of memberships, information technology experts are mainly unattainable and tend to drain budgets to acquire the needed staff to accommodate these authentications.

   b. Standards. The CFPB is positioned to set standards for authentication and portal access. This standard could be structured similarly to the National Automated Clearing House Association (NACHA) and the Federal Reserve third-party access portals and provide a reliable system with secure access and safe harbor from litigation and regulatory enforcement action. Additionally, the CFPB must discourage or prohibit the practice of screen scraping and harvesting credentials. The third party is not currently required to comply with security frameworks, such as NACHA, Federal Reserve, Payment Card Industry (PCI), and agency security standards similar to NCUA Part 748. Consumer credentials in clear text astronomically increase the risks of unauthorized access, creating financial risk to the consumer, and necessitating the credit union to reimburse the members under Regulation E.

   c. Security. The security of the third-party access portal is of the highest importance and could significantly impact both the credit unions and the consumers. Again, consistent with previous comments, the data recipient is not affected by the portal's security now. The credit union must ensure multifactor authentication (MFA) is used to access online, mobile, telephonic, and bill pay platforms. Each system is unique; however, each requires a set of credentials, MFAs, and possible tokens. The CFPB should prescribe minimum security standards for accessing portals, including security tokens and MFA. The more consumer nonpublic information a system contains, the more emphasis needs to be placed on securing the system, authenticating access requests, and scrutinizing compliance with security frameworks and regulations. The proposed rule and the implications of the amount of nonpublic information shared with data recipients warrant an emphasis on the need for a standardized security framework.

   d. Costs and Timeline. The credit union has incorporated one API in recent months. As discussed, the project was time-consuming and costly to create the API, with continuing expenses to ensure security and maintenance. The CFBP is vastly understating the costs associated with complying with this proposed rule. The financial industry will be required to undertake large projects to modify and replace current systems, which demand experts in the area of databases and integrations. These items are costly and time-consuming for financial institutions. The credit union will likely pass these costs to the members. The wide range of information needed to satisfy

the proposed rule and the systems designed to generally not provide third-party access would increase the difficulty of designing internal systems to comply with the envisioned data access. The credit union employs a well-known core provider for many of its operating systems. When consulting with our core provider for other projects, the timeline is typically six to eighteen months for beginning the project as they have many clients. The credit union cannot anticipate the timeline associated with it or the total costs likely to be accrued for a project with a sizeable scope as the one related to this type of data share. The CFPB should collectively work with core providers and credit unions to determine a timeline and estimated costs for building and implementing the APIs and modifying systems. Consideration should be given to the feasibility of meeting the compliance requirements and designing a secure viable option. The costs and timeline to comply with the proposed rule place a disproportionate burden on credit unions, ultimately negatively affecting members.

Credit unions are member-centric and want to continue to provide quality products and services securely to members and prospective members. We appreciate the opportunity to express our concerns and views with the CFPB on the Consumer Financial Data Rulemaking process. We hope to have provided quality feedback and are happy to answer any questions or provide additional information. Please do not hesitate to contact me at 940-720-8026 or monica.davis@unionsquare.org.

Sincerely,

Monica Davis

Monica Davis
Senior Vice President Risk Management
Union Square Credit Union

February 14, 2023

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

RE: CFPB's Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights

Dear Sir or Madam:

New Market Bank ("NMB") appreciated the opportunity to respond to the Bureau of Consumer Financial Protection's ("CFPB" or "Bureau" or "Agency") Outline of Proposals and Alternatives Under Consideration ("Outline") to implement Section 1033 of the Dodd-Frank Act ("Section 1033"). In addition to submitting this written comment, New Market Banks' Compliance Officer, Jeff Jacobson participated in the Small Business Review Panel Process (SBREFA) hosted by the CFPB.

We believe 1033 will disproportionately affect small entities, Community Banks like us due to:

- Reliance on third parties (core processors and other ancillary providers) for development and ongoing hosting of systems that retain customer data.
- The process of changing core processors is time consuming (2-3 years) and extremely expensive (excess of $250,000), so it is unlikely that a Community Bank would be able to change core processors to meet the requirements of 1033.
- Resources will likely need to be redirected from customer service roles to implement and maintain the 1033 regulation, which could have a negative impact on customer service.

The assertion that financial institutions which already have a portal such as online and/or mobile banking could simply utilize that source for 1033 information sharing is not appropriate. These systems allow customers the ability to access and transmit funds (internal transfers, external ACH and/or Wire transfers), which would cause serious consumer harm if access to those funds were granted. Therefore, a new portal would need to be created for 3rd party access to 1033 required data.

The Outline includes six categories of information the CFPB is considering requiring as covered data. The 2023.02.02 slide deck for the 1033 SBREFA panel included tables on pages 26-28, which asserted which categories "Generally provided on an online management portal". We believe the assertion that 5 of the 6 categories are currently available via an online account portal are incorrect. The 1st category "Periodic statement information for settled transactions and deposits" is currently available via our online and mobile banking platforms. Our core and/or ancillary systems may retain data associated with categories 2-4, however they are not currently available through our online or mobile banking portals. Substantial work with our core processors and other third-party vendors would be required in order to incorporate those categories into a universal portal for consumer direct or indirect access. We ask that the Bureau to consider a "Phase In" approach of the categories to expedite the process of providing what is already available.

We believe that other regulatory requirements (Regulation B) preclude us from obtaining and/or retaining some items (age, gender, race, ethnicity) in category 5 (account identity information) as they may relate to protected classes. Other regulations (Reg C-HMDA) require us to collect demographic information, but it is solely allowed to be used to meet the requirements of that regulation and data fields related to it shouldn't be housed in our core systems to ensure discrimination of protected classes doesn't occur.

It is hard to estimate the time and cost to implement due to the reliance on 3rd parties for the implementation and ongoing support of a portal. Our best estimate is it would take 4-7 years to fully implement access to all of the categories proposed at a cost in excess of $500,000, regardless if we have an existing online/mobile banking portal or not. These estimates are based on core conversion and other ancillary project implementation experience. Small community banks such as ours can't absorb these costs and would be required to share these costs with customers, either directly if allowed, or by increasing other account fees. 1033 would likely cause us to discontinue no monthly fee or low fee deposit accounts. We also believe these expenses are so great it could likely cause the sale or closure of rural community banks as they may not have the capital to absorb the costs. This could be catastrophic as they may be the only financial institution for multiple communities they serve.

The potential for substantial increases of consumer fraud is inherent whenever financial institutions are required to provide confidential financial information to other parties in the ecosystem via a 3rd party portal. We take customer privacy very seriously and are required under the Gramm-Leach-Bliley Act ("GLBA") to safeguard consumer data. We ask that the Bureau to require data recipients and data aggregators be held to GLBA or comparable requirements so they are on an even playing field with financial institutions. In order to ensure adherence to consumer data protection laws we ask the Bureau to exercise regulatory authority over data recipients and data aggregators. Without the ability to enforce data privacy laws the potential for fraud increases exponentially at the risk of grave consumer harm.

Conversations with other financial institutions included uncertainty in relation to Electronic Funds Transfer Act ("EFT") or Regulation E as it pertains to 1033. Our concerns revolve around potential consumer losses as a result of data obtained by other parties in the ecosystem, particularly data users and aggregators. Consumers and Community Banks should be protected and held harmless due to breaches or fraudulent collection of consumer data from 3rd parties. Data users and aggregators should be held to Reg E requirements like financial institutions and ultimately need to reimburse any losses instead of the financial institutions. Without such requirements Community Banks will unjustly be held financially liable for losses due the negligence of others.

In conclusion, NMB requests the CFPB to carefully consider our comments and address our concerns. We would be happy to respond to any questions you may have by contacting us at: Anita Drentlaw, adrentlaw@newmarket.bank, 952-223-2330; Jeff Jacobson, jjacobson@newmarket.bank, or 952-223-2321.

Sincerely,

/s/

Anita Drentlaw
CEO, CFO, & President

/s/

Jeff Jacobson
Vice President, Compliance Officer

Peninsula
CREDIT UNION

February 15, 2023

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

Re: Small Entity Representative (SER) Comments for the Personal Financial Data Rights Rulemaking SBREFA Panel

Dear Director Chopra,

Peninsula Community Federal Credit Union (PCFCU) is located in Shelton, Washington. PCFCU is a National Credit Union Administration (NCUA) designated Low Income Credit Union (LICU) as well as a U.S. Treasury designated Certified Development Financial Institution (CDFI). We serve a five county rural field of membership (FOM) by providing financial products and services to roughly 22,000 members who have entrusted us with approximately $280 million of their hard earned savings which are PCFCU's assets. More specifically, we have a mission that is focused on households that are living at or around a household survival budget, those that are under and unbanked. As a financial cooperative, we are committed to providing financial products and services that help our members achieve greater financial well-being.

My comments below are responding to the Outline of Proposals and Alternatives Under Consideration (Outline), dated October 27, 2022. Hopefully my comments during the panel meetings and these written thoughts are useful in crafting forthcoming proposed rule.

Overview

The overall scope of the proposals under consideration is extensive. However, consumer control over their personal data has the potential to improve the financial well-being of all Americans.

The CFPB's stated objective of this rulemaking is to intensify competition and improve the provision of financial services. This is a laudable goal and a valuable starting place, but the Bureau must ask the fundamental questions: whether competition will be fostered, existing products and services will be improved, and whether or not new products and services will be developed.

These goals cannot be achieved without community financial institutions, like PCFCU. The rulemaking must account for the financial, operational, regulatory, and tangential impacts on LICUs, CDFIs, rural

financial institutions dedicated to the journey of achieving a consumer's financial well-being. If not, the impact on those financial institutions in the market could significantly derail the aim.

Coverage of Data Providers

The universe of covered entities subject to Section 1033 is generally broad. The scope of this the definition to include Regulation E "financial institutions" and Regulation Z "card issuers" is well defined.

Potential Exemptions

The pursuit of empowering consumers to have more complete ownership and access to their personal financial data is viewed to be beneficial. The services being contemplated in the Outline are very expensive and it will be difficult to get all the data together. It will at a minimum take time and money.

The definition of the 100 "large" banks, thrifts, and credit unions as $10 billion and above was defined by the CFPB when issuing its guide to supervision in October 2011[1]. It would be appropriate for the Bureau to evaluate this line of differentiation now just over 12 years later. Utilizing the number of accounts along with asset size of a covered entity could be another useful metric to use for differentiation.

If exemptions are not considered, there is a possibility that an unequitable landscape could be created by having some covered data providers left behind-- potentially smaller entities serving minority populations.

Recipients of Information

General Third-Party Authorization

The proposals under consideration would include a requirement that, in order to access consumer information under the rule, the third party accessing the information would need to: (1) provide an authorization disclosure, (2) provide the consumers informed, express consent, and (3) certify to the consumer to abide by certain obligations. As such, data aggregators and third parties should be held responsible by the CFPB to abide by these requirements.

The existing financial services industry infrastructure, at least for smaller entities such as PCFCU, is likely not able to be repurposed for consumer-authorized financial data sharing. A new solution would need to be created for covered entities to comply with the rulemaking's requirements. Some questions that arise related to this include: How do we, as a covered party, keep track of what consent a third party has obtained? And for what data the consumer has granted permission for the third party to obtain? Currently, our core data processing platform, nor any other system PCFCU supports or maintains, does not have a way to track the authorizations contemplated in the Outline. Hence, the effort will be extremely significant for small credit unions that do not have the staff or money to build out a new third party verification system. Such a verification system would be separate from the online portal, but the third party verification system would need to interface with the portal to ensure the third party making the request was authenticated.

The CFPB should own the process of authenticating third parties as it will be the primary regulator issuing the rules. This ownership by the Bureau should provide covered data providers with a list or database of

[1] Consumer Financial Protection Bureau, *Supervision and Examination Manual* (2011).

verified third parties that are deemed qualified and authenticated by the Bureau. The National Automated Clearing House Association's (Nacha's) third-party access portal would be an excellent type of model when developing this system. Additionally, a covered data provider will be relying on other parties' consumer identity information when authenticating a third-party recipient of consumer financial data. Finally, there should be a safe harbor from agency action against covered data providers by the Bureau for their reliance on this authentication information.

Authorization Disclosure and Process for Third Parties

The CFPB should develop a standard authorization disclosure form for third parties to use when obtaining consumer access. The disclosure should make clear the scope and terms of use for the consumer data. The Outline provides some general terms including, "general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, how to revoke access, the identity of intended data recipients and data aggregators to whom the information may be disclosed properly"[2]. The scope and use terms should be much more specific than the general categories envisioned in the Outline. For instance, the consumer should know exactly what information they are authorizing the third-party to access. Also, the consumer should receive clear assurances the third party is going to be a responsible steward of their personal financial information. Furthermore, the consumer should also be made aware of any identities the third party may utilize, including "doing business as" (dba) names, both when the authorization takes place as well as if it changes in the future.

The best place for authenticating the consumer's authorization for a third party to access their personal financial data is with the covered data provider. The Outline proposes this should be handled by the third party[3]. Additionally, if a third party is granted the right to access consumer information, they should certify to the consumer that they will abide by certain obligations regarding the use, collection, and retention of the consumers' information. At the top of this list should be full adherence with the Gramm-Leach Bliley Act (GLBA) of 1999 (15 USC 6801) along with record retention requirements in Regulations B, E, and Z, the truth in lending act, the equal credit opportunity act, the electronic fund transfer act, the fair credit reporting act, and other consumer protection regulations. Finally, as any personal data is transferred to a third party, the third parties should then become fully liable for any loss or fraud related to the third party having received said data.

Having said that, having the covered data provider obtain the consumer's consent provides a better defense against bad actors because the data provider has already implemented an account verification system. The covered data provider could additionally compare the authenticity of the third party against the Bureau's data base of authorized third parties (see reference to Nacha third-party access portal above). As such, covered data providers should have the ability to block or terminate a request for access when they suspect foul play or when the consumer make the request directly of the covered data provider as an alternative to the consumer making the request of the third-party. To be clear and for the greatest ease of use for the consumer, either the covered data provider or the third party should be able to block or terminate access.

---

[2] Outline at Page 16.

[3] *Id* at 15.

Types of Information that would need to be made available

The Outline[4]describes six different categories of information. The following thoughts are offered for consideration:

1. Periodic Statement Information – Data here is already broadly provided to consumers via a digital banking system (either online banking, mobile banking, or both) where the portal either contains or brings together through the portal information for settled transaction and deposits. The CFPB should provide a clear account of the elements contained within this category that is consistent with existing regulatory requirements including Reg E, Reg DD, and Reg Z.

2. Information regarding prior transactions and deposits that have not yet settled – Generally this matches what is being provided via digital banking platforms as well. When there are transactions noted as "ending" or "not yet settled", the third party should likewise provide that same vision to the status of the transactions through the products and services provided to the consumer.

3. Other information about prior transactions not typically shown on periodic statements – Examples provided in the outline such as the bank into which a card, ACH, check or other transaction was deposited by a merchant or other payee is not always known. Likewise, the name and account number at the bank of the merchant or other payee that deposited the payment transaction is not known or available to the consumer's financial institution. The CFPB should consider excluding this category.

4. Online banking transactions that the consumer has setup but that have not yet occurred. – This category raises many challenges. For instance, scheduled, one-time, bill payments the consumer established would be known. However, consumers can also schedule for bills to be paid on a recurring basis or to pay any number of future months invoices. Neither the consumer nor the credit union will know the amount a credit card payment will be one or two months hence. This is also true if a consumer has authorized a biller to automatically deduct their payment for an on-going bases using an ACH debit. The CFPB should consider excluding this category.

5. Account identity information – First of all, account identity information is strictly confidential because of the significant risks of fraud, security breaches, privacy breaches, misuse of information and other significant consumer protection risks should this information be disclosed. Financial institutions are bound by fair lending (Reg B), truth in lending (Reg Z), and other regulations that limit their collection, use, and retention of this information, let alone the sharing of this information with third parties.

   There are also identified in the outline[5] several pieces of demographic information such as gender, marital status, number of dependents, race, ethnicity, and citizenship or immigration status that invite serious concerns regarding the use of this data by third parties. Use of this demographic data could lead to discriminatory practices or the equivalent of Reg Z violations when being used

[4] *See id* at 18-24.
[5] *Id* at 22.

by third parties. The CFPB should consider excluding this category.

6. Other information – It is not clear how this category, including examples of consumer reports, bonuses/rewards/discounts/incentives, and information about breaches, are within the language of Dodd-Frank 1033. Further, under our contracts with the credit bureaus, a copy of a report used for a decision is restricted to a single purpose or incurs additional costs with regards to providing the information to a consumer. The CFPB should consider excluding this category.

How and when information would need to be made available

Direct and Third Party Access
Definition of financial account management portal - The CFPB's proposal for Direct Access by the consumer considers doing so through online financial account management portals[6]. The Bureau should consider what types of portals would be options to meet this direct access. Online portals generally refer to the online banking platforms used by members. Consumers also have access to much of the same, but not always all, information through mobile banking channels. Comprehensively, digital banking covers these two points of access, however, both points of access may not be appropriate for this proposed use cases. Without the clarity of what is meant by a financial account management portal, the segments of data that are being contemplated, the authorization methodology, and so forth, determining costs or time associated with implementation becomes extremely if not virtually impossible to figure out.

Furthermore, online and mobile banking platforms today are not only portals consumers use to look up historical data. Consumers conduct transactions using online and mobile banking platforms to make loan payments, transfer funds between their accounts held at the financial institutions, transfer money to/from an account at our institutions from/to accounts at other financial institutions, and person-to-person payments. In short, money is moving within and outside of the consumers accounts. Hence, it really is not appropriate for the online and mobile banking platforms we use today to be utilized for the purposes contemplated within the Outline. Doing so would expose these transactional portals potentially to bad actors intending to defraud consumers, third parties, data aggregators, and the covered data providers.

Third Party Access Portals
Development Standards - For direct access, the CFPB is considering proposing that a covered data provider would be required to make information available in a machine-readable format. However, there is no definition of machine-readable format. At a minimum, there needs to be not only compliance standards developed, but the Bureau needs to put in place development standards for this access format. That is, a file format that includes such things as a description for each type of data, the order data should be provided, the length of the data fields, whether the data being provided for each field is alpha or numeric, etc. Examples that we have utilized in implementing or continue to utilize in operation are file formats for Nacha, Zelle, ATMs, digital banking, and others utilize for The Clearing House Real-Time Payments or the Federal Reserve's new FedNow. Implementing such common development standards would make implementation more efficient. If left for the industry to figure out, there are many core providers that will develop their own set of file formats and development standards that must be adhered to. A third party

[6] *Id* at 28.

would have to code to each different requirement of each different core system. There are some core processing systems which do allow for the use of APIs, and this would certainly be preferable across the board, however, many institutions core systems are not so modern.

Screen Scraping - Screen scraping is another option being considered. There are significant security concerns related to screen scraping. Multi-factor authentication (MFA) is implemented by financial institutions to add appropriate levels of security, as the consumer can conduct financial transactions. However, MFA can provide some turbulence when being used by screen scraping to gain access. It is not very precise and can have significant operational issues when consumers change passwords on a host, covered data provider's platform, but do not update with the third parties service. This method could also open up levels of disparity when some consumers may not have access to banking services being provided via an online portal.

Third Party Access Portals – Authorization - The outline provides that a covered data provider would be required to make information available to third parties once the required authorizations have been provided. It is unclear how we as a covered data provider would keep track of what consent a third party has obtained. Our core data process platform does not have a way to track that type of third party information. The Outline focuses a lot on the time, money, and effort around a data portal, but it does not seem to address all the "engines" (i.e. core data processors) that would need a lot of development in order to make any of this a reality.

Third Party Obligations

Limits on Collection

Credit Unions such as PCFCU must establish a written privacy policy and provide certain disclosures and notices to individuals when credit unions collect nonpublic information about these individuals. The credit union may not disclose nonpublic personal information about a consumer to nonaffiliated third parties unless the credit union satisfies various notice and opt-out requirements, providing the consumer has not already elected to opt out of the disclosure. The regulatory requirements have been in place since President Clinton signed into law the Gramm-Leach Bliley Act. As a result, the National Credit Union Administration (NCUA), credit unions' prudential regulator, issued Part 716 of its Rules and Regulations entitled "Privacy of Consumer Financial Information" which was effective in November 2001. The regulator guidance for federally insured credit unions can be found in NCUA Letter 01-CU-02, February 2001, and Appendix Z to Part 716 which has become 12 CFR Part 1016 or Reg P. There are also related specific privacy disclosures, processes, and forms that we provide to the consumer, our credit union members.

Significantly, the CFPB will need to articulate how any new rule related to this Outline will change, supersede, or clarify any conflicts with this existing regulatory direction.

Revocation also becomes an issue whereby a consumer may revoke their authorization under the aforementioned privacy regulations or perhaps directly to a third party. The Bureau needs to clarify how revocation will work. One solution would be for the Bureau to ensure financial institutions would not be held responsible for revocations that are provided to the third party but not communicated, or not communicated in a timely manner to the financial institution.

Limits on Use
The Bureau must strictly regulate and curtail secondary uses of consumer data disclosed to third parties to ensure usage for only those disclosed and agreed to by the consumer and for compliance with other laws and regulations relating to the provision of products and services. Any monetization or sale of consumers' personal financial data should be subject to an opt-in provision presented by the third-party to the consumer.

Limits on Retention
(See "Record Retention Obligations and Implementation Period" below)

Data Security Requirements
At a minimum, the CFPB should require third parties to comply with GLBA regulations. As a regulated and federally insured credit union, we are required to adhere to a vendor due diligence process. This due diligence requires us to review a third party vendors' data security audits (i.e. SOC 1 – SSAE 18 or SOC 2 audits). A similar due diligence requirement should be put in place for third parties and data aggregators with the Bureau having the oversight authority to ensure covered data providers that the appropriate data security standards are met by third parties.

Federal Data Privacy Standard - Further, the CFPB should request of the United State Congress, to carry out what Congress has asked in 1033, that a federal data privacy data standard be considered. As referenced in the Outline (p. 46, footnote 50), there are multiple state specific privacy laws that are emerging in California, Virginia, and Colorado. To have 50 different state privacy laws will further complicate implementation of any rule related to Personal Financial Data Rights.

Record Retention Obligations and Implementation Period

Record Retention
As a credit union and financial institution, we are required to have a Records Management Retention Policy. This policy outlines how PCFCU manages the preservation, retention and disposition of our vital records and business and operational records, including personal financial data. We are required to comply with all federal and state laws applicable to the creation, preservation, retention and destruction of our records. This Records Management Policy includes: (i) a Records Preservation Program required by NCUA Rules and Regulations (Part 749) for federally insured credit unions, (ii) Record Storage, Retention, Retrieval and Destruction Guidelines for the efficient, timely and cost effective storage and destruction of Credit Union business and operational records, (iii) a Record Retention/Destruction Schedule, and (iv) forms to evident the Credit Union's Records Management actions and compliance.

Implementation Period
The implementation period for this rulemaking should be no less than 3 years. While this may be disappointing for some, it is necessary to implement a thorough, secure, and well-functioning system. The alternative would be detrimental first and foremost to the consumer, but also to all covered data providers, third parties, and data aggregators.

There are a few reasons for why this amount of required implementation time is necessary. Neither our core processing nor digital banking platforms have an open API service. Instead, both utilize an older

proprietary interface with third parties. Therefore, our vendor will need to add this effort to its roadmap, with the financial institutions bearing the development costs, and then each third party will need to write code to interface with what our core provider provides.

Screen scraping is out of date, less secure, and fraught with more potential for breakage and failure. So it is not the best method to use as performance would be encumbered. There are third parties that use screen scraping today, however, without modifications all the categories of data being considered would not be present within our online banking portal today. Even if considered for a short term bridge to a better solution, screen scraping at best would not support the desired objectives.

Potential Impacts on Small Entities

Covered Data Providers - Costs

The costs of implementation will be significant. There will be direct costs to covered data providers, such as PCFCU, for allowing access to consumers or third parties related to system upkeep, staff allocations, and member service matters. Most of our internal systems that house consumer data were not designed to share data with outside parties at the request of a member or on a an ad hoc basis. Therefore, our institution would not be able to provide direct access without significant modifications to existing systems, which is costly. Furthermore, since there are many details contemplated by the Outline, no covered data provider or the systems we obtain from vendor partner systems provide for our use will be able to be modified or developed until a final rule is issued. The Bureau needs to provide extended timelines for implementation of this rule.

Based on past experience, the vendors used, particularly the core processing vendors, do not proportionately distribute the costs of development or significant changes to a new system when all institutions using that system are obligated to meet new regulatory requirements. Each customer of the core vendor pays relatively more than just their share of the cost; the total cost of development is not evenly divided.

If the CFPB does not contemplate the costs associated with implementation of Outline, the pursuits of the CFBPs overall objectives related to competition and product and services enhancements will create a free rider problem. That is, a situation would be created where covered data providers are sharing with third parties valuable resources at no cost to the third party. This generates little incentive to contribute to collective resources since they can enjoy its benefits even if they do not pay for it.

As a financial cooperative, credit unions share such costs across all member owners or must result in charging fees. Currently, there are no fees for accessing PCFCU's digital platforms (online or mobile banking) which includes not only the periodic statement information, but also the ability to transfer between accounts, transfer to/from accounts at other financial institutions as long as PCFCU is one of the parties to the transaction, bill payment, person-to-person payments, personal budgeting tools, and free credit score information including how to improve that score. Implementation of this rule with the costs being borne by our institution would require us to charge fees either for digital access that is free today, account fees, or negative impacts on loan or deposit rates. In other words, charging our member, the consumer, for the expense our institution would bear the responsibility for implementing and maintaining.

The CFPB should consider the ability of covered data providers to charge third parties or data aggregators for access to the data held by an entity such as our credit union. Far too much of the burden for developing, implementing, and maintaining these systems falls on the covered data provider. These burdens include:

- General reliability and response to electronic requests;
- The length of time between the submission of a call to a third party access portal and a response;
- System maintenance and development that involved both planned interruptions of data availability and response to unplanned interruptions;
- Response to notifications of errors; and
- Limitations or restrictions on fulfilling a call from an authorized third party eve when data are otherwise available.

The third parties are deriving significant benefits from the investment of time, money, and continued upkeep that covered data providers will be putting into this new system without bearing much of the cost. If the third party contributes relatively less money initially or over an on-going basis, then the covered data provider is unable to be sufficiently compensated.

Additional Impacts and Considerations
Currently, federally charted credit unions and most state credit union charters limit membership to a defined field of membership (FOM) area. This creates a market that is already not open to fair market competition because these credit unions are bound by their field of membership and cannot accept members outside of those limitations.

Credit Unions are also not-for-profit financial cooperatives. As such, the only way Credit Unions are able to increase capital is through net income. There is not the ability for credit unions to raise money by selling stock or capital contribution by private owners. Also, additional expenses, such as would be significantly required to implement this rule, would reduce net income. Net Income is utilized to enhance products and services we strive to provide to our members in order to be competitive in the marketplace.

PCFCU is charged for each user that is registered to utilize online and mobile banking. Not all of our members (consumers) want or use online banking. If a third party was requested personal data for an inactive consumer, we would need to activate that person's account for online banking access. For the protection of the personally identifiable information and data entrusted to us, we do not want to have all accounts "activated" or "available" for online access. Not to mention, it would increase PCFCU's per user operating costs by about forty-percent (40%). As more personal financial data is shared with third parties, this naturally increases the probability of fraud occurring. When fraud increases, financial institutions have obligations to reimburse the consumer for the fraud losses on their account. This is directly why there needs to be a liability shift from a financial institution to the third party should a loss result from a third party losing data due to fraud.

In addition, financial institutions carry catastrophic insurance for this type of fraud which means additional insurance premiums. Also, to provide the appropriate customer service when fraud takes place requires additional FTEs to be added to our staff.

The CFPB should also evaluate how the U.S. Treasury Community Development Financial Institutions (CDFIs), which could include both some third parties and some covered data providers (i.e. credit unions).

These are institutions that share a mission for serving unbanked and underbanked consumers in financially distressed communities. Utilization of CDFI grant dollars and other programs could possibly be leveraged for implementation of this rule. The process for applying and ultimately winning grant awards can take anywhere from 9 to 18 or more months, depending on the timetables used by the CDFI Fund. The Bureau should research how CDFIs are serving consumers, make recommendations to the U.S. Treasury for CDFI grant funding specific to this proposal, and exempt for a longer period of time CDFIs as those that apply for grant funds wait for those grant decisions to be made.

Conclusion

The opportunity to serve as a small entity representative (SER) as part of the Personal Financial Data Rights Rulemaking, Small Business Regulatory Enforcement Fairness Act (SBREFA) Panel has been very insightful.

Some context about why allowing a small entity such as Peninsula Community Federal Credit Union (PCFCU) to provide feedback as part of the rule making process can be best exemplified by a story from our financial institution. The ramifications of this rule, while striving to benefit consumers in general, could also curtail our ability to pursue our mission as a LICU and CDFI.

All PCFCU staff receive financial education certifications to be able to personally serve each individual member interaction. PCFCU also has a dedicated Community Financial Educator (CFE) who spends one-on-one time coaching community members who are having trouble keeping up with basic expenses, saving for life's unpredictable emergencies, and trying to build or repair credit.

To exemplify our community development mission, las year, PCFCU's CFE assist "Ryan" out of homelessness and into an apartment by signing him up for Credit Sense, a free online resource available through online and mobile banking that PCFCU provides to understand and improve one's credit score. After an unsuccessful apartment search, Ryan was left to live in his car. One apartment community had rejected Ryan's application and share that his score was too low at 468. By working with our CFE and using Credit Sense, Ryan was able to identify how to update his credit score and achieve a score of 649. This re-incentivized Ryan to search for another apartment, opening doors to a better way of life. Ryan was approved for an apartment and a new financial future with a roof over his head.

Collaboratively, a well thought out rule that allows a sufficient timeline for the covered data providers and, more importantly, the vendor partners we are reliant upon to make changes, is necessary to continue and not overly encumber our mission.

Sincerely,

James M. Morrell
President/CEO

SaverLife

Jan 25, 2023

Rohit Chopra, Director
Bureau of Consumer Financial Protection
1700 G Street, N.W.
Washington, DC 20552
Via Financial_Data_Rights_SBREFA@cfpb.gov

Dear Director Chopra,

Thank you for the opportunity to respond to the Consumer Financial Protection Bureau's Rulemaking on Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act and to share our perspective on this important and complex issue.

SaverLife is a nonprofit financial technology organization leveraging financial technology to solve America's savings crisis and to advocate for a fair and equitable financial system in which all people in the United States can experience financial stability and economic mobility. SaverLife is designed to help people with low-incomes to take control of their financial future and build savings habits to last a lifetime. Our 600,000 members, the majority of whom are women of color and parents, work hard yet struggle to get ahead due to insufficient and inconsistent incomes, high daily living costs, inadequate financial services, and high-cost consumer debt. As both a fintech and social justice leader, SaverLife advocates for our members and partners with fellow nonprofits, the private sector, industry experts, and policymakers to bring real-world perspectives and data-driven insights to issues of financial inequity.

Our financial system is rapidly becoming more open[1], bringing with it a revolution in financial services. Traditionally, a consumer and a bank could only share financial data with one another. An open system opens doors as consumers share their data with other financial service providers, such as fintechs, merchants, or other digital platforms. An open system can create better financial products and services for all, and particularly for the underserved.

Open data sharing allows SaverLife to provide value to the 600,000 low and moderate income households nationwide who use our services to build savings, and ultimately wealth, for themselves and their families. At the heart of these efforts lies our ability to connect directly to consumers and to understand their financial lives through the use of consumer-permissioned data. At SaverLife, we use consumer-permissioned data in three primary ways: to increase savings behavior and financial stability through a variety of interventions, to provide insights into the real financial lives of low-income consumers, and to measure the impacts of social policy

[1] Egan, J. 2021. "What Is Open Banking?" U.S. News & World Report.

interventions on household finances. With consumer consent, data can and should drive innovation in the marketplace and inform public policy decisions.

Consumers today have complicated financial lives. As a result, consumers increasingly seek out fintech and other tools to help them manage their money. More than three out of every four people (81%)[2] have linked their primary banking account to a fintech tool. Access to consumer data is the new bedrock for financial services and platforms that are greatly impacting the way consumers handle their money. For someone with multiple accounts across different financial institutions, a data sharing system opens up tremendous possibilities by allowing consumers to view and manage all of their transactions in a single interface through account aggregator applications. More than two-thirds (69%) of consumers say that it is easier to keep on top of their money, and a majority (55%) say that it is easier to stick to a budget as a result of using such services.[3]

The majority of SaverLife members are hourly-wage workers, and many work multiple jobs, earn additional income from self-employment, or make-up their household balance sheets through a blend of earned income and public support. Financial services that allow consumers to access a variety of data in a secure and robust manner provide real value: bringing disparate income and expense streams into one user experience can minimize the burdens on Americans with lower incomes to manage an increasingly complex financial picture.

It is through our experience working directly with communities of color, women, and households with low- and moderate-incomes that we see the paramount importance of personal financial data rights. A robust data sharing ecosystem, through technology, has the potential to create better financial products and services for the underserved. However, the current state of the industry creates challenges for consumers and fintech providers alike.

All consumers deserve access to and rights over their financial data. In addition, consumers with low- to-moderate incomes, in particular, deserve particularly robust consumer protections against unfair, deceptive, and abusive practices, given our country's long history of racist and legacy systems of exclusion and wealth stripping. It is why we believe the following considerations are requisite, particularly for those historically underserved by the financial mainstream to effectively manage their financial lives.

- Promising Technology. A robust data sharing ecosystem, powered by rapidly advancing technologies, has the potential to create better financial products and services that meet

[2] Mastercard. December 2021. "The Future Is Here: New Mastercard Study Finds Majority of Consumers Embrace Open Banking to Power Digital Financial Experiences," Mastercard.com.
[3] Open Banking Implementation Entity. 2021. Open Banking Impact Report. Accessed at openbanking.foleon.com/live-publications/the-open-banking-impact-report-october-2021-ug/executive-summary/.

the needs of everyone in our economy. However, the current state of the industry creates risks for consumers and fintech providers alike. If used correctly — with financial inclusion and financial health as the core values — fintech has the potential to create better financial products and services for all consumers.

- Covered Entities. Consumers should be able to access their data regardless of where they bank, including accounts owned by any covered provider. These may include checking, savings, credit cards, loans, mortgages from the same institution, and from a range of providers, including EBT, mortgage providers, small business lenders, auto lenders and more, as these collectively form the pieces of a consumer's broader financial picture. Moreover, the landscape is changing rapidly; for instance, mortgages are increasingly originating from non-financial institutions. Regulatory frameworks should expand to cover a broader set of providers that better reflect the reality and complexity of the financial lives of consumers.

- Data Access. While innovation can open new doors and more choice to consumers, it is because data is the ultimate commodity. Because the potential benefits for consumers of authorized data access are matched only by the potential risks, the Bureau must issue a strong rule to include vigorous, substantive safeguards for consumers, while ensuring equitable and reliable access to consumer data. These protections must consider issues of consent, time frame, privacy, sale of data, while ensuring consistent access to accurate and high quality data throughout the financial system.

- Equity. An open data ecosystem can open access to and foster a more competitive marketplace for innovative financial services, which can rewrite the rules for millions of those who bank in the United States. We achieve equity only when we give it priority, and consistently evaluate advances in technology with equity as the first criteria.

Promising Technology

Facilitating access to consumer data through technology can be a tremendous benefit. SaverLife is but one example of how the ability to connect directly to consumer accounts across thousands of financial institutions has changed the game for households looking to build financial security, for organizations like SaverLife to scale effectively and, most importantly, achieve meaningful, measurable and lasting impact for communities.

In particular, technology can usher rapid change. Older systems in the United States, such as credit scoring, are flawed; new technologies can address consumer pain points, particularly for consumers currently underserved by the financial system. Digital financial services are growing rapidly and increasingly reaching lower-income households. During the COVID-19 crisis, for instance, growth in digital financial services led to efficient and quick access to public benefits

and a range of government support measures, while simultaneously opening doors to greater financial inclusion. In a rapidly changing landscape, data sharing can power flexible tools to reach an ever growing need for better and faster financial services. If used correctly — with the goals of financial inclusion and financial health as the core values — it has the potential to create better financial products and services for the underserved.

The potential benefits for consumers of authorized data access, assuming strong provisions for consumer control, security, and use limitations, are significant, as consumer use of their own data could provide a better alternative and provide true competition in the marketplace.

Covered Entities

Consumers should be able to access their data regardless of where they bank, including all accounts owned by any covered provider, in keeping with the intent of the consumer. These may include checking, savings, credit cards, loans, mortgages from the same institution, and from a range of providers, including Electronic Benefits Transfer cards (EBT), mortgage providers, small business lenders, auto lenders and more, as these collectively form the pieces of a consumer's broader financial picture. Moreover, the landscape is changing rapidly; for instance, mortgages[4] are increasingly originating from non-financial institutions. Regulatory frameworks should expand to include a broader set of covered providers.

Data providers: expanded rule

Since consumers bank across a variety of financial institutions, we encourage the Bureau to expand the definition of a data provider to any entity or an authorized third party information concerning any financial product or service that the consumer obtained. This can include a variety of information related to financial products and services, such as investment, mortgage, auto loan, among other accounts. Developing clear requirements over the governance over this broader set of data will ensure that millions of Americans have the highest level of protections, insights, access, and ultimately choice, over their data and financial lives.

Public benefits providers

The Bureau should extend coverage of the proposed rule to include providers of government benefit accounts - Electronic Benefit Transfer (EBT) cards - used to distribute needs-based benefits programs. At present, the marketplace for consumers who access public benefits is defined by limited competition, poor service, and service providers who feel little to no pressure to improve their offerings. Financial services that allow consumers to access a variety of data in a secure and robust manner provide real value: bringing disparate income and expense streams into one user experience can minimize the burdens on Americans with lower incomes to manage an

[4] McCaffrey, O. "Nonbank Lenders Are Dominating the Mortgage Market." Wall Street Journal, June 22, 2021.

increasingly complex patchwork of accounts and services. For the millions of Americans whose household balance sheets form a combination of both earned income and public assistance, an effective system would allow consumers to manage all of their finances, regardless of source.

Small businesses

Small business owners increasingly rely on third party services to manage their business finances. Millions of small business owners rely on software that allows for data aggregation so they can maintain a bird's eye view of their finances, from credit cards to checking accounts to loans, in order to minimize the actual cost and opportunity cost of maintaining accurate books and records and therefore a clear understanding of the progress of their business. The uniformity in bookkeeping created by these services also impacts tax preparers and allows them to serve more customers, more efficiently. SaverLife recommends expanding the covered entities under 1033 in order to better reflect the financial complexity of small businesses.

Data Access

While innovation can open new doors and more choice to consumers, it is because their data is the ultimate commodity. Because the potential benefits for consumers of authorized data access are matched only by the potential risks, the Bureau must issue a strong rule to include vigorous, substantive safeguards for consumers. Consumer data protections must consider issues of consent, time frame, privacy, and sale of data. Ensuring consistent and high quality data access across all covered entities — via screen scraping or APIs, for instance — is also a critical consideration of this rule.

Consent

Consumers have a right to transparency over how their data will be used, over a specific time period. Even now, consumers provide consent for their financial data to be shared, thanks to strong protections under the Electronic Funds Transfer Act, Equal Credit Opportunity Act, and the Fair Credit Reporting Act, among others. Yet, most consumers are likely unaware of precisely what they are consenting to or how to view, modify, or revoke their consent.

Managing permission should be designed carefully, so as not to limit consumer choice and intent. Consumer consent mechanisms should be simple and consistent and consumer preferences should be easily adjusted to ensure that data is used for specified informed purposes and time periods. Not only will this build consumer trust, it will allow for the data rights to remain with the consumer. Consumers should also have the right to fully manage their data, including periodic reauthorization and the option to ask for elimination of their data.

Consumers must also have the right to appeal a decision in an independent forum. Identity theft, fraud, and errors at critical financial bureaus are becoming increasingly common. Over one-third

(34%)[5] of Americans found at least one error on their credit report, and fraud cases rose by 19%[6] from 2020 to 2021. Consumers should have the right and opportunity to dispute any transaction made by a third party or by their financial institution in an independent forum, composed of representatives of both consumer and financial entities.

Timeframe and frequency

The timeline of consumer data can span from the immediate (during the use of a service) to a lifetime (the entirety of a consumer's financial history). Immediacy has some benefits: it limits the consumer's exposure to risk. Yet, limiting the frequency of access will also limit consumer choice if third parties could collect consumer information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. "Reasonably necessary" is vague and doesn't necessarily center the consumer. SaverLife, for instance, rewards people for putting money in savings over a period of time. Accessing a consumer's data even while they are not actively using the product is central to the service and value that we provide, as are many financial technology innovations that are built upon principles of behavioral science designed to encourage positive financial outcomes, or those designed to prevent harm to consumers, for example, by notifying consumers of low-balances or upcoming payments or changes in credit score that might require immediate attention.

Consistency of connectivity and reliability of data access

A major issue we encounter involves the consistency of account connectivity and the reliability of data access. When financial institutions cut off, disrupt, slow down or otherwise inhibit data access this creates a poor experience for consumers who are largely unaware of the details of data sharing and how it works. These types of deliberate disruptions cause high disconnect rates - meaning that large numbers of our users experience a disruption in using SaverLife that they are often unaware of and did not authorize or request. In our case, this may mean that users were disqualified from savings supports, emergency grants or other incentives and rewards that we rely on data to facilitate. Covered entities should be required to provide access to data that is consistent and of a high-quality.

Screen scraping and APIs

There are significant issues of equity and access when it comes to supporting smaller financial institutions, such as credit unions and community banks. A robust data sharing system will foster healthy competition, which will provide the greatest quality and value to the consumer. When companies compete in an open and competitive marketplace, they innovate to lower prices and

[5] Fox, Michelle. 2021. "A Third of Americans Found Errors on Their Credit Reports. Here's How to Fix Those Mistakes." CNBC. Accessed at: https://www.cnbc.com/2021/06/11/how-to-fix-those-mistakes-on-your-credit-report.html.
[6] Akin, Jim. 2022. "Identity Theft Is on the Rise, Both in Incidents and Losses." Experian.com. Accessed at: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

improve the quality of goods and services, which ultimately gives consumers choice. Requiring financial institutions to adopt application programming interface (API) protocols as a part of a data sharing ecosystem may have significant implications. If the industry moves in that direction, and there are many good reasons (such as reliability and security) to do so, we must ensure that thousands of smaller institutions, and the millions of consumers they represent, do not get left behind. This could force consumers to choose from a small number of large banks if they want to access fintech services and innovations, which are increasingly becoming a part of the financial mainstream, and in effect reduce competition.

The cost to create and maintain direct APIs is beyond the capacity and budgets of many smaller institutions, thereby potentially excluding those consumers from advances in financial technology. For example, 80% of SaverLife members bank at one of just 30 financial institutions; the remaining 20% bank at one of 3,600 financial institutions. It is the 20% who are most likely to be excluded from financial innovation if screen scraping is not permitted. Until the ecosystem achieves a sufficient level of maturity, SaverLife recommends retaining access to screen scraping: with the right security measures, screen scraping will maximize choice for the consumer, while promoting competition in the marketplace for innovative services. In addition, we strongly encourage the CFPB to examine the role of the vendors who provide technology services to banks and credit unions - core processors - and how these companies may be affecting access to consumer permissioned data.

Similarly, data aggregators must do more to allow reliable and high quality access to consumer data held by smaller financial institutions. Large financial institutions with the money to invest in technology and who represent a larger share of the consumer market are prioritized by data aggregation companies while smaller institutions are often excluded. If driving equity and access and fueling competition are the cornerstone arguments for open access to data, then a great deal more needs to be done to make that claim a reality and not simply a talking point.

Privacy

Sensitive consumer data should only be accessed safely and securely, and data access intermediaries and recipients should be subject to robust data safeguard obligations to the same extent as the entities from which the data was obtained. This will ensure that entities that access consumer data or information should only use that data or information in a manner consistent with the consumer’s permission. A system of opt-in or opt-out of many aspects of data usage and management for Protected Personal Information is one option: by designing the system to encourage consumers to select when and where their data is used, consumers will retain the choice in the marketplace.

Sale of personal consumer data

Currently, financial institutions may sell personal consumer data to unaffiliated companies as long as consumers have been notified and given choice over the transaction. Many financial institutions have voluntarily adopted stricter information sharing policies than the law now requires. Consumers must retain the opportunity to inform and protect themselves through regulations and laws that safeguard their interests, including anonymization of identifying information, to protect privacy and security of personal financial data.

Equity

A more equitable financial system that centers the financial health of all people in America can only come about if we make it a priority and consistently evaluate advances in financial technology, products, and services against that criteria. An open data ecosystem can open access to and foster a more competitive marketplace for innovative financial services, which can rewrite the rules for millions of those historically underserved and left behind by financial systems in the United States. Ultimately, this means ensuring equity is achieved through measurable outcomes: by structuring regulations as “outcomes-based,” by defining the desired measurable outcomes and permitting institutions to achieve those outcomes in different ways.

Financial technology, and the broader tech-driven revolution in banking services, has the potential to drive greater financial inclusion and give all consumers better choices and agency when it comes to safe and affordable financial services. A data sharing ecosystem can and does deliver value to the consumer, and the possibility of financial security and mobility along with it. To minimize the risk of further entrenching a two-tiered financial system in which millions of consumers remain underserved by the financial mainstream and excluded from financial products that build financial stability and wealth, consumers’ rights to their own data must be protected.

SaverLife applauds the Bureau’s commitment to engage, in an ongoing conversation, with varied stakeholders to ensure that consumer financial markets work for consumers, responsible providers, and the economy as a whole, on section 1033(a) and beyond.

Sincerely,

Leigh Phillips
President & CEO, SaverLife

Steady

Comment of Adam Roseman, CEO of Steady On the CFPB's Outline of Proposals and Alternatives Under Consideration for Rulemaking on Personal Financial Data Rights

Introduction

Steady, a mission-driven fintech, was founded in 2017 to help low-to-moderate income workers improve their earnings potential and increase the stability of their income. Specifically, our consumer-facing smartphone application, Steady App, helps non-standard workers (i.e. contingent, 1099, gig, and self-employed) track, understand, and optimize their income.

When consumers download the Steady App, they are offered the opportunity to link their deposit account(s), through our integration with Plaid, to unlock personalized income recommendations and community-driven financial insights. Our income tracker allows workers to track their weekly and monthly earnings across all accounts, breaking down earnings by income source and over time. They can also categorize deposits into a single source and view advanced insights. In addition, the Steady App offers a marketplace with vetted financial products tailored to low-to-moderate income workers (e.g. no-fee checking accounts, discounted insurance), as well as work opportunities (e.g. rideshare earning). Our member community now includes over six million members, with 2.5 million members with linked bank accounts.

While we believe directly interfacing with our members is impactful, we also believe that there are broader and deeper ways we can serve this workforce. This need came to the fore at the onset of the pandemic, when we saw many non-standard workers initially left out of government aid packages and, when they finally did become eligible for unemployment relief through Pandemic Unemployment Assistance (PUA), many struggled to verify and report their income to qualify. We saw both of these issues as opportunities to pilot broader interventions for systems change.

Specifically, we developed two solutions, housed under the SteadyIQ brand, to meet these pandemic-era needs, creating: (1) the income passport, which helps non-standard workers verify their income for eligibility for government benefit programs; and (2) social impact automation, which allows us to distribute direct cash assistance to workers (non-standard or otherwise) in need.

SteadyIQ's income passport is a user-directed, permissioned, and tech-enabled solution that allows non-W2 earners to submit proof of income for public benefits and financial products. After logging into the SteadyIQ solution, applicants connect to the accounts where they earn income - both their deposit institutions (through our integration with Plaid) and their work platforms (through our integration with Argyle) - and SteadyIQ's solution surfaces their income transactions, checks for conflicting names/identities, and allows the user to submit a comprehensive report of their earnings directly to the relevant program (e.g. the state agency, a credit union, etc.). This solution relies on extracting insights from data on more than 1.5 billion

enriched financial transactions and over 151 billion enriched deposits, enabling us to quantify earnings, help streamline benefits administration, expand access to credit, reduce fraud, improve outcomes, and increase equity.

SteadyIQ's social impact suite is an end-to-end solution for administering social programs, from intervention to outcome. With this product suite, we help our partners automate and streamline each stage of social impact programs, including identifying cohorts, screening applicants for eligibility, distributing funds, and measuring real-time impact. For this work, participants download the Steady App, link a bank account (via Plaid) where they would like to receive funds, and then we distribute the funds through an integration with Dwolla. To date, we have completed direct transfers to over 17,000 participants across our guaranteed income and emergency cash distribution work.

All in all, we believe our work with members, governments, and financial institutions is having a significant impact on the low-to-moderate, non-traditional earners that we serve. We are honored to be given the opportunity to participate in the SBREFA Panel Meetings for Rulemaking on Personal Financial Data Rights, and we are happy to submit our written commentary below.

Steady

Coverage of Data Providers

Q5: Data Types

- Almost 40% of our member base receives SNAP benefits; as such, we advocate that EBT processors are explicitly included as covered data providers under Section 1033, and that EBT processors should be required to allow account holders to access and share access to their account information electronically with third parties. We believe this is necessary for third parties to better serve our members, who need up-to-date information about their EBT balances while making in-the-moment purchasing decisions.
- We continue to see that non-standard workers use a variety of different financial sources that are not well-served, particularly payroll data.

Q6: Exemptions

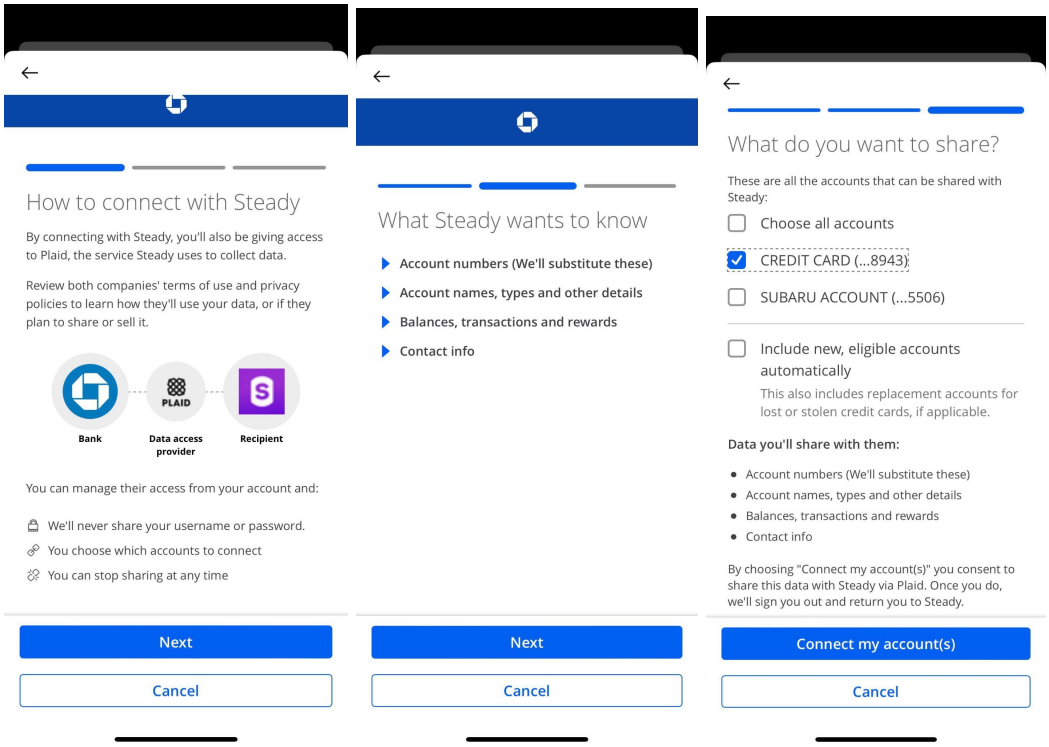
- It is critical that 1033 be as applied as broadly as possible given that it is largely smaller FIs that have not yet enabled data access. This oftentime forces data aggregators and approved third parties to use less accurate screen scraping methods to access the data (if even that is available).
- For example, in our data we see that 69% of our members connect to one of 12 popular FIs (Wells Fargo, Chime, etc.), but the remaining 31% connect to an additional 6.6k unique FIs, with no individual bank having more than 1% of our members.
- Without readily available access to data, non-standard workers can be shut out of the modern benefits system. For example, during Hurricane Ida, people who wanted DUA insurance got access to funds from the Louisiana government w/in 24 hours when they showed proof of income. Those who can't access that data are still waiting ~18 months later.

Recipients of Information

Q14, Q17: Authorization

- Any time an authorized third party leverages a data aggregator (which is what most similar-sized companies do), there is little that we can do to control the authorization consent that the user is making.
- If the CFPB wants to make it easier for users to better understand what is happening with their data, they need to make it easier for authorized third parties such as Steady to be able to communicate that to users, since currently that is extremely limiting.

- For example, these login screens are what a user sees when going through the Plaid connection experience, and are not things Steady can control, such as adjusting the lookback period, opting out of certain biographical information, and/ or limiting the timer period to the account.



Types of Information

Q30 - 37: Types of Information

- Though access should be more easily managed, we firmly believe that the more data that can be made available to authorized third parties, the more we can make use of that data for consumer-facing products, and do not believe any of the outlined data elements should be under the exception.
- Furthermore, we have seen that data aggregators (and data providers) have artificially limited the amount of data that consumers are able to access. For example, on average we only get access to 4 months of transaction data from Chime, Aspiration, and Varo, but average 15 months with Chase, Wells Fargo, and USAA.
- Without a more comprehensive backfill of data that is set by technical boundaries instead of business ones, consumers will continue to receive reduced access to benefits and product features.

- Other actions that the CFPB could take which would be helpful include…
    - Establish normalization standards to make data interpretation by authorized third parties easier, and to reduce development costs for data providers. For example, Nacha has been instrumental in creating common ACH standards for financial institutions.
    - Make explicit to authorized third parties what data was sent or not.
    - In addition to the data types already enumerated, consider making metadata (such as merchant location) available for broader use by third parties.

Data Availability

Q41, Q63: Costs

- Consumers can access the data and data providers don't charge, but third parties almost always have to pay, either because we have to build custom connections, or to pay an aggregator for it.
- These costs can be quite significant, and our aggregator costs represent our single largest budgetary line item (~10% of monthly spend), and the largest contributor to our COGS for income verification.
- If you allow data providers to charge a fee, it will be passed on to the consumer one way or the other. For one off, high revenue events, that's not a big deal. For ongoing, lower revenue events, it can be more problematic, particularly for the non-standard users who make up the core of our user base.
- Monetizing data access in general seems to go against the very idea of making the data more accessible.

Q82: Inaccurate Information

- Though every effort should be made by data providers to ensure that inaccurate information is never passed on to a third party, those situations do occur, and we must plan for it accordingly.
- If inaccurate data is transmitted, data providers must have some capability to alert and send corrected data to authorized third parties once it is adjusted.
- Without that capability, authorized third parties have no way of knowing if a poor decision was made from faulty data inputs (eg, did not meet income thresholds for benefits because earnings were overstated), directly contributing to consumer harm.
- Any rule interpretation which leads to regular reauthorization of credentials would make the correction of input data from data providers much more difficult.

Q74, Q75, Q93: Third Party Authorization

- In order to better enable consumer protections, data providers should make available to them information about how their data was accessed, similar to how a CRA already does so for credit reporting. That should include information about data types, authorized third parties, and access history.
- This capability is much preferred to any standard related to data revocation.
- Requiring users to reconnect to their accounts to authorize third party access will almost certainly lead to unnecessary friction with the consumer, and reduced likelihood of product access.
- For example at Steady, of the roughly 1.1 million users we have suggested reconnect to their bank account through multiple in-app messages and/ or emails, only 3.6k (.32%) actually ever end up reconnecting their account.

Third Party Obligations

Q90. Screen Scraping

- Screen scraping should be considered a last resort alternative to well documented, maintained, and secured APIs with agreed upon development and data standards.
- It's harder to audit the trail of screen scraping, vs. using a clear API with credentials and good logging.
- That said, given how much the industry currently relies on it though, shutting it off all at once would be really problematic to consumers.

Q139. Data Deletion

- Given that we have users in California, we have been responsive to CCPA deletion requests.
- Because we are still a relatively new startup, ensuring compliance with this request without the requisite technology and process support is quite burdensome.
- All in for a <50 person organization, it took ~3 data analysts, data scientists, and data engineers about a month to comb through every database to ensure that we complied with the most recent request.
- The scale of data deletion matters a lot, and much of the consumer protections that the CFPB is considering to be put in place could likely be achieved by just de-identifying the data that a user asks, instead of requiring a full-scale deletion.

Q121. Retention

- Depending on the firm's (e.g. Steady's) customers' (e.g. partners/programs) contractual requirements, maintaining data may be mandated.
    - Specifically, we may need to retain data for ongoing programs, e.g. annual, to be able to continue providing services, depending on lookback provisions.
    - Immediate deletion after rendering services could be problematic for later auditing purposes, and/or billing.
- A data retention policy which requires that a firm immediately delete the data after providing a service, could limit consumer welfare by…
    - Limiting the amount of research and development that can be done on pre-existing datasets. For example, SteadyIQ has only been able to build a product specifically designed for non-standard workers because of the data that was acquired through our consumer app.
    - Firms launch new services all the time which take advantage of pre-existing data, and this would limit that ability. For example, SteadyIQ will soon be trialing ongoing income verification instead of one-time use reports.

February 15, 2023

Submitted via email to Financial_Data_Rights_SBREFA@cfpb.gov

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

To Whom It May Concern:

Petal Technology Holdings, Inc. ("we," "us," "our," or "Petal") would like to thank the Consumer Financial Protection Bureau (the "CFPB" or "Bureau") for convening the Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights and inviting Petal to participate as a small entity representative, or SER. We have been honored to participate in this next important step by the Bureau toward its rulemaking under Section 1033 ("Section 1033") of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act"). Except as otherwise defined in this letter or required by the context herein, wherever we have used terms in this letter that are defined in Appendix B: Glossary of the Bureau's Outline of Proposals and Alternatives Under Consideration (the "Outline of Proposals"), we have ascribed the meanings to such terms that are set forth in the Outline of Proposals.

Background on Petal

Petal is a financial technology company that operates two businesses through its subsidiaries: Petal Card, Inc. ("Petal Card"), a consumer-facing credit card company; and Prism Data Technologies, Inc. ("Prism Data" or "Prism"), a business-to-business data analytics and technology software platform. Both businesses utilize consumer-authorized financial information, also referred to as "open banking data," in providing products and services.

- Petal Card uses open banking data to make safe and affordable credit more accessible to consumers, particularly those who lack credit scores or credit history. Petal offers access to a suite of credit cards (which are issued by WebBank, Member FDIC) as well as a mobile app that helps consumers better manage their financial lives.

- Prism Data is an open banking data analytics platform powering the next generation of credit risk scoring. Prism's suite of products enable financial institutions, financial technology firms, and other companies to derive powerful insights from open banking data. Prism clients can use those insights to better manage credit risk, create new products, and ultimately serve more consumers, especially those who have been underserved historically due to their lack of traditional credit bureau data.

Under the terms of the Outline of Proposals, Petal would be considered both a covered data provider as well as an authorized third party or data recipient.

Since our founding in 2016, Petal has been on a mission to expand access to opportunity by making responsible and modern financial services available to everyone. We are devoted to improving the financial lives of consumers, especially those who are underserved and underrepresented.

Our mission started with building a proprietary cash flow underwriting technology that we refer to as the CashScore™. Since our first product launch, this technology has enabled consumers applying for Petal-branded credit cards to leverage their personal financial data, including transaction data documenting their history of income, savings, bill payments, and other cash flows, to demonstrate their creditworthiness. Petal's technology analyzes this consumer-authorized information in an automated process to help make more holistic and accurate credit decisions.

Over the years, we have used this technology to evaluate millions of credit applications. Working together with our bank partner, we have provided credit cards to over 350,000 consumers, the vast majority of whom would be considered "underserved" because they had little or no previous credit history at the time they applied, or because they had a low credit score. More than 40% of consumers approved for Petal credit cards in the last year were first declined by a traditional bank. And, looking at the universe of Petal Card members ever approved for a card, a majority had either thin or no credit history when they were first underwritten. Petal Card members who joined the program with no prior credit history and were underwritten using open banking data have gone on to achieve an average credit score of 681 after 12 months as cardholders—typically considered a "prime" score.

Through Prism Data, we now make this technology available to other businesses, including banks, credit unions, lenders, and financial technology firms. The Prism technology platform helps partners analyze open banking data and incorporate actionable insights into their business processes and decision-making. Through the use of open banking data, Prism has

simplified consumer cash flow underwriting to a three-digit score—Prism's CashScore—that provides partners with a standardized and automated credit risk score similar to a FICO Score or VantageScore, but based on open banking data rather than traditional credit bureau data. The CashScore can be used as easily as traditional credit scores, and in a manner that is reliable, accurate, and compliant with applicable laws and regulations.

The Promise of Cash Flow Underwriting

Although the use of cash flows and bank statement information in loan underwriting is well established and widespread, that process has typically been a time-consuming and largely manual task. This inefficiency has historically accounted for the exclusion of this information from most small-dollar credit decisioning processes industry-wide. But the ability of consumers to share financial data, electronically in machine-readable format, has given rise to new capabilities like Prism's CashScore.

By accessing and sharing their electronic financial data, consumers may now provide lenders with a more complete and accurate view of their financial picture, including income, expenses, assets, and savings. Traditional credit data, by contrast, provides only a limited view into a consumer's financial status, focused on their debt. For too many consumers, traditional credit data is missing entirely. In addition, there are widely cited concerns regarding the accuracy of traditional credit data. In 2012, a congressionally mandated study by the Federal Trade Commission (FTC) found that one out of five study participants identified a material error in their credit report, which resulted in correction by a national Credit Reporting Agency ("CRA") after a dispute was filed, and that 13% of participants experienced a change in score due to such a correction.[1] [2]

The Bureau has estimated that 26 million Americans are "credit invisible" (i.e., they have no record at the major CRAs) and another 19 million are "unscorable" (i.e., their credit file is either

[1] Federal Trade Commission, *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003* (December 2012), *available at:* https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf, at i.

[2] A 2021 study found that errors on credit reports may impact as many as one in three consumers. See Gill, Lisa L. "More Than a Third of Volunteers in a Consumer Reports Study Found Errors in Their Credit Reports." Consumer Reports, June 11, 2021, *available at:* https://www.consumerreports.org/credit-scores-reports/consumers-found-errors-in-their-credit-reports-a6996937910/

too thin or too stale to generate a reliable score).[3] More recent data suggests these populations may be expanding in the absence of better market solutions.[4] Experian estimates that an additional 62 million U.S. consumers are "thin-file consumers", with financial histories so sparse that it may not be possible to generate an accurate credit score (or any score at all).[5]

Credit invisible and thin-file consumers do not comprise a representative sample of the U.S. population. Black and Hispanic Americans are almost two times more likely to be credit-invisible or unscorable than white or Asian Americans.[6] Not only are communities of color more likely to be credit invisible, but when they do have a credit score, as a group those scores are significantly lower than those of whites.[7] Based on research published by the Urban Institute in 2017, median credit scores in predominantly non-white areas across 60 major U.S. cities lagged median credit scores in predominantly white areas by almost 80 points (697 vs. 621, respectively).[8] In 38 of the 60 cities, this disparity was 100 points or more. In addition, in 50 of the 60 cities, predominantly non-white areas had below-prime median credit scores of 660 or lower, most of which were actually subprime credit scores of 600 or lower, whereas only four of the 60 cities had below-prime median credit scores in predominantly white areas. Credit invisibility also has an outsized impact on younger Americans. A 2022 study by Experian and Oliver Wyman found that 40% of credit invisibles in the United States were under the age of 25.[9]

Broad-based industry research, along with our experience at Petal, has undermined the commonly held view that credit invisible and thin-file consumers are categorically high-risk. In a whitepaper from 2016, VantageScore studied a sample population of unscorable consumers by

---

[3] Consumer Financial Protection Bureau, *Data Point: Credit Invisibles* (May 2015), *available at:* http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf (hereinafter, "CFPB Data Point").

[4] Experian and Oliver Wyman, *Financial Inclusion and Access to Credit* (January 2022), *available at:* https://us-go.experian.com/driving-growth-with-greater-credit-access-white-paper (hereinafter, "Experian and Oliver Wyman on Credit Access"). Found that 28 million Americans are now credit invisible, and 21 million are unscoreable.

[5] White, Jennifer, "What Is a Thin Credit File?". Experian blog, May 25, 2022, *available at:* https://www.experian.com/blogs/ask-experian/what-is-a-thin-credit-file-and-how-will-it-impact-your-life/

[6] CFPB Data Point, at 6.

[7] National Consumer Law Center (NCLC), *Credit Invisibility and Alternative Data: The Devil is in the Details* (June 2015), *available at:* https://www.nclc.org/images/pdf/credit_reports/ib-credit-invisible-june2015.pdf (hereinafter, "NCLC Credit Invisibility").

[8] Brown, Steven, and Ratcliffe, Caroline, Urban Institute, *Credit scores perpetuate racial disparities, even in America's most prosperous cities* (November 2017), *available at:* https://www.urban.org/urban-wire/credit-scores-perpetuate-racial-disparities-even-americas-most-prosperous-cities.

[9] Experian and Oliver Wyman on Credit Access, at 6.

appending demographic and economic data to traditional credit data and found that the unscorable consumers exhibited “a reasonable capacity for repaying debt in terms of income and income generation in light of their occupation profile” notwithstanding credit profiles that would traditionally be categorized as high-risk.[10]

In the absence of an established, reliable alternative source of data, the lending industry has become increasingly reliant on traditional credit data and scores to underwrite consumer and small business loans, and as a result, credit invisible and thin-file consumers face limited access, higher prices, and exclusion from mainstream financial options. As the use of credit scores has expanded into other industries over the past 10 years, credit invisible and thin-file consumers also may face difficulties obtaining employment, housing, and telecommunications and utility services.

Credit invisible and thin-file consumers are not the only U.S. consumers who have been shut out by underwriting based on traditional credit scores and need help accessing safe and affordable credit. Nearly half of all American adults today have non-prime credit scores.[11] In many cases, these individuals are fundamentally creditworthy but have in the past experienced some form of financial volatility or distress, like unexpected medical bills or loss of employment.

Consumer-authorized personal financial data can shine light on these blindspots in traditional credit scoring, and as a result, help unlock access for millions of consumers who are underserved. In July 2019, the nonprofit innovation center FinRegLab released a groundbreaking empirical study that analyzed the use of open banking or “cash flow” data by six non-bank financial services providers, including Petal Card, to predict creditworthiness.[12] In addition to validating the efficacy of cash flow underwriting models with regard to predicting creditworthiness, the report also found that cash flow data has the potential to improve the representation of underserved consumers who may have faced historical constraints, without introducing discrimination on the basis of age, race, or other protected factors. For example, for participants who provided sufficient data to analyze the percentage of customers with no or low traditional credit scores, the study found that these customers likely included “relatively high numbers of ‘no file’ and ‘thin file’ borrowers, as well as borrowers [who] may be having some difficulty accessing credit after past periods of financial instability.” In addition, with

---

[10] VantageScore, *Exclusionary Credit Score Modeling Limits Credit Access* (November 2016), *available at:* https://www.vantagescore.com/resource/144/exclusionary-credit-score-modeling-limits-credit-access.
[11] CFPB, *The Consumer Credit Card Market* (August 2021), *available at:* https://files.consumerfinance.gov/f/documents/cfpb_consumer-credit-card-market-report_2021.pdf, at 19.
[12] FinRegLab, *The Use of Cash-flow Data in Underwriting Credit: Empirical Research Findings* (July 2019), *available at:* https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

respect to "ZIP codes in which racial minorities exceed 50 percent or 80 percent of the total population as measured by the 2017 American Community Survey," the study found, based on data provided by certain participants, that these "participants served substantial populations in such ZIP codes, with 28 percent to 64 percent of their [customers] residing in 'majority minority' ZIP codes and 8 percent to 29 percent in 'predominantly minority' ZIP codes, respectively."[13]

Underwriting based on open banking data is not only more inclusive, it can be significantly more accurate as well. In our experience, even in instances where a full traditional credit file and score are available, cash flow underwriting using consumer-authorized information improves credit card loss rates by 30%. Open banking data is also more timely, more available, and more accurate than traditional credit data. Contrasting with the 45 million estimated American adults who are credit invisible or thin-file, approximately 96% of American households were banked in 2021 with financial data that could be accessed via Section 1033 for the purpose of demonstrating creditworthiness.[14] And unlike traditional credit bureau data, open banking data represents a virtually real-time leading indicator of consumers' financial health—their latest bank account balances, inflows, and outflows—as opposed to a lagging indicator that may trail months behind reality. Last, open banking data has a high degree of accuracy and quality because it is typically furnished directly from the ledger of a financial institution and associated with the authorizing consumer. Strong controls, incentives, and regulatory oversight already exist regarding the accuracy of this data as it is used in the ordinary course for banking and payments.

As a result, there is an emerging industry consensus that open banking data will become an increasingly focal component of consumer credit underwriting. VantageScore CEO Silvio Tavares recently noted that the "history of credit models is that they're not based on . . . bank account-type data. But probably over the next 10 to 15 years, bank account data is going to be one of the primary sources of credit scoring, just because it's timely, it's often more accurate, and it gives a much better picture of the consumer's actual behavior."[15] And earlier this year, FICO's vice president of scores & analytics noted, "For the millions of American consumers whose traditional credit files don't fully reflect their financial history and readiness for credit,

---

[13] *Id.* at 30.
[14] Federal Deposit Insurance Corporation, *2021 FDIC National Survey of Unbanked and Underbanked Households* (October 2022), *available at:* https://www.fdic.gov/analysis/household-survey/2021report.pdf.
[15] Adams, Kimberly and Shin, Daniel. "How one credit scoring company is thinking about financial inclusion." American Public Media's Marketplace, July 8, 2022, *available at:* https://www.marketplace.org/shows/marketplace-tech/how-one-credit-scoring-company-is-thinking-about-financial-inclusion/.

cash flow data provides a promising approach to fill in those gaps."[16]

As noted in the Bureau's outline, by "accessing their financial data, consumers are better able to manage their financial lives." For the most vulnerable consumers, accessing their financial data is quickly becoming foundational to building any stable financial life at all. Long-awaited technologies now exist that can correct for the blindspots, inaccuracies, and inequities in legacy credit scoring and include millions more consumers in the mainstream financial system. But the potential to do so rests heavily on the question of whether consumers will finally be able to safely and reliably access and share their financial data. Indeed, it is our belief that in the coming years, consumer financial data access and consumer credit access will become increasingly synonymous.

Consumers must be provided with the ability to demonstrate their creditworthiness using their own financial data. Today, consumers are routinely stymied in their attempts to do so. In 2020, approximately 39% of attempts by consumers to share financial data with Petal Card failed.[17] As a result, two in five consumers were unable to share evidence of their creditworthiness despite their clear intention and authorization to do so. Beyond our experience, a study of connectivity data provided to the Financial Data and Technology Association of North America ("FDATA North America") by a number of the largest U.S. data aggregators revealed that consumers and small businesses endure connectivity failure rates of between 47.39% and 40.16% when they first attempt to link their bank accounts to third-party financial applications, depending on the type of financial institution they use.[18] This frustration of consumers' will and intent can occur for a variety of reasons, but a vast majority are related to financial institutions that fail to provide reliable connections to third-party data aggregators.

It is clear in Section 1033 of the Dodd-Frank Act that Congress anticipated these problems and has provided a legislative solution. Section 1033(a) says that a financial institution (or data provider), as a "covered person" under the Dodd-Frank Act, "shall make available to a consumer, upon request, information in the control or possession of the [financial institution] concerning the consumer financial product or service that the consumer obtained from such [financial institution], including information relating to any transaction, series of transactions, or

---

[16] Gaskin, Joanne. "Cash Flow Data Can Improve Credit Access with an UltraFICO Score." FICO Blog, January 5, 2023, *available at:* https://www.fico.com/blogs/cash-flow-data-can-improve-credit-access-ultraficor-score.

[17] Internal Petal data. 'Attempts' are characterized as cases where a consumer took all steps available to link their bank account through a data aggregator and did not voluntarily abandon the effort at any step.

[18] Written Submission of Steven Boms, Executive Director, FDATA North America, Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, CFPB, February 26, 2020, https://files.consumerfinance.gov/f/documents/cfpb_boms-statement_symposium-consumer-access-financial-records.pdf, at 4.

to the account including costs, charges, and usage data." Such information "shall be made available in an electronic form usable by consumers."

Congress specifically delineated in Section 1033(b) four limited exceptions to the obligations of Section 1033(a).[19] Outside of these explicit exceptions, covered persons under the Dodd-Frank Act are required to comply with their statutory obligation to share financial data upon consumer request. The right to data access that Congress granted to consumers is unambiguous.

That right to robust and reliable access to financial data was passed into law nearly 13 years ago. In the years that have followed, private industry has taken up the vision set out by Congress, building a wealth of digital financial products and services that make it easier for consumers to save, borrow, invest, and responsibly manage their financial lives. New innovations like the CashScore have emerged as a byproduct, offering solutions to some of the most intractable and entrenched limitations of the existing credit system. But progress in this area has been limited by the unreliable nature of today's data access systems and processes. The progress that has been made is brittle and the potential in this area is far from fully realized. The reliable system by which consumers can access and share financial data that Congress envisaged is long overdue.

Recommendations

In prescribing rules for Section 1033, as further described below, we encourage the Bureau to place the consumer at the heart of the contemplated data access framework. Consumers must be granted fully the rights conferred to them by Congress to obtain fulsome financial data upon request and to control the disposition of that data thereafter. Once data is provided to a consumer, the right to determine who to subsequently share data with, for how long, and for what purpose, should vest entirely in the consumer whose financial history the data describes. While we acknowledge the complexities and practical challenges incumbent in establishing this new data access regime, any further delay must be weighed against the harm done to consumers unable to avail themselves of the data access rights promised to them by Congress. Every day we wait for full implementation of Section 1033 is an additional day that underserved consumers who need, and would otherwise qualify for, a loan, mortgage, or credit card, may be unable to obtain one, and instead are left with fewer options and greater expense. We are heartened that the Bureau has taken up rulemaking efforts in this area and encourage

[19] Pursuant to Section 1033(b), a covered person may not be required pursuant to Section 1033 to make available to the consumer-- (1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors; (2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; (3) any information required to be kept confidential by any other provision of law; or (4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

an expeditious rulemaking process in the interests of fairness, competition, and most importantly, the U.S. consumer.

As a general matter, it is our belief that Congress intended in Section 1033 to grant consumers a broad and reliable right and ability to obtain copies of their financial data from covered persons, subject only to a limited set of exceptions specifically delineated in 1033(b). Congress contemplated that consumers would then go on to use that data for their desired purposes, and specifically provided that "the information shall be made available in an electronic form usable by consumers."[20] In other words, Congress provided that (1) consumers, and authorized agents acting on their behalf, should be able to access copies of their financial information from institutions holding such information, and (2) after such requested information is provided, the consumer should have the ability to use the information as they see fit. As with a periodic statement mailed to a consumer in the ordinary course of using a financial product, it is our contention that the information conveyed through this process becomes the *property* of the consumer, in both the ordinary and legal use of the term.[21]

"Property" is defined generally as "the right to possess, use, and enjoy a determinate thing" and is "protected from undue governmental interference."[22] Property ownership confers a "bundle-of-rights" over the thing in question, central to which are rights of control, exclusion, and disposition. Among other things, a property owner can use their property, share it with others, exclude others from it, and sell it, without interference. No one disputes today that periodic statements relating to covered accounts, in PDF or paper form, including the data contained therein, are the property of consumers; we are not aware of any legal, contractual or other purported limits on what consumers can do with such statements, including the scope of the data they may share from such statements and with whom, for how long, and for what purposes they may share such statements.

It follows that this should apply equally to electronic financial data a consumer obtains by operation of their Section 1033 rights. We believe that the rules prescribed in this area must, at their core, mandate that covered persons provide another, easier way for consumers to access the information that is their property. These rules must respect the consumer's fundamental property right in their data, and with it their ability to share data with third parties of their

[20] We agree with the Bureau's interpretation of Dodd-Frank Act section 1002(4), which defines consumer, in this context, as "an individual or an agent, trustee, or representative acting on behalf of an individual."
[21] We believe a strong argument may also be made that the original version of the financial information held by the covered person, and not just the copies provided upon request, is the property of the consumer whom the information describes. In Section 1033(a) Congress states that the subject information is "in the control or possession of the covered person" rather than the property of the covered person.
[22] Black's Law Dictionary (9th ed. 2009).

choosing, on whatever terms, for whatever duration, and for whatever purposes the consumer determines. Just as it is the consumer's choice today as to how widely they share a PDF or paper copy of a periodic statement relating to a covered account, the rules promulgated by the Bureau under Section 1033 should honor consumer rights in using more advanced electronic delivery mechanisms as well. Our responses to many of the Bureau's questions in the Outline of Proposals flow from these core principles.

In our view, this position is required on not only legal, but public policy grounds as well. As further detailed below, any restrictions on the ability of consumers to share data for certain purposes, including so-called "secondary uses" beyond uses "reasonably necessary to provide the product or service that the consumer has requested," would risk freezing *today's* financial products and services, and the processes and systems with which they are provided, to the detriment of any new products, models, and capabilities that may be subsequently developed.

Similarly, "reauthorization" requirements that force consumers to express, again and again, on some periodic basis, their intent to share data, would frustrate the intent of the consumer and sap the utility of many useful financial products and services of ongoing nature derived from persistent data access (including those in market today and that may be developed in the future). Pursuant to the clear language and mandate of Section 1033(a), consumers should be able to obtain all of the financial data that a data provider has in their "control or possession . . . concerning the consumer financial product or service that the consumer obtained from such [data provider]"; placing limitations on the amount of historical data that a consumer may obtain pursuant to a Section 1033 rulemaking is arbitrary, contrary to the plain text of the Dodd-Frank Act, and disadvantages to both (i) Section 1033 data recipients relative to data providers (who don't have any comparable limitations) and (ii) underserved consumers, by diminishing the availability and efficacy of Section 1033 consumer-authorized financial information relative to other types of legacy financial data such as credit bureau data more easily provided by consumers that are well-served. These limitations, and similar restrictions on the consumer's ability to use their data contemplated in the Outline of Proposals risk undermining the Bureau's policy objectives related to competition, consumer choice, and consumer-friendly innovation.

Statutory Considerations

Q2. Are there any relevant statutes or regulations with which you must comply that you are concerned may duplicate, overlap, or conflict with the CFPB's proposals under consideration beyond those described in Appendix C? What challenges or costs would you anticipate in complying with any such statutes or regulations and the CFPB's proposals under consideration?

As a participant in the extension and servicing of consumer credit accounts, Petal and its partners are obligated to comply with a number of federal statutes and regulations, including those listed in Appendix C. Notably absent from Appendix C are the Equal Credit Opportunity Act (the "ECOA") and the CFPB's implementing regulation, Regulation B, as well as the Bank Secrecy Act (the "BSA"), all of which include substantial obligations which may conflict with the CFPB's proposals under consideration. In each case, in addition to other regulatory obligations listed in Appendix C that also contain record retention requirements, limitations on the retention of certain data collected through data aggregation could conflict with a financial institution's ability to comply with its record retention obligations. Additionally, small entities such as Petal would face significant technical, legal, and compliance burdens in separating data elements collected through data aggregation into relevant buckets for retention.

The BSA and its implementing regulations broadly cover establishing a reasonable belief for the true identity of a financial institution customer, establishing and maintaining risk ratings of customers, and identifying and reporting suspicious activity. Each of these areas has current and potential use cases enabled by access to personal financial information shared pursuant to the proposed rule. For example, bank account identifying information collected through data aggregation is used by Petal to establish that a bank account used for payments to a credit card account belongs to the same consumer, which is a critical source of non-documentary verification, valuable to both the Customer Identification Program ("CIP") and investigations related to Suspicious Activity Reporting ("SAR") investigations. In each case, records must be retained for at least five years with no affirmative deletion obligation.[23]

The ECOA and Regulation B broadly cover fair and responsible lending, including nondiscrimination obligations and technical requirements for deciding and notifying applicants of the outcome of an application for credit. Petal, on behalf of the issuing bank, uses customer-authorized financial information provided by data aggregators to deliver a credit decision to applicants in compliance with ECOA and Regulation B. This includes augmenting or substituting traditional credit bureau data with open banking data, which may result in a decision not to extend credit to certain applicants. In each of these cases, an Adverse Action Notice is delivered to the applicant listing the specific reason(s) for the denial of credit.[24] Where insights derived from open banking data are used as the principal reason(s) for denial, those specific reasons are included in the Adverse Action Notice. In order to comply with the record retention requirements of Regulation B, creditors using open banking data in this manner would

---

[23] Federal Financial Institutions Examination Council's BSA/AML Manual. "Appendix P: BSA Record Retention Requirements," *available at:* https://bsaaml.ffiec.gov/manual/Appendices/17.

[24] 12 CFR 1002.9(a)(2)(i).

be obligated to retain personal financial data records for a minimum of 25 months with no affirmation deletion obligation.[25]

Each of the regulations with record retention obligations listed in Appendix C, as well as the BSA and ECOA, define minimum retention periods without creating an obligation to delete relevant data once a required retention period has passed. Should the Bureau proceed with its proposed retention limitations for data covered under the proposed rule, it would create a first-of-its-kind federal regulatory obligation for the deletion of certain records in financial services. This would introduce a substantial new burden to small entities such as Petal and discourage other small entities from using covered data in the future to improve and enhance consumer financial services, as net new systems, processes, and controls must be built to ensure each data element is separated and treated in accordance with the various retention and/or deletion obligations that may apply. Further, any such limitations could diminish the utility of open banking data for use-cases like underwriting, as historical performance information over long periods of time and under different economic conditions is critical in the development of credit models and risk management strategies.

Scope of Covered Data Providers

Q5. Please provide input on the approach the CFPB is considering with respect to the coverage of data providers discussed in this part III.A. What alternative approaches should the CFPB consider? For example, should the CFPB also consider covering payment account providers that are not Regulation E financial institutions as presently defined, such as providers of government benefit accounts used to distribute needs-based benefits programs? Should the CFPB consider covering any providers of credit products that are not Regulation Z credit cards? How could the CFPB clarify coverage of the proposals under Consideration?

We agree with the Outline of Proposal that this Section 1033 rulemaking should cover Regulation E financial institutions and Regulation Z credit card issuers, but we have significant concerns that limiting Section 1033 data access rights only to products and services procured from those entities would deny the benefits of open banking to the millions of American consumers using other types of financial products from the full range of covered persons as defined in Section 1033 (including, among others, providers of mortgages, student loans, car loans, personal loans, or certain closed-loop prepaid card issuers, for example government benefit accounts like SNAP and EBT).

[25] 12 CFR 1002.12(b)(1)(i).

In Section 1033's language authorizing the Bureau to make rules effectuating consumer rights to access information, it states, "a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person…" While Section 1033 does not itself define "covered person," Section 1002 of the Dodd-Frank Act defines a covered person, in part, as "any person that engages in offering or providing a consumer financial product or service."[26]

The Bureau's use of "financial institution" as defined by Regulation E and "card issuer" as defined by Regulation Z significantly narrows the coverage of the proposed rule in a way that we believe does not benefit consumers and does not comport with the legislative intent of Congress. In doing so, the Bureau treats certain covered persons (including, among others, providers of mortgages, student loans, car loans, personal loans, or certain closed-loop prepaid card issuers, for example government benefit accounts like SNAP and EBT) differently from others, and it does so in a way that could disadvantage the consumers whose data are held by non-covered data providers who are covered persons.

Consumers with those types of financial products and services may have extensive histories documenting their ability to pay, and consistency in doing so. That data could, in turn, help consumers qualify for more and better financial products with more favorable terms. But if those other data providers are not covered by the rule, despite meeting the statutory definition of covered persons under Section 1033, consumers using their products and services will not enjoy the same choices and long-term economic benefits, and will be prevented from using important pieces of their own financial histories to demonstrate their creditworthiness. In many other contexts, like saving, planning, budgeting, and wealth management, it is imperative that consumers are able to access financial information describing their entire personal balance sheet; if consumers cannot access financial data describing their full financial picture, their ability to manage their finances in an informed and convenient manner may be seriously diminished.

This issue manifests in two ways that we see at Petal: (1) consumers who spend their money, time, and efforts to responsibly manage certain consumer financial products—products that could help them demonstrate their creditworthiness—are unable to use their data from non-covered data providers (organizations which meet the definition of 'covered persons' under the Dodd-Frank Act) to help them gain access to new consumer financial products offered by data recipients who leverage open banking data to expand access; and (2) these same data recipients who leverage open banking data to expand access are unable to access

[26] 12 U.S.C. § 5481(6).

and use consumer-authorized information more broadly to develop new and better products and services to further expand access to underserved consumers. For example, failure to include mortgage servicing in the proposed rule prevents the future development of a consumer product or service that uses information from a consumer's current mortgage to assess available refinance or purchase options and their specific monetary benefits or effects on consumers. Such a product or service could contribute meaningfully to promoting competition and supporting household financial stability, a stated goal of the Bureau.[27] Failure to include public benefits in this rulemaking would prevent the users of such benefits from taking advantage of modern financial products and services to manage their financial lives, including the potential advantages afforded by cash flow underwriting. This result seems contrary to the purpose and goal of ECOA and Regulation B, which require the inclusive consideration of public benefit income in credit decisions.[28]

In drafting the Dodd-Frank Act, Congress had available to it pre-existing definitions of "financial institution" and "card issuer" set forth in regulations promulgated by the Federal Reserve Board of Governors, yet chose to include neither in defining a consumer right to access information through Section 1033. Petal believes the Bureau should more closely align coverage of the proposed rule with the Dodd-Frank Act's definition of covered persons.

If the Bureau elects *not* to include this larger group of covered persons within the scope of the rule now, we encourage the Bureau to explicitly reserve its rights to expand the scope in the future. We agree with the sentiment Plaid's Global Head of Policy John Pitts expressed on this point in the company's submitted comments relating to the Outline of Proposals:[29]

> If the Bureau decides not to expand the scope of this rule to include categories described…then, at a minimum, the Bureau should make clear in the rule that the scope of the rule is not exhaustive or otherwise intended to limit the applicability of §1033, and that a regulation issued pursuant to §1033 is not necessary for enforcement of the statutory requirement.

---

[27] Consumer Financial Protection Bureau. "CFPB Launches Effort to Spur New Opportunities for Homeowners in the Mortgage Market." September 22, 2022, *available at:* https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-effort-to-spur-new-opportunities-for-homeowners-in-the-mortgage-market/.

[28] 12 CFR 1002.1(b).

[29] Written submission from John Pitts, Global Head of Policy, Plaid, "Re: Outline of Proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights," January 25, 2023, at 11 & 12.

Q9. Please provide input on whether asset size or activity level would be an appropriate metric for a possible exemption for covered data providers that are depository institutions. If so, what should the asset size or activity level threshold be? What would be an appropriate metric and threshold for a possible exemption for covered data providers that are not depository institutions? What alternative metrics should the CFPB consider?

In order to accomplish the stated objective of the proposed rule and spur marketplace competition, we encourage the Bureau not to exempt covered persons from proposals under consideration. The proposal outlines clear roles and responsibilities, and is not overly burdensome for data providers.

Consumer access to innovative financial products and services should not differ based on where a consumer chooses to bank. And consumers who may have made banking choices years or even decades ago should not be placed at a disadvantage today, and have their rights to access curtailed, based on exemptions they could not have anticipated.

Any exemptions based on asset size or activity level of covered data providers would unfairly and unnecessarily disadvantage customers of small banks and credit unions. Certified CDFI credit unions and banks/thrifts—institutions with perhaps the greatest focus on supporting underserved consumers—have average assets of $416 million and $356 million, respectively.[30] Consumers of small institutions, if such institutions are exempted from the proposed rule, would effectively be denied access to important and innovative financial services options that are available to consumers who have an ability to access and use their own financial data, significantly reducing competition and effectively leaving many consumers behind. Ensuring coverage for small institutions would incentivize the market, including core banking providers, to build data access portals and other necessary technologies to support consumer access to their own data. We also believe this coverage is critical to ensure competition among financial institutions and potentially for the long-term survival of many of the small and medium-sized community banks and credit unions who serve so many American consumers today.

While the Bureau will undoubtedly hear from and consider costs of compliance for small entities who might be subject to a more expansive definition of “data provider,” we believe that the importance of consumer access to data from these entities far outweighs the cost of

[30] U.S. Department of the Treasury, *CDFI Annual Certification and Data Collection Report (ACR): A Snapshot for Fiscal Year 2020*. (October 2021). *Available at:* https://www.cdfifund.gov/sites/cdfi/files/2021-10/ACR_Public_Report_Final_10062021_508Compliant_v2.pdf, at 33.

making it available. In our view, Congress has already made the public policy decision that offering consumers fulsome and reliable electronic access to financial data should be a requirement of entities that seek to provide consumer products and services in this country. Exempting covered persons from compliance with Section 1033 creates an unfair competitive advantage for those exempted and a disadvantage for their customers, leaving them with less control over and choice in managing their financial lives.

Q16. Where a covered account is held by more than one consumer, should the rule allow any consumer holding the account to authorize access, or should authorization procedures include a requirement that the third party provide authorization disclosures to and obtain consent from each consumer who is an Accountholder?

Where more than one consumer is identified as an account holder with full access to the account, Bureau precedent and current financial institution practices necessitate that only one consumer need authorize action on the account. For example, a joint account held by two consumers does not require both consumers to sign a check in order to be considered valid. Similarly, the commentary to 12 CFR § 1026.51 provides that income may be considered in a credit card applicant's ability to pay where the applicant has access to the account.

For example, applicants applying for a card through the Petal Card program may link bank accounts for consideration of their ability to pay in compliance with Regulation Z. Should the Bureau further restrict the ability for joint account holders to individually authorize this data sharing, it would unduly burden applicants relying on spousal or household income, presenting significant barriers to consumers' ability to access credit and also potentially posing fair lending concerns.

Retention & Availability of Consumer-Authorized Personal Financial Data

Q24. Please provide input about the length of time for which covered data providers retain transaction-detail information or can obtain the information from the relevant payment network, such as pursuant to the network's contractual obligations to the covered data provider.

We believe that covered data providers should be required to make available to consumers all covered information in their "control or possession" and to maintain covered information for a minimum of seven years. This requirement is necessary for consumer-authorized information to be fully utilized in underwriting use-cases on parity with traditional credit bureau data.

Today, data providers typically make only three to 24 months of data available upon consumer authorization - but this practice is inconsistent both with the text of Section 1033 and with the Bureau's stated policy objectives in this area.

First, Section 1033 describes data subject to consumer access rights as the information "in the control of possession of a covered person concerning the consumer financial product or service that the consumer obtained from such covered person." Where data is both (i) "in the control or possession of a covered person" and (ii) "concerning the consumer financial product or service that the consumer obtained from such covered person," Section 1033 data access rights clearly apply.

In practice, covered persons maintain consumer financial transaction records for far longer than 24 months, because the data provides ongoing utility to the covered person, and to their customers. Consumers have the ability to request offline records concerning their accounts going back considerably longer than this time period – often, dating back to the point of account opening. The shorter duration of record accessibility offered via an online user interface or mobile application is a reflection only of a market standard that is still in development and for which there has been (to date) little regulatory guidance. But it is clear that in practice financial institutions store, access, and use far more consumer data for their own purposes than what they currently make available to consumers. In fact, the Bank Secrecy Act currently requires that banks retain most customer records (including deposit records) for a minimum of five years,[31] and under the Fair Credit Reporting Act, CRAs are permitted to retain most negative information for up to seven years.[32]

Credit underwriting requires assessing a borrower's historical financial stability, in addition to their current ability to afford the financial product in question. For this reason, traditional credit data often includes seven years of history that can be used to assess a consumer's financial situation over time. Especially when considering financial products of longer duration, like mortgages, longer historical financial information is critical in assessing the qualification of a consumer. For example, a minimum of two years' history is typically required for mortgage qualification, as had been previously codified in Appendix Q to the Bureau's Qualified Mortgage Rule.

At Petal, we've found insights from cash flow underwriting to be particularly useful when combined with traditional credit bureau data to assess a consumer's creditworthiness. We believe that parity between the amount of data available via consumer authorization and the

[31] 31 CFR 501.601.
[32] 15 U.S.C § 1681c(a).

amount of data available from the CRAs is necessary to realize the full potential of cash flow based underwriting, and to maximize the potential for consumers to use their personal financial data to improve their economic standing.

Data providers may argue that there are not legitimate use cases for consumer-authorized data extending back multiple years. To that we respond that (i) we have an immediate use case in consumer credit underwriting at Petal, and (ii) today's digital financial tools have been constructed around today's limitations—if more consumer-authorized financial data is available, more information will be used in offering innovative and competitive financial products and services. In addition to the use cases of which we're aware today, the coming years will undoubtedly see new and innovative technologies developed that may require additional transaction history to effectively deliver financial products and services to consumers.

Q38. Please provide input on the approach the CFPB is considering with respect to making current and historical information available. What alternative approaches should the CFPB consider? Please provide input on whether or how the CFPB should define "current."

As stated in our response to Question 24, we believe that covered data providers should be required to make available to consumers (and furnish to third parties upon consumer authorization) all covered data in their control or possession, and a minimum of seven years' worth of history.

This approach would be in keeping with the Bureau's stated intention to benefit consumers and unleash increased competition with this proposed rulemaking. Requiring data providers to make an extensive set of historical transaction data available would maximize the variety of ways and use cases, now and in the future, in which consumers could put their personal financial data to use to improve their economic standing. It would give consumers even more ability to shop for lower rates and better products and services, knowing that they could choose a new financial services provider without losing details about their financial history. It would enable new innovation, with companies competing to create more tailored products and services to serve more consumers and more diverse consumer needs, informed by a longer-term and fuller understanding of more consumers' financial histories. Companies like Petal Card and Prism Data could further expand access to financial services and credit.

At Petal Card, we have seen that having access to a greater depth of a consumer's financial transaction history can help with more accurate underwriting (and, conversely, that the less

history a consumer has available, the harder it is to accurately underwrite them). Indeed, that is why mortgage applicants are typically required to provide a minimum of two years' financial history in order to qualify for a mortgage. The Financial Health Network spoke to the importance of this extended view in its submitted comments about the Outline of Proposals:[33]

> To most effectively help consumers make choices about product selection and usage, and to help them manage their finances more generally, third party providers generally rely on multiple quarters of historical transaction detail from transaction, savings, and credit card accounts. Earnings and spending both fluctuate seasonally, and a consumer's earnings and costs of living–and their susceptibility to spikes and dips in either—are most discernible over a full year. Tax preparation and planning generally requires the last full year's worth of expense detail. So does planning—in the form of short-term savings—for lumpy but recurring expenditures (such as winter heating bills or back-to-school expenses in the fall).

Requiring covered persons to make available at least seven years of consumer historical transaction detail information would enhance competition by creating a truly level playing field between CRA and non-CRA data. CRAs are authorized to retain a full seven years of consumer credit records, and data providers covered by the Bank Secrecy Act retain a minimum of five years of consumer deposit data. Limiting the amount of data that consumers are able to access would harm consumers by giving CRAs a permanent information advantage that cements their status as the exclusive arbiters of long-term financial stability. And nascent competitors would be at an information disadvantage, confined to a much more limited set of data than the data providers.

We encourage the Bureau to avoid codifying the status quo and further cementing the dominant position of data providers and CRAs and put consumer-authorized data at least on equal footing.

In addition, we concur with The Financial Transaction Association's suggestions, in comments the organization submitted in support of this rulemaking, encouraging the Bureau to be wary of ways in which data providers could potentially game the Section 1033 rule:[34]

---

[33] Written submission from The Financial Health Network, Re: The Outline of Proposals and Alternatives Under Consideration, Required Rulemaking on Personal Financial Data Rights. January 25, 2023, at 14.
[34] Written Submission of Penny Lee, Chief Executive Officer, Financial Transaction Association ("FTA"), to CFPB re: Section 1033, submitted January 23, 2023, at 9.

While FTA supports the concept that a provider should make available such historical data, we caution that FIs should not use this rule to begin limiting or reducing the date ranges made available to consumers on such online account interfaces in order to reduce what historical data they must share under this rulemaking. This would be an example of an FI effectively gaming the rule to the detriment of the consumer and for anti-competitive purposes.

Limitations on Collection, Use, and Retention

Q88. Please provide input on the approach the CFPB is considering to limit third party collection, use, and retention of consumer-authorized information to what is reasonably necessary to provide the requested product or service. What alternative standards should the CFPB consider? In providing this input, please describe any guidance the CFPB should consider to clarify the applicability of the standard or any alternative standards the CFPB should consider.

The limitation on collection, use, and retention of consumer-authorized information to only "what is reasonably necessary to provide the product or service the consumer has requested" or "limitation standard" proposed by the Bureau, while well intentioned, would undermine consumer control, stifle competition and ultimately erode consumers' access to innovative financial products. This limitation standard would prevent the development of cash flow underwriting as a viable alternative to traditional credit scores, and negatively impact many data recipients seeking—today and in the future—to build new, innovative, and competitive financial products and services that benefit consumers.

There are no restrictions today that limit a consumer's rights to use the information featured on their periodic statements. This information is treated as the consumer's property, to do with as they choose—including sharing for whatever purposes they see fit. The same should be true of electronic financial data obtained via Section 1033; consumers should have a full and unencumbered right to determine with whom they share data and for what purposes in accordance with the terms of their authorization.

The proposed limitation standard would shut down the process of innovation that has played out over the past decade and yielded the great many consumer advantages that the Bureau enumerates in its Introduction to the Outline of Proposals. If consumer-authorized information could only be used for products or services that consumers are currently requesting, it would be impossible to improve existing products or services or develop new and more inclusive products or services that meet the needs of underserved communities. In other words, the status quo would be frozen in place.

Financial products and services that use consumer-authorized information are reliant on that data not only to directly provide products or services requested by consumers, but also to improve those products or services for the future. For example, credit models make predictions about future applications for credit based on past decisions and the corresponding outcomes. Utilizing consumer-authorized information in this way is not "reasonably necessary to provide the product or service the consumer has requested," but is nevertheless essential for open banking data to factor into credit decisions at all. The limitation standard would therefore make it difficult—if not impossible—to iterate and improve on existing products that utilize consumer-authorized information.

The impact of the limitation standard on new innovation may be even more severe. New products and services that utilize consumer-authorized information can be developed only by using that data, yet anything new is by definition outside of the products or services consumers are currently requesting. Many of the modern financial tools that consumers now enjoy are the product of innovation using consumer-authorized information, outside of that data's direct use for the product or service being offered. Similar arguments may be made in favor of use of this data for academic or government research, non-profit advocacy, and other important use cases outside of the direct provision of a specific product or service.

Further, the limitation standard risks creating a vastly uneven playing field, putting data recipients at a tremendous disadvantage relative to data providers. Covered data providers enjoy broad usage and storage rights under the GLBA framework and the terms and conditions presented to consumers upon account opening and periodically thereafter. Any asymmetry between the constrained rights of data recipients to use consumer-authorized information, on the one hand, and the unfettered rights of covered data providers to use the data generated by consumers' usage of covered accounts on the other, would be incredibly stifling to competition, providing a strong lock-in effect in favor of legacy financial institutions. Instead of spurring consumer-friendly competition in the marketplace, such a rule would further entrench the market position of data providers.

We concur with comments submitted by the Financial Health Network as part of this process on the importance of parity between third-party data recipients and data providers in treatment under this rulemaking[35]:

[35] Written submission from The Financial Health Network to CFPB, Re: The Outline of Proposals and Alternatives Under Consideration, Required Rulemaking on Personal Financial Data Rights. January 25, 2023, at 25.

> Innovations of all sorts depend on the ability of third party data recipients to learn from those data. Indeed, consumers' grants of data access to their financial data has in numerous circumstances created a virtuous circle in which third party data recipients both provide valuable services and use incoming data to further improve or expand upon their services in much the same way that data providers themselves may do as part of their own product development processes. At the same time, once a third party data recipient has obtained data it was authorized to obtain, the privacy risks associated with that third party itself mining those data for new insights seem minimal at most.

Beyond the anti-competitive impact that would result from establishing a different framework for covered data providers and authorized third parties, such a framework would also result in unnecessary operational complexity and undesirable consumer confusion. Like Petal, many authorized third parties will also themselves be data providers, and vice-versa. Applying different standards to otherwise similar data would create a Gordian Knot for consumers to untangle.

While well-intentioned, the limitation standard ultimately comes into unavoidable conflict with the rights afforded to consumers by Congress in Section 1033. The consumer should have the ability to decide how data they have shared should or should not be used, and what limitations, if any, should apply.

Instead of limiting the rights of the consumer to determine acceptable uses of their personal financial data, a more appropriate path to mitigating the identified risks would be to require third parties to present clear, user-friendly, plain-language terms and conditions to the consumer, delineating what the third party is allowed to do with the consumers' data, making clear what restrictions exist, requiring affirmative opt-in, and providing reasonable and convenient procedures for revocation of access in the future.

Consumer Reauthorization and Revocation

Q92. Please provide input on the approach the CFPB is considering that would establish a maximum durational period for all use cases, along with any alternative approaches the CFPB should consider. Please provide input on the length of the maximum durational period, including whether certain use cases should have shorter or longer maximum durational periods.

Q93. If the rule were to require third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and

unnecessary costs on authorized third parties? For example, should the CFPB consider proposals that would allow authorized third parties to:

- **Seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses?**
- **Establish a presumption of reauthorization, subject to a consumer's ability to opt out of the presumption, based on the consumer's recent use of a product or service? If so, what should be considered "recent" use?**
- **Require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers?**

As the owners of their personal financial data, consumers should be able to use and share that data with as many trusted third-party data recipients as they wish, for as long as they wish. Consumers should also have the ability to control the nature, extent and duration of a data recipient's use, which can be accomplished through two important means: (1) the data recipient's presentation of an appropriate authorization disclosure and the consumer's informed consent to the disclosed key terms and certification regarding access to and collection, use and retention of the applicable consumer-authorized information; and (2) the consumer's unambiguous right and ability to revoke access to their information at any time. Other limitations that frustrate the consumers ability to share data, like forced reauthorization, would arbitrarily limit the consumer's rights, and undermine the consumer's ability to use many modern financial products and services that require ongoing access to data.

Take for example services that provide ongoing account monitoring to prevent overdrafts. The nature of such a service is "always on" and running "in the background." Not only would periodic reauthorization impose inconvenience on the consumer, it would result in service outages and failures, which could in turn result in real financial consequences and consumer harm. Forced reauthorization strips consumers of the ability to opt-in to programs that require persistent access, a decision that should be within the rights afforded consumers under Section 1033.

As the FTA noted in its submitted comment, in the United Kingdom, the Financial Conduct Authority initially imposed reauthorization requirements, and subsequently scrapped them after finding they resulted in friction and lower consumer adoption of products and services utilizing consumer-authorized data.[36]

[36] Written Submission of Penny Lee, Chief Executive Officer, Financial Transaction Association (FTA), to CFPB, Re: FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights. Submitted January 23, 2023, at 15.

> With respect to consumer reauthorization, FTA suggests that the Bureau take note of the experience in the UK, where the FCA recently scrapped the prior 90-day reauthorization rule that required consumers to log into their banking account to reauthorize the ability of a third-party provider to receive that account's information. The FCA noted that the prior rule "creates friction . . . and increases the likelihood of customers dropping off. . . "Instead of requiring a strong, repeated authentication for reauthorization within the primary account providing information, the FCA now allows reauthorization to occur within the third-party app. FTA supports this approach as consistent with the consumer's best interest.

Q101. For third parties: please describe your current practices for using consumer-authorized information in ways that are not reasonably necessary to provide the consumer's requested product or service. Please describe your reasons for doing so.

Prism Data helps banks and other financial providers to interpret and analyze de-identified, consumer-authorized financial data. Prism uses historical financial data to build models, data attributes, and scores that can be used by clients to predict future financial outcomes. This process of model development requires that consumer-authorized information be used, not only to deliver a "requested product or service" but also to build and improve on models that will be used to deliver products or services requested by others in the future.

For example, by studying historical financial data, Prism has devised a methodology by which we can identify rental transactions within consumer-authorized banking history. This methodology now gives lenders the ability to identify a consumer's history of rental payments in an automated way. Going forward, this capability can put renters on more even footing with homeowners that have their mortgage payment history reported to the CRAs. This is important for racial equity and access; as Fannie Mae noted in its Equitable Housing Finance Plan, Black homeownership in the United States still lags far behind white homeownership (42% compared to 72% of white households).[37]

This is just one example of the many secondary uses that deliver substantial value to consumers, allowing Prism Data and Petal to enhance our existing products and services, identify new ways to meet consumers' financial needs, and most importantly, to make credit more easily accessible to individuals that are currently underserved. These secondary uses are commonplace in today's market and are an important part of the product development

[37] Fannie Mae, *Equitable Housing Finance Plan*, July 2, 2022, *available at:* https://www.fanniemae.com/media/43636/display.

process. Limiting this process, and doing so in a manner that impacts data recipients, but not data providers, could have disastrous unintended consequences for consumers and small entities who compete to serve them.

Q110. Should the CFPB consider more flexibilities related to retention beyond an exception for compliance with other laws? For example, should the CFPB consider allowing authorized third parties to retain de-identified consumer information? For what purposes might authorized third parties seek to retain deidentified consumer information, and by what standards should consumer information be de-identified?

As noted in our response to Q88, we believe that introducing retention limitations that apply only to third-party data recipients in the open banking ecosystem, and not to covered data providers, creates an uneven playing field that will reduce competition and create unintended consumer harm. These limitations would have a particularly outsized impact on small entities like Petal and Prism Data—who would be disadvantaged in competing against entrenched market dominants who are subject to no such limitations or restrictions—and the traditionally underserved consumers who benefit most from new products and services.

While we believe that the rationale for limiting usage of consumer-authorized, de-identified consumer information is theoretically even more difficult to discern than personally identifiable information, we strongly believe, as we've stated elsewhere in this letter, that the Bureau should not create a limitation here on data recipients' ability to retain consumer-authorized information.

That being said, if the Bureau insists on setting some limitations on retention of consumer-authorized information, we believe the standard should be different and more flexible for de-identified information. By its very nature, de-identified data no longer contains information that might identify a consumer or expose the consumer to potential harm. Therefore, it is unclear what risk such a limitation might be deployed to mitigate.

We concur with the sentiments expressed by the Financial Technology Association in its January 2023 comment letter on the Outline of Proposals:[38]

> ....[T]o the extent that the Bureau considers deletion requirements of certain consumer personal financial data, FTA recommends a common-sense exception

[38] Written Submission of Penny Lee, Chief Executive Officer, Financial Transaction Association, to CFPB, "Re: FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights", January 23, 2023, at 15.

> for anonymized information to be kept for research and innovation purposes. This type of data is critical to developing new products and services for consumers, can help develop fraud mitigation tools, and its ongoing retention and use would pose no harm to consumers.

De-identified data sets (in addition to identified data sets) are regularly used in other areas of the industry for model and other product development, without specific limitations on storage or usage. The ability to retain and leverage this data is crucial for participants in the ecosystem to observe trends over time, understand outcomes, build a richer understanding of consumer behavior, and iterate on existing approaches, products and services.

* * *

We hope that the Bureau will consider the foregoing suggestions in developing regulations to implement Section 1033, and we appreciate the opportunity to provide our thoughts and perspective and to participate as a Small Entity Representative in this process.

Respectfully submitted,

Petal

APPENDIX C: LIST OF MATERIALS PROVIDED TO SMALL ENTITY REPRESENTATIVES

In advance of the Panel Outreach Meetings, the CFPB provided each of the SERs with the materials listed below. Each of these items was also made available on the CFPB's website at https://www.consumerfinance.gov/personal-financial-data-rights/.

- Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for the Required Rulemaking on Personal Financial Data Rights (Oct. 27, 2022).

- High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights (Oct. 27, 2022).

(See Appendix D and Appendix E, respectively.)

In addition to the above materials, SERs also received a copy of the presentation materials for the Panel Outreach Meetings. (See Appendix F.)

APPENDIX D: OUTLINE OF PROPOSALS AND ALTERNATIVES UNDER CONSIDERATION

See attached.

SMALL BUSINESS ADVISORY REVIEW PANEL FOR REQUIRED RULEMAKING ON PERSONAL FINANCIAL DATA RIGHTS

OUTLINE OF PROPOSALS AND ALTERNATIVES UNDER CONSIDERATION

October 27, 2022

Table of Contents

I. Introduction

Section 1021(a) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) states that the purpose of the Consumer Financial Protection Bureau (CFPB or Bureau) is "to implement and, where applicable, enforce Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."[1] Consistent with that purpose, section 1033(a) of the Dodd-Frank Act authorizes the CFPB to prescribe rules requiring

> a covered person [to] make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.[2]

In addition, section 1033(d) states that "[t]he Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section."[3]

Prior to issuing a proposed rule regarding section 1033, the CFPB is moving forward with fulfilling its obligations under the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA),[4] which amended the Regulatory Flexibility Act (RFA),[5] to assess the impact on small entities that would be directly affected by the proposals under consideration prior to issuing a proposed rule regarding section 1033.

In modern consumer finance, financial entities hold a great deal of data about their customers and the products and services they offer. Such data have always been valuable to the account-holding entity, but consumers have been less able to benefit from their data for their own purposes. However, as technology has made it possible to store, analyze, and share personal financial data electronically, interest has grown within the financial services industry and among policymakers in the potential benefits of bolstering consumers' rights to access personal financial

[1] Public Law 111-203, section 1021(a), 124 Stat. 1376, 1979 (2010) (codified at 12 U.S.C. 5511(a)).

[2] Dodd-Frank Act section 1033(a), 124 Stat. 2008 (codified at 12 U.S.C. 5533(a)). The full text of section 1033 is included as Appendix A.

[3] Dodd-Frank Act section 1033(d), 124 Stat. 2008 (codified at 12 U.S.C. 5533(d)).

[4] Public Law 104-121, tit. II, 110 Stat. 857 (1996) (codified at 5 U.S.C. 609) (amended by Dodd-Frank Act section 1100G).

[5] 5 U.S.C. 601 *et seq*.

data and, if they wish, share their data with others, including competing financial services providers.[6]

By accessing their financial data, consumers are better able to manage their financial lives. Today, many financial entities make a great deal of consumers' financial information available to them through online financial account management portals, but consumers may benefit from increased direct access to their financial data, as well as from the ability to share their data with third parties offering them a product or service that complements or relies on data about the products and services they already use.

Data access rights also hold the potential to intensify competition in consumer finance. This can happen in three main ways: by enabling improvements to existing products and services, by fostering competition for existing products and services, and by enabling the development of new types of products and services.[7] If consumers can authorize the transfer of their account data to a competitor, new providers will be able to treat new customers more like customers with longer account relationships, and may have greater ability to provide the better products usually reserved for long-time customers. Customers would not have to "start over," but could transfer the relationship built with an old provider to a new provider, potentially giving them access to higher credit limits or lower account fees. This could enhance competition and drive better service aimed at keeping customers. In addition, as firms use consumer-authorized data to both improve upon and provide greater access to existing products and services, as well as develop new products and services, consumers' motivation to switch providers to get a better deal may grow, making them more likely to abandon providers who treat them poorly. This should incentivize providers to earn their customers through competitive prices and high-quality service. Today, we believe there is evidence that market-driven consumer data access has already produced some of these benefits.[8]

[6] In the financial services industry, "data aggregation" firms emerged in the 2000s to enable consumer-authorized access to personal financial data. *See, e.g.*, Michael S. Barr *et al.*, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, Univ. of Mich. Ctr. on Fin., L. & Policy, Working Paper No. 1 (Nov. 1, 2019), https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[7] Bureau of Consumer Fin. Prot., Advance Notice of Proposed Rulemaking, Consumer Access to Financial Records, 85 FR 71003 (Nov. 6, 2020).

[8] Many consumers have adopted fintech services that tend to rely on or utilize direct access to consumer-authorized data and have authorized third parties to access their financial data. One trade association estimates that the number of consumers who have utilized a service affected in some way by consumer-authorized data sharing may be as large as 100 million, and that the number of consumer and small business accounts accessed by authorized third parties is estimated to be 1.8 billion. *See* Fin. Data & Tech. Ass'n (FDATA), *Competition Issues in Data Driven Consumer and Small Business Financial Services* 11 (June 2020), https://fdata.global/north-america/wp-content/uploads/sites/3/2020/06/FDATA-US-Anticompetition-White-Paper-FINAL.pdf. Further, the EY Global FinTech Adoption Index shows that in 2019, 46 percent of digitally active U.S. consumers were "fintech adopters," up from 17 percent in 2015 and 33 percent in 2017. EY, *Global FinTech Adoption Index* 6 (2019), https://www.ey.com/en_us/ey-global-fintech-adoption-index. Fintech adopters are consumers who use at least one fintech service from at least two of these five categories: savings and investments; borrowing; insurance; money transfer and payments; and budgeting and financial planning. Many such services, when offered by fintechs, rely on or routinely utilize consumer-authorized data access. To the extent this widespread adoption indicates consumers are voting with their feet, and to the extent such opting for improved offerings is catalyzed by consumer-authorized

While the CFPB is encouraged by some of the competitive effects of market-driven data access occurring today, it has become clear that these gains cannot be guaranteed until disagreements over consumer-authorized information sharing are addressed through rulemaking. Action is also needed to ensure that consumer-authorized information shared with third parties is not used for purposes not requested by the consumer or obtained using misleading tactics, particularly by firms whose surveillance revenue models incentivize them to use and abuse consumer data. Such practices have contributed to a lack of trust among market participants, and a growing sense of powerlessness among consumers.

As noted, Dodd-Frank Act section 1033(a) authorizes the CFPB to prescribe rules requiring a covered person to make information available to a consumer. In turn, Dodd-Frank Act section 1002(4) defines the term "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual."

This Outline of Proposals and Alternatives Under Consideration (Outline) describes proposals the CFPB is considering that, if finalized, would specify rules requiring certain covered persons that are data providers to make consumer financial information available to a consumer directly and to those third parties the consumer authorizes to access such information on the consumer's behalf, such as a data aggregator or data recipient (authorized third parties).[9] In addition to considering proposals applicable to data providers, the CFPB is considering proposals applicable to third parties, as discussed in part III.B.2 and part III.E below.

The full text of section 1033 is included as Appendix A. Appendix B sets forth a glossary of defined terms used in this Outline. Appendix C contains a list of Federal statutes and regulations that are closely related to section 1033.

II. The SBREFA Process

The Dodd-Frank Act requires the CFPB to comply with SBREFA, which imposes additional procedural requirements for rulemakings, including this consultative process, when a rule is expected to have a significant economic impact on a substantial number of small entities.[10] The SBREFA consultation process provides a mechanism for the CFPB to obtain input from small entities early in the rulemaking process. SBREFA directs the CFPB to convene a Small Business Review Panel (Panel) when it is considering proposing a rule that could have a significant

data access, competition in consumer finance appears to benefit from the ability of consumers to permit third parties to directly access their personal financial data.

[9] For purposes of this Outline, a "data provider" means a covered person with control or possession of consumer financial data. The term is intended to refer to the same types of entities described as "data holders" in the CFPB's 2020 Advance Notice of Proposed Rulemaking (ANPR). *See* 85 FR 71003, 71004 (Nov. 6, 2020). A "data recipient" means a third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer. The term is intended to refer to the same types of entities described as "data users" in the ANPR. *See id.* A "data aggregator" (or aggregator) means an entity that supports data recipients and data providers in enabling authorized information access. Depending on the context and its activities, a particular entity may meet several of these definitions. In this Outline, the CFPB refers to data recipients and data aggregators, generally, as "third parties."

[10] *See* 5 U.S.C. 609(b).

economic impact on a substantial number of small entities. The Panel includes representatives from the CFPB, the Small Business Administration's (SBA) Chief Counsel for Advocacy,[11] and the Office of Information and Regulatory Affairs in the Office of Management and Budget.

The Panel is required to collect advice and recommendations from small entities or their representatives (referred to as small entity representatives, or SERs) that are likely to be subject to the regulation that the CFPB is considering proposing. For this purpose, the RFA defines "small entities" as small businesses, small organizations, and small governmental jurisdictions. The term "small business" has the same meaning as "small business concern" under section 3 of the Small Business Act (SB Act);[12] the term "small organization" is defined as any not-for-profit enterprise which is independently owned and operated and is not dominant in its field; and the term "small governmental jurisdiction" is defined as the governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than 50,000.[13] Thus, to determine whether a business is a small entity, the CFPB looks to the SBA's size standards.[14]

Small entities likely to be affected by the proposals under consideration are those that meet the definitions of covered data providers,[15] data recipients, or data aggregators. The CFPB estimates that over 8,000 small covered data providers are likely to be affected by the proposals under consideration. These covered data providers include depository institutions, such as Commercial Banks, Savings Associations, and Credit Unions with assets of $750 million or less.[16] In addition, some nondepository institutions likely meet the definition of covered data providers.

Nondepository financial institutions and entities outside of the financial industry may also be affected, though it is important to note that entities within these industries would only be subject to the proposals under consideration if they meet the definitions of covered data provider, data recipient, or data aggregator. The CFPB expects that thousands of these small nondepositories likely meet the definition of data recipient, and a smaller number likely meet the definitions of covered data provider or data aggregator. Examples of potentially affected small data recipients include entities using consumer-authorized information to underwrite loans, offer budgeting or

[11] The Office of Advocacy (Advocacy) is an independent office within the SBA, so the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration.

[12] Public Law 85-536, section 2, 72 Stat. 384 (1958) (codified at 15 U.S.C. 631).

[13] *See* 5 U.S.C. 601(3) through (6).

[14] *See* Small Bus. Admin., *Table of Small Business Size Standards Matched to North American Industry Classification System Codes* (effective May 2, 2022), https://www.sba.gov/sites/default/files/2022-05/Table%20of%20Size%20Standards_Effective%20May%202%202022_Final.pdf (SBA Size Standards).

[15] As explained below in part III.A.1, the proposals under consideration would use two existing definitions to establish coverage over data providers: "financial institution" as defined by Regulation E, and "card issuer" as defined by Regulation Z. In this Outline, the CFPB refers to financial institutions and card issuers collectively as "covered data providers."

[16] The North American Industry Classification System (NAICS) codes for these types of depository institutions are 522110, 522120, 522130. Affected entities could potentially also fall into the category of credit card issuing institutions (NAICS 522210); these entities are considered small if they have assets of $750 million or less.

personal financial management services, or facilitate payments. These examples are not intended to cover all potential third parties or uses of consumer-authorized information.

The nondepository financial institutions that may be affected are those involved in Non-Depository Credit Intermediation, Activities Related to Credit Intermediation, and Securities and Commodity Contracts Intermediation and Brokerage.[17] Potentially affected entities outside of the financial industry include Software Publishers; Data Processing, Hosting, and Related Services; Payroll Services; Custom Computer Programming Services; and Credit Bureaus.[18] To be considered small, the maximum size standard for any of these nondepository financial institutions or entities outside of the financial industry is $41.5 million in average annual receipts, though several have lower thresholds.

SBREFA requires the CFPB to collect the advice and recommendations of SERs concerning whether the proposals under consideration might increase the cost of credit for small entities and if alternatives exist that might accomplish the stated objectives of applicable statutes and that minimize any such increase.[19] During the Panel outreach meeting, SERs will provide the Panel with important advice and recommendations on the potential impacts of the proposals under consideration. They may also provide feedback on regulatory alternatives to minimize these impacts.

Within 60 days of convening, the Panel is required to complete a report on the input received from the SERs during the SBREFA process. The CFPB will consider the SERs' feedback and the Panel's report as it prepares the proposed rule. Once the proposed rule is published, the CFPB is required to place the Panel Report in the public rulemaking record. The CFPB also welcomes further feedback from the SERs during the public comment period on the proposed rule.

In accordance with the above requirements, the CFPB is convening a Panel to obtain input from SERs on the proposals under consideration for making consumer financial information available pursuant to Dodd-Frank Act section 1033. The CFPB has prepared this Outline to provide background to the SERs and to facilitate the SBREFA process. However, the SBREFA process is only one step in the CFPB's rulemaking process. No data provider or third party will be required to comply with any new regulatory requirements before a proposed rule is published, public comment on the proposed rule is received and reviewed by the CFPB, a final rule is issued, and the implementation period between the final rule's issuance date and its compliance date concludes. One of the specific questions on which the CFPB seeks input during this SBREFA process is how long small entities would need to conform their practices to the proposals under consideration if those proposals were ultimately to be adopted in a final rule.

[17] The 2022 four-digit NAICS codes for these categories are 5222, 5223, and 5231. Specific industries and six-digit NAICS codes potentially affected within these categories include Sales Financing (522220); Consumer Lending (522291); Real Estate Credit (522292); Financial Transactions Processing, Reserve, and Clearinghouse Activities (522320); Other Activities Related to Credit Intermediation (522390); Investment Banking and Securities Dealing (523110); Securities Brokerage (523120); and Commodities Contracts Brokerage (523140).

[18] The 2022 six-digit NAICS codes for these industries are 511210, 518210, 541214, 541511, and 561450.

[19] Dodd-Frank Act section 1100G, 124 Stat. 2112.

The CFPB is also conferring with other Federal agencies, including the other prudential regulators and the Federal Trade Commission (FTC), and is seeking feedback from a wide range of stakeholders on the proposals under consideration.[20] Stakeholders are welcome to provide written feedback on the CFPB's proposals under consideration by emailing it to Financial_Data_Rights_SBREFA@cfpb.gov.[21] The CFPB requests that stakeholders who are not SERs and who wish to provide feedback do so no later than January 25, 2023. The CFPB will coordinate with SERs on the timing for their feedback on the Outline.

III. Proposals and Alternatives Under Consideration to Implement Section 1033 of the Dodd-Frank Act Regarding Making Consumer Financial Information Available to Consumers

In this part III, the CFPB first discusses the overall scope of coverage of the proposals under consideration, including the data providers that would be subject to the proposals, the consumers and authorized third parties that would be permitted to access information from covered data providers, and the types of information that covered data providers generally would have to make available to consumers and authorized third parties. The CFPB then discusses proposals under consideration related to how and when covered data providers would be required to make information available directly to consumers and to authorized third parties. Next, the CFPB discusses proposals under consideration with respect to authorized third parties' obligations regarding collection, use, and retention of consumer information. The CFPB then addresses proposals under consideration related to record retention and the implementation period for the final rule.

Throughout this Outline, the CFPB lists questions it would like SERs to answer regarding its proposals and alternatives under consideration. The CFPB is generally interested in input from SERs on all of the proposals under consideration and any alternatives the CFPB should consider.

For all these questions, the CFPB invites feedback from data providers and third parties that access data on behalf of consumers. When providing feedback on the proposals and alternatives under consideration discussed in this Outline, please include feedback on the costs and benefits of those proposals and alternatives, including implementation costs. Quantitative information about SERs' own experienced or expected implementation costs is particularly valuable. If

[20] In addition to conferring with staff from Advocacy and OIRA, the CFPB has invited discussion on these proposals under consideration with staff from the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, and the Bureau of Fiscal Service of the Department of the Treasury. The CFPB plans to continue conferring with these and other agencies throughout the rulemaking process.

[21] Written feedback from SERs will be appended to the Panel Report. Any feedback the CFPB receives from other stakeholders may also be subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. SERs and other stakeholders considering submitting proprietary or confidential business information should contact the CFPB in advance to discuss whether and how that information should be provided.

possible, when providing feedback on specific questions, please include the relevant question number(s).

The questions in this Outline are numbered sequentially throughout for ease of reference, and begin here:

Q1. Do you believe any of the requirements of the closely related statutes and regulations identified in Appendix C duplicate, overlap, or conflict with the CFPB's proposals under consideration?[22] What challenges or costs would you anticipate in complying with those statutes and regulations (if applicable) and the CFPB's proposals under consideration?

Q2. Are there any relevant statutes or regulations with which you must comply that you are concerned may duplicate, overlap, or conflict with the CFPB's proposals under consideration beyond those described in Appendix C? What challenges or costs would you anticipate in complying with any such statutes or regulations and the CFPB's proposals under consideration?

Q3. What factors disproportionately affecting small entities should the CFPB be aware of when evaluating the proposals under consideration? For example, would a small entity's reliance on a core processor or other service provider affect the costs or burdens associated with any of the proposals under consideration? Would any of the proposals under consideration provide unique benefits to small entities?

Q4. Please provide input on any costs or challenges you foresee with the enforcement or supervision of the proposals under consideration. In particular, please provide input on whether enforcement or supervision of the proposals under consideration may be impractical in certain circumstances and how the CFPB could address those concerns.

A. Coverage of data providers subject to the proposals under consideration

As noted above, the CFPB is considering proposals that, if finalized, would specify rules that would require a defined subset of covered persons that are data providers to make consumer financial information available to a consumer or an authorized third party.[23] Specifically, under the proposals the CFPB is considering, the subset of data providers that would be required to make information available are entities that meet the definition of "financial institution" set forth

[22] Appendix C lists the Electronic Fund Transfer Act (EFTA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Truth in Lending Act (TILA), the Truth in Savings Act (TISA), and the Real Estate Settlement Procedures Act of 1974 (RESPA), and the CFPB's implementing regulations of those statutes.

[23] The term "covered person" is defined at section 1002(6) of the Dodd-Frank Act. *See* 12 U.S.C. 5481(6). The term "authorized third party" is defined in Appendix B to refer to third parties that follow the authorization procedures discussed in part III.B.2 below.

in § 1005.2(i) of the CFPB's Regulation E (12 CFR part 1005) or "card issuer" set forth in § 1026.2(a)(7) of the CFPB's Regulation Z (12 CFR part 1026).

Further, under the CFPB's proposals under consideration a financial institution would be required to make available to a consumer or an authorized third party information that pertains to an "account" as defined in Regulation E § 1005.2(b); and a card issuer would be required to make available to a consumer or an authorized third party information that pertains to a "credit card account under an open-end (not home-secured) consumer credit plan" as defined in Regulation Z § 1026.2(a)(15)(ii).

The CFPB is proceeding to regulate first on these consumer financial products—Regulation E accounts and Regulation Z credit card accounts—because they both implicate payments and transaction data. The CFPB intends to evaluate how to proceed with regard to other data providers in the future. This coverage enables use cases such as transaction underwriting, payment services, comparison shopping for financial products and services that best fit the consumer's deposit and transaction patterns, overdraft and other fee avoidance, and personal financial management. Specifically, these use cases rely on data from consumers' asset and credit card accounts, and this coverage would ensure that consumers are able to provide access to data from these accounts to third parties that provide these products and services. This coverage also addresses some of the most significant areas of potential consumer risk, given the significant potential for abuse of consumers' payment data in particular.[24] At the same time, from the perspective of feasibility of industry implementation, this coverage would leverage, to the greatest extent presently possible, existing industry infrastructure for consumer-authorized financial data sharing.

The remainder of this part III.A discusses in more detail the data provider and consumer financial product coverage of the CFPB's proposals under consideration.

> Q5. Please provide input on the approach the CFPB is considering with respect to the coverage of data providers discussed in this part III.A. What alternative approaches should the CFPB consider? For example, should the CFPB also consider covering payment account providers that are not Regulation E financial institutions as presently defined, such as providers of government benefit accounts used to distribute needs-based benefits programs? Should the CFPB consider covering any providers of credit products that are not Regulation Z credit cards? How could the CFPB clarify coverage of the proposals under consideration?

[24] In October 2021, the CFPB issued a series of orders to collect information on the business practices of large technology companies operating payments systems in the United States. As the CFPB then stated: "Families and businesses benefit from faster, cheaper, and more secure payment systems. As online commerce and electronic payments have become consumers' normal expectation—especially during the pandemic—companies have developed new products and business models to meet this demand. At the same time, these changes present new risks to consumers and to a fair, transparent, and competitive marketplace." *See* Bureau of Consumer Fin. Prot., *CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans* (Oct. 21, 2021), https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-tech-giants-to-turn-over-information-on-their-payment-system-plans/.

1. Financial institutions and card issuers

The proposals under consideration would use two existing definitions to establish coverage over data providers: "financial institution" as defined by Regulation E, and "card issuer" as defined by Regulation Z.

The data providers that would be directly affected by the proposals under consideration include depository and nondepository financial institutions that provide consumer funds-holding accounts or that otherwise meet the Regulation E definition of financial institution. Entities that meet the Regulation E definition of financial institution include the following:

- Banks and credit unions[25] that directly or indirectly hold a consumer asset account (including a prepaid account);
- Other persons that directly or indirectly hold an asset account belonging to a consumer (including a prepaid account); and
- Persons that issue an access device and agree with a consumer to provide electronic fund transfer (EFT) services (including mobile wallets and other electronic payment products).

The data providers that would be directly affected by the proposals under consideration also include depository and nondepository institutions that provide credit cards or otherwise meet the Regulation Z definition of card issuer.[26] Entities that meet the Regulation Z definition of card issuer include persons that issue a credit card and those persons' agents with respect to the card.

In the remainder of this Outline, the CFPB refers to financial institutions and card issuers collectively as "covered data providers."

2. Asset accounts and credit card accounts

Under the proposals the CFPB is considering, a Regulation E financial institution would be a covered data provider with respect to an "account," as that term is defined in Regulation E § 1005.2(b). Under that regulatory provision, an *account* is "a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes."[27] The term includes a prepaid account.[28] In this Outline, the CFPB refers to an "account" as that term is defined in § 1005.2(b) as an "asset account."

The CFPB emphasizes here that a financial institution that does not hold consumer accounts, but that issues access devices,[29] such as by issuing digital credential storage wallets, and provides

[25] Under the SBA size standards, banks and credit unions with assets of $750 million or less are small entities.

[26] *See* 12 CFR 1026.2(a)(7).

[27] *See* 12 CFR 1005.2(b)(1).

[28] *See* 12 CFR 1005.2(b)(3).

[29] *See* 12 CFR 1005.2(a)(1) (defining "access device" as "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers").

EFT services, such as by providing payment services through those digital credential storage wallets, would be a covered data provider with respect to the consumer EFTs that it processes. This would be the case notwithstanding that those EFTs rely on funds in an account held at another financial institution. The types of information that a non-account-holding financial institution would be required to make available to a consumer or an authorized third party are discussed below in part III.C.

Also, under the proposals the CFPB is considering, a Regulation Z card issuer would be a covered data provider with respect to a "credit card account under an open-end (not home-secured) consumer credit plan" as that term is defined in Regulation Z § 1026.2(a)(15)(ii). Under that regulatory provision, a credit card account under an open-end (not home-secured) consumer credit plan is "any open-end credit account that is accessed by a credit card."[30] In this Outline, the CFPB refers to such an account as a "credit card account."

The CFPB emphasizes here that a card issuer that does not hold consumer credit card accounts, but that issues credit cards,[31] such as by issuing digital credential storage wallets, would be a covered data provider with respect to the consumer credit card transactions it processes, notwithstanding that those transactions rely on consumer credit card accounts held at another entity.

In the remainder of this Outline, the CFPB refers to asset accounts and credit card accounts collectively as "covered accounts."

The CFPB recognizes that many covered data providers also provide numerous consumer financial products and services other than covered accounts, such as mortgages, auto loans, closed-end installment loans, etc. These numerous other financial products would not be subject to the CFPB's proposals under consideration.

Part III.C below discusses the types of information that the CFPB's proposals under consideration would require a covered data provider to make available with respect to the covered data provider's covered accounts.

3. Potential exemptions for certain covered data providers

The CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers. However, in determining if exemptions would be appropriate, the CFPB is interested in whether there are ways to design the proposals under consideration to reduce impact on covered data providers. The CFPB seeks to ensure that the proposals under consideration appropriately balance benefits provided to consumers with the burden imposed on covered data providers, including smaller

[30] 12 CFR 1026.2(a)(15)(ii). The term does not include: a home-equity plan subject to the requirements of § 1026.40 that is accessed by a credit card (12 CFR 1026.2(a)(15)(ii)(A)); an overdraft line of credit that is accessed by a debit card (12 CFR 1026.2(a)(15)(ii)(B)); or an overdraft line of credit that is accessed by an account number, except if the account number is a hybrid prepaid-credit card that can access a covered separate credit feature as defined in § 1026.61 (12 CFR 1026.2(a)(15)(ii)(C)).

[31] *See* 12 CFR 1026.2(a)(15)(i) (defining "credit card" as "any card, plate, or other single credit device that may be used from time to time to obtain credit").

covered data providers, in a manner that is consistent with the statutory purposes of the Dodd-Frank Act.

i. Identifying criteria for potential exemptions

The CFPB understands that some of the proposals under consideration, such as a general obligation to make information available to authorized third parties through a data portal (see part III.D.2.i below), may be more burdensome for some covered data providers than others.

> Q6. Should the CFPB exempt certain covered data providers from any particular proposals under consideration? For which covered data providers would such exemptions be appropriate, and why? Which proposals should such data providers be exempt from, and why?
>
> Q7. For third parties: would exempting certain covered data providers negatively impact your organization? For example, if you rely on a core service provider, do you believe an exemption would lead it to offer fewer data access solutions?
>
> Q8. For third parties: would exempting certain covered data providers negatively impact your customers? Would any particular community, such as those you serve, be disproportionately affected by such exemptions?

To the extent exemptions would be appropriate, the CFPB is interested in how to define eligibility criteria. The CFPB seeks to strike a balance between benefitting as many consumers as possible by the proposals under consideration and avoiding undue burden on covered data providers. The CFPB also seeks to develop criteria that would allow a covered data provider to easily determine whether it is exempt.

One approach would be to establish a threshold based on asset size. There are a number of thresholds that are used in other contexts to differentiate financial institutions for various purposes based on asset size, ranging from $750 million (which is used for various purposes under the guidance of the SBA) to $10 billion (which is used for various purposes under the Dodd-Frank Act). Another approach would be to define eligibility based on activity levels, such as the number of accounts at an institution. The CFPB is also considering combining different measures of size and activity to ensure that eligibility for any exemptions is appropriately targeted.

> Q9. Please provide input on whether asset size or activity level would be an appropriate metric for a possible exemption for covered data providers that are depository institutions. If so, what should the asset size or activity level threshold be? What would be an appropriate metric and threshold for a possible exemption for covered data providers that are not depository institutions? What alternative metrics should the CFPB consider?

ii. Transition periods for changes in exemption eligibility

If the CFPB were to exempt certain covered data providers from the proposals under consideration, the CFPB is considering whether and how it should address a situation in which a data provider that previously did not meet the criteria for an exemption later meets the criteria, and a data provider that no longer meets the criteria.[32]

Q10. Please provide input on whether and how the CFPB should address these scenarios, including the amount of time that would be appropriate for a data provider to come into compliance with the rule.

B. Recipients of information

1. Consumers

Section 1033(a) of the Dodd-Frank Act generally requires data providers to make information available to a "consumer." Section 1002(f) defines a consumer as an "individual."[33] In this Outline, the CFPB refers to covered data providers making information available, upon request, directly to a consumer as "direct access."

The CFPB is considering how its proposals under consideration should address a covered data provider's obligation to make information available directly to a consumer when the account is held by multiple consumers, such as an account held jointly by spouses. The CFPB is not considering any proposal that would affect covered data providers' existing obligations to provide information directly to consumers under other Federal consumer financial laws, such as the Electronic Fund Transfer Act (EFTA), the Truth in Savings Act (TISA), and the Truth in Lending Act (TILA), and their implementing regulations. Those regulations generally permit covered data providers to satisfy the relevant information disclosure requirements by providing the information to any one of the consumers on the account.[34] Here, the CFPB is considering proposing that a covered data provider would satisfy its obligation to make information available directly to a consumer by making the information available to the consumer who requested the information or all the consumers on a jointly held account.

Q11. Please provide input on the approach the CFPB is considering with respect to accounts held by multiple consumers. What alternative approaches should the CFPB consider?

[32] The CFPB notes that these types of transition-period issues are addressed in subpart B of Regulation E, which governs remittance transfer providers. *See* § 1005.33(f)(2).

[33] *See* 12 U.S.C. 5481(4).

[34] *See* 12 CFR 1005.4(c), 1030.3(d), 1026.5(d).

2. Third parties

i. Authorization procedures

Section 1033(a) of the Dodd-Frank Act generally requires data providers to make information available to a "consumer," which includes an agent, trustee, or representative acting on behalf of an individual consumer.[35] In this Outline, the CFPB uses "third-party access" to refer to covered data providers making information available, upon request, to authorized third parties.

The CFPB is considering proposals related to authorization procedures for third parties to access consumer information on consumers' behalf. These proposals seek to ensure that such third parties are acting on behalf of the consumer. The proposals under consideration would include a requirement that, in order to access consumer information under the rule, the third party accessing the information would need to: (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information (certification statement). These third party obligations are discussed further below in part III.E.1.

Q12. Please provide input on the approach the CFPB is considering with respect to the authorization procedures, described in greater detail below. What alternative approaches should the CFPB consider? In providing input, please describe the authorization procedures that third parties and/or covered data providers currently employ and the benefits and drawbacks of those procedures in comparison to the procedures the CFPB is considering. What costs would third parties or covered data providers face with respect to the authorization procedures under consideration?

Q13. What alternative approaches should the CFPB consider? Please describe any additional authorization procedures or any suggested changes to the procedures the CFPB is contemplating.

Q14. Where a data recipient relies on a data aggregator to access consumer data from the covered data provider, which authorization procedures and third party obligations should apply to the data recipient, the data aggregator, or both parties? For example, should the data recipient or the data aggregator be responsible for providing the authorization disclosure to the consumer? What obligations, if any, should apply to parties other than a data recipient or an aggregator who receive consumer data?

Q15. How could the CFPB reduce costs and facilitate compliance for small entities? Should the CFPB consider alternative authorization procedures for

[35] *See* 12 U.S.C. 5481(4).

certain categories of third parties? If so, why would such procedures be appropriate?

Q16. Where a covered account is held by more than one consumer, should the rule allow any consumer holding the account to authorize access, or should authorization procedures include a requirement that the third party provide authorization disclosures to and obtain consent from each consumer who is an accountholder?

ii. Authorization disclosure

The proposals under consideration would include a requirement that the third party provide the consumer with an authorization disclosure containing certain key terms of the requested access. The authorization disclosure also would solicit the consumer's consent to those terms of access.

a. Authorization disclosure content

The CFPB is considering proposing that the authorization disclosure would contain key scope and use terms. Key scope terms might include the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access. Key use terms might include the identity of intended data recipients (including any downstream parties) and data aggregators to whom the information may be disclosed, and the purpose for accessing the information. The CFPB is also considering proposing that the authorization disclosure include a reference to the third party's certification statement and solicit consent to access consumer information, as described in part III.B.2.iii and iv.

Q17. Please describe any additional content that should be included in the authorization disclosure or whether there are circumstances in which more limited disclosures would be appropriate. In providing input, please describe the extent to which third parties currently inform consumers about the scope and use of data when obtaining authorization.

Q18. Should the CFPB provide model clauses and/or forms for some or all of the content of the authorization disclosure?

b. Authorization disclosure timing and format

The CFPB is considering proposing that the third party would be required to provide the authorization disclosure close in time to when the third party would need the consumer-authorized information to provide the product or service requested by the consumer. The CFPB is also considering proposing that the third party would be required to provide the authorization disclosure clearly, conspicuously, and segregated from other material.

Q19. Please provide input on whether the CFPB should include any particular requirements or restrictions on the timing and format of the authorization disclosure to prevent the use of potentially misleading practices aimed at soliciting consent, such as a prohibition on pre-populated consent requests.

iii. Consumer consent

The CFPB is considering proposals under which, to be authorized to access consumer information, a third party would be required to obtain consumer consent to the terms described in the authorization disclosure. Specifically, a third party would be required to obtain consent in writing or electronic form, evidenced by the consumer's signature or the electronic equivalent. The CFPB is also considering proposing that a third party would be required to provide consumers a copy of their signed consent, either electronically or through the mail.

Q20. Please provide input on the approach the CFPB is considering with respect to providing consumers a copy of the signed authorization, including input on the costs of such a requirement and whether there are circumstances in which this requirement would not be necessary. What alternative approaches should the CFPB consider?

iv. Certification statement

The CFPB is considering proposals under which, to be authorized to access consumer information, a third party would be required to certify to the consumer that it will abide by certain obligations regarding use, collection, and retention of the consumer's information. Specifically, as discussed further below in part III.E.1, the CFPB is considering proposals related to limits on collection, use, and retention; revocation mechanisms; data security; data accuracy; and certain disclosures. The authorization disclosure would contain a reference, in the form of a link, to a separate statement that describes the third party obligations.

Q21. Please provide input on whether the full certification statement should be included in the authorization disclosure.

C. The types of information a covered data provider would be required to make available

As noted above, Dodd-Frank Act section 1033(a) requires a data provider to make available information "concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."

In turn, Dodd-Frank Act section 1033(b)[36] sets forth four exceptions to the section 1033(a) requirement. Specifically, section 1033(b) states that a data provider may not be required by section 1033 to make available—

- any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
- any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;

[36] Dodd-Frank Act section 1033(b), 124 Stat. 2008 (codified at 12 U.S.C.5533(b)).

- any information required to be kept confidential by any other provision of law; or
- any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

In addition, Dodd-Frank Act section 1033(c)[37] generally states that section 1033 does not impose any duty on a data provider to maintain or keep any information about a consumer.

The following three subsections discuss the CFPB's proposals under consideration with respect to section 1033(a), (b), and (c), respectively.

1. Section 1033(a)—Making information available

Section 1033(a) of the Dodd-Frank Act authorizes the CFPB to require a data provider to make available information in the control or possession of the data provider that concerns the consumer financial product or service that the consumer obtained from the data provider. This part III.C.1 discusses the proposals under consideration that address the information a covered data provider would be required to make available to a consumer or an authorized third party concerning the consumer financial product or service that the consumer obtained from the covered data provider. The proposals under consideration would not affect covered data providers' obligations under existing statutes and regulations—*i.e.*, statutes and regulations other than Dodd-Frank Act section 1033—to make available to consumers the information specified in those existing statutes and regulations.

The following subparts set forth six categories of information the CFPB is considering requiring covered data providers to make available with respect to covered accounts (see part III.A.2 above). The categories are intended to reflect the type and range of information the CFPB is considering. The specific data elements set forth within each of the six categories should not be taken as exhaustive but as representative of the data elements the CFPB is considering.

As described more fully below, the six categories would be:

1. Periodic statement information for settled transactions and deposits (part III.C.1.i);
2. Information regarding prior transactions and deposits that have not yet settled (part III.C.1.ii);
3. Other information about prior transactions not typically shown on periodic statements or portals (part III.C.1.iii);
4. Online banking transactions that the consumer has set up but that have not yet occurred (part III.C.1.iv);
5. Account identity information (part III.C.1.v); and
6. Other information (part III.C.1.vi).

> Q22. Please provide input on the approach the CFPB is considering with respect to these categories of information. What alternative approaches should the CFPB consider? In part III.C.1.vi, the CFPB is seeking feedback on what other

[37] Dodd-Frank Act section 1033(c), 124 Stat. 2008 (codified at 12 U.S.C. 5533(c)).

categories and data elements not identified in the subsections below should be covered.

Q23. Is additional clarity needed with respect to the data elements the CFPB is considering proposing? What further information would be helpful? For example, should the rule set forth all the specific data elements that the rule requires covered data providers to make available?

i. Periodic statement information for settled transactions and deposits

First, the CFPB is considering proposing that covered data providers would need to make available the information with respect to settled transactions and deposits that generally appears on the periodic statements that covered data providers are currently required to provide for asset accounts[38] and for credit card accounts.[39] The data elements in this category include the following—

- For each transfer, the amount, date, and location of the transfer, and the name of the third party (or seller) to or from whom the transfer was made;
- Any fees charged to the account;
- Any interest credited to an asset account or charged to a credit card account;
- The annual percentage yield (APY) of an asset account or the annual percentage rate (APR) of a credit card account;
- The current account balance;[40]
- The account balance at the beginning and at the close of the statement period, as well as, for credit card accounts, upcoming bill information (including whether a payment is overdue or the account is delinquent);
- The terms and conditions of the account, including a schedule of fees that may be charged to the account;[41]

[38] This information is required under Regulation E § 1005.9(b) and under Regulation DD § 1030.6(a). Regulation DD applies to depository institutions except for credit unions. *See* § 1030.1(c). By statute, the National Credit Union Administration (NCUA) Board must prescribe a substantially similar regulation applicable to credit unions which takes into account the unique nature of credit unions and the limitations under which they may pay dividends on member accounts. *See* 12 U.S.C. 4311(b). The NCUA has prescribed such regulations at 12 CFR part 707. The credit union periodic statement disclosures set forth in 12 CFR 707.6(b) are substantially similar to those set forth in 12 CFR 1030.6(a).

[39] This information is required under Regulation Z § 1026.7(b) and 1026.8.

[40] Although the current account balance need not be provided on or with a periodic statement, covered data providers typically make this information available to consumers via the covered data providers' online financial account management portal.

[41] Although account terms and conditions need not be provided on or with a periodic statement, covered data providers are generally required to disclose the terms and conditions of covered accounts. *See, e.g.*, §§ 1005.7 and 1030.4 for the regulatory provisions regarding disclosure of terms and conditions for asset accounts and § 1026.5 and 1026.6 for the regulatory provisions regarding disclosure of terms and conditions for credit card accounts.

- For an asset account, the total dollar amount of all charges for paying overdraft items and for returning items unpaid, both for the statement period and for the calendar year-to-date, as required by Regulation DD § 1030.11(a); and
- For an asset account, the account number as required by Regulation E § 1005.9(b)(2).

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

Second, the CFPB is considering proposing that covered data providers would need to make available information regarding transactions and deposits that have not yet settled. Many covered data providers, through their online financial account management portals, make available to a consumer data about transactions by the consumer that the covered data provider has approved, or agreed to pay, but that have not yet settled. Many covered data providers also make available to a consumer data about deposits to an asset account, or payments to a credit card account, that have not settled or might not be available to the consumer to use.

The data elements within this category of information would be, generally speaking, a subset of the data elements described above that covered data providers make available to consumers on periodic statements. While transactions on the periodic statement have settled and are complete, the data elements about approved but not settled transactions and deposits that the CFPB is considering proposing be made available are typically shown to consumers in the transaction history that covered data providers make available through their online financial account management portals.

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

Third, the CFPB is considering proposing that covered data providers would need to make available information about prior transactions that covered data providers typically do not display on periodic statements or online financial account management portals.

The CFPB understands that, with respect to many transactions displayed on a periodic statement or online financial account management portal, covered data providers receive and retain from the payment networks in which they participate certain data about the transactions that are not reflected on the periodic statement or portal. The payment networks in which a covered data provider would typically participate, and which provide transaction-specific data to the covered data provider, include card networks, ATM networks, automated clearing house (ACH) networks, check-collection networks, and real-time payment networks.

From these payment networks in which they participate, covered data providers typically receive various data elements about each of the payment transactions that each of their consumer accountholders undertakes. For a given payment transaction, the covered data provider in turn reflects some, but not all, of these data elements in the transaction's line-item in the list of transactions on the periodic statement or online financial account management portal. (Those are the data elements at issue in parts III.C.1.i and ii above.) Certain other data elements associated with the given payment transaction, which the covered data provider also receives from the

payment network in which it participates, are not typically reflected on the periodic statement or online financial account management portal.

Many of the data elements covered data providers receive from payment networks, but do not typically make available on periodic statements or online financial account management portals, may be helpful to consumers as they seek to exercise their rights with respect to payments, including fraudulent or otherwise erroneous payments, that may be charged to their accounts. In particular, the data elements that a covered data provider receives from a payment network that are not typically reflected on a periodic statement or online financial account management portal include data elements regarding the interbank routing of a transaction. These data elements might indicate, for example, the bank into which a card, ACH, or check transaction was deposited by a merchant or other payee, such as a fraudster. They might also indicate the name and account number at that bank of the merchant or other payee (such as a fraudster) that deposited the payment transaction. In addition, they might indicate which banks in between the merchant's bank and the consumer's bank handled the transaction.

These types of transaction details may be useful to a consumer or an authorized third party seeking to resolve a dispute with, or recover funds from, a fraudster or the fraudster's bank. Further, recovery of fraudulent, unauthorized, incorrect, or otherwise erroneous transactions, including when such transactions are small in dollar amount, may be especially important to consumers who often have low balances and who may not be able to obtain the formal services of an attorney to assist in recovery. Requiring covered data providers to make these data elements available to consumers and authorized third parties could therefore assist consumers with personal financial management and promote financial inclusion. On the other hand, compelling covered data providers to make this information available could increase privacy risks to consumers.

Q24. Please provide input about the length of time for which covered data providers retain transaction-detail information or can obtain the information from the relevant payment network, such as pursuant to the network's contractual obligations to the covered data provider.

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

Fourth, the CFPB is considering proposing that covered data providers would need to make available information regarding banking transactions a consumer has set up but that have not yet occurred.

Many covered data providers, through their online financial account management portals, enable a consumer to set up, in advance, payments from the account that the consumer wishes to make in the future. For example, a consumer might input into a covered data provider's online financial account management portal 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" or "identification" number with the biller. Further, the consumer might also input into the covered data provider's online financial account management portal information about monthly (or other) bills from the biller for which the consumer would like the

covered data provider to transfer the payment, such as the amounts of the bills and the dates on which the consumer would like payments to be transferred. Moreover, in the days leading up to the date of a payment the consumer has set up and input into the covered data provider's online financial account management portal, the covered data provider might provide notice (*e.g.*, a reminder) to the consumer that the covered data provider will be making the designated payment to the biller and debiting the amount of the payment from the consumer's account.

This type of information about near-future transactions could be useful to a consumer or authorized third party when the consumer, for example, seeks assistance regarding the prevention of overdrafts of the consumer's account. In this example, consumer-authorized access to information about near-future transactions that will be 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 from being assessed against the consumer.

Q25. Please provide input on whether the CFPB should require a covered data provider to make available to a consumer or an authorized third party information about all of the companies, or other payees, for which the consumer has provided information to the covered data provider to make payments to the companies on the consumer's behalf, including information about the consumer's "account" or "identification" number with the companies. What alternatives should the CFPB consider?

v. Account identity information

Fifth, the CFPB is considering proposing that covered data providers would need to make available information related to the identity and characteristics of the consumer accountholder. Specifically, the CFPB understands that covered data providers typically maintain certain identifying information about their consumer accountholders. Such information about a consumer might include the following—

- Name
- Age
- Gender
- Marital status
- Number of dependents
- Race
- Ethnicity
- Citizenship or immigration status
- Veteran status
- Residential address
- Residential phone number
- Mobile phone number
- Email address
- Date of birth
- Social Security number
- Driver's license number

This type of information could be useful to an authorized third party seeking to verify a consumer's ownership of an account with a covered data provider, whether for purposes of an interaction with the covered data provider or with another entity, such as a potential lender. For example, if the authorized third party is seeking to facilitate a loan to the consumer, the authorized third party or the lender may require verification that the consumer owns the account at the covered data provider. However, the CFPB has concerns about fraud, privacy, and other consumer protection risks that could arise through compelling covered data providers to make available this information to authorized third parties. The CFPB also has questions about 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.

The CFPB understands that these risks could be at least somewhat mitigated through a "confirm/deny" approach under which an authorized third party, seeking to verify consumer account ownership, would present to a covered data provider the identity information that the consumer provided to the authorized third party. In turn, the covered data provider, rather than actually provide any account identity information to the authorized third party, could merely confirm or deny that the information presented by the authorized third party matches the information that the covered data provider has on file about the consumer.

Q26. Please provide input about the data security and privacy risks that would result from a requirement that covered data providers make available to authorized third parties the above-described information.

Q27. Please provide input on whether the above-described confirm/deny approach would be feasible to implement and could suffice to achieve the contemplated consumer benefits of authorized third-party access to consumer financial data. Are there alternative approaches that the CFPB should consider?

vi. Other information

In addition to the five categories of information described above, the CFPB is considering proposing that covered data providers would need to make available other information they might have about their consumer accountholders. Specifically, the CFPB is considering proposing that covered data providers would need to make available:

- Consumer reports from consumer reporting agencies, such as credit bureaus, obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer;
- Fees that the covered data provider assesses in connection with its covered accounts;
- Bonuses, rewards, discounts, or other incentives that the covered data provider issues to consumers; and
- Information about security breaches that exposed a consumer's identity or financial information.

Q28. Please provide input on whether the CFPB should require a covered data provider to make available to a consumer or an authorized third party any category of information other than the five categories of information discussed in

part III.C.1 above. Are there any other data elements not described herein that the CFPB should consider proposing?

Q29. What would be the potential costs or challenges of requiring the disclosure of some or all the information outlined in this part III.C.1.vi? How could the CFPB reduce costs and facilitate compliance for small entities?

2. Section 1033(b)—Statutory exceptions to making information available

As noted above, Dodd-Frank Act section 1033(b) sets forth four exceptions to the general section 1033(a) requirement to make information available. Specifically, section 1033(b) states that a data provider may not be required by section 1033 to make available—

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

This part discusses each of these exceptions. As a general matter, the CFPB seeks feedback from the SERs on how these exceptions should affect the CFPB's proposals under consideration regarding the types of information that covered data providers would be required to make available.

Q30. Please provide input on the approach the CFPB is considering with respect to the statutory exceptions to making information available. What alternative approaches should the CFPB consider? Are there specific data elements that should be covered under any of these exceptions? If so, please specify the data element(s) and exception(s).

Q31. What considerations disproportionately affecting small covered data providers should the CFPB be aware of as it seeks to define these exceptions?

i. Section 1033(b)(1)—Confidential commercial information

Dodd-Frank Act section 1033(b)(1) states that a data provider may not be required by section 1033 to make available any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors.

The CFPB is aware that the phrase "confidential commercial information" is used in other legal contexts.[42] The CFPB expects to interpret the meaning of the phrase specifically within the

[42] One such context is the Freedom of Information Act (5 U.S.C. 552).

context of Dodd-Frank Act section 1033. Section 1033 provides the consumer a statutory right to information that consumers could use to obtain a product or service from an entity other than the covered data provider or enable the consumer to better evaluate the consumer's use of a consumer financial product or service from the covered data provider.

The CFPB is considering whether it should propose an interpretation of the phrase "confidential commercial information," identify specific examples of such information, or both.

Q32. How should the CFPB interpret "confidential commercial information"? What existing legal standards, if any, should inform the CFPB's considerations regarding interpreting that term in the context of Dodd-Frank Act section 1033? To what extent should a covered data provider's ownership interest in such information be a factor?

Q33. To what extent are there data elements kept confidential from the consumers to which they pertain? To what extent are there data elements concerning the consumer financial product or service that the consumer obtained that are kept confidential from the consumers to which they pertain?

ii. Section 1033(b)(2)—Information collected for the purpose of preventing fraud or money laundering, or detecting or reporting potentially unlawful conduct

Dodd-Frank Act section 1033(b)(2) states that a data provider may not be required by section 1033 to make available any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct.

The CFPB is aware that covered data providers collect information that can be used to prevent fraud or money laundering or to detect or report potentially unlawful conduct. The CFPB believes, however, that collecting information that can be used in these ways is distinguishable from collecting information *for the purpose of* preventing fraud or money laundering or detecting or reporting potentially unlawful conduct.

The CFPB is considering whether it should interpret "for the purpose of" to generally mean information that a covered data provider actually uses to prevent fraud or money laundering or to detect or report potentially unlawful conduct or that the covered data provider would not have collected but for a legal requirement to collect the information for these purposes. Under this approach, for example, fraud detection parameters, such as higher-risk payee lines of business and combinations of transaction amounts, frequencies, and forms (such as cash or wire transfer) that trigger a covered data provider's heightened scrutiny or reporting obligations, would be subject to the exception; however, the data elements of consumers' transactions—such as their payee, dollar amount, date, time, and location (and so on)—would not be subject to the exception.

Q34. How should the CFPB interpret "for the purpose of"? What existing legal requirements, if any, should inform the CFPB's considerations regarding which

information covered data providers collect for the purpose of preventing fraud or money laundering, or detecting or reporting other unlawful conduct?

iii. Section 1033(b)(3)—Information required to be kept confidential by other law

Dodd-Frank Act section 1033(b)(3) states that a data provider may not be required by section 1033 to make available any information required to be kept confidential by any other provision of law.

The CFPB is aware that covered data providers control or possess information that the law requires them to keep secure from unintentional disclosure or from disclosure to parties that are not authorized to see the information. The CFPB believes that these types of legal requirements to protect and secure information are distinct from a statutory or regulatory requirement to keep information confidential. In addition, Dodd-Frank Act section 1033 is a statutory requirement that a data provider make available to a consumer information that is in the control or possession of the data provider and that concerns a consumer financial product or service that the consumer obtained from the data provider.

The CFPB is considering whether it should interpret "information required to be kept confidential by any other provision of law" to generally mean information subject to a statutory or regulatory requirement to keep the information confidential from the consumer who obtained the consumer financial product or service to which the information pertains. Under this approach, for example, account information that the covered data provider is statutorily required to keep confidential from the consumer (if there is any such information) would be subject to the exception; however, information that the covered data provider must keep confidential from persons *other than* the consumer, but need not keep confidential from the consumer themself, would not be subject to the exception.

Q35. How should the CFPB interpret "kept confidential"? What existing legal requirements, if any, should inform the CFPB's considerations regarding which information covered data providers should be required to keep confidential from consumers?

Q36. What specific "other law(s)" should the CFPB be aware of when interpreting "kept confidential"?

iv. Section 1033(b)(4)—Information that cannot be retrieved in the ordinary course of business

Dodd-Frank Act section 1033(b)(4) states that a data provider may not be required by section 1033 to make available any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

The CFPB is aware that the information covered data providers control or possess is stored in various forms and systems, and that the effort required to retrieve the information varies depending on the form and system in which the information is stored. Further, the CFPB

believes that "ordinary course of business" is a particularly ambiguous phrase capable of being interpreted in many different ways.

Q37. How should the CFPB interpret "ordinary course of business"? What existing legal requirements, if any, should inform the CFPB's considerations regarding which information covered data providers cannot retrieve in the ordinary course of business?

3. Current and historical information

The CFPB is also considering proposals with respect to defining the scope of current and historical information that covered data providers would be required to make available to consumers or authorized third parties, depending on what type of information is requested. The CFPB is considering proposing that a covered data provider would need to make available the most current information that the covered data provider has in its control or possession at the time of a request for current information.

With respect to historical information that may be requested, as noted above, Dodd-Frank Act section 1033(c) states that section 1033 shall not be construed to impose a duty on a data provider to maintain or keep any information about a consumer. In light of section 1033(c), the CFPB is considering proposals under which a covered data provider would be required only to make available information going as far back in time as that covered data provider makes transaction history available directly to consumers, such as, but not limited to,[43] through the covered data provider's online financial account management portal. For example, if when a customer logs on to the covered data provider's website the consumer may retrieve transaction history going back 36 months, then the covered data provider, pursuant to the CFPB's proposals under consideration, would be required to make available to the consumer or the authorized third party 36 months of the consumer's information, if such information were requested.[44]

Q38. Please provide input on the approach the CFPB is considering with respect to making current and historical information available. What alternative approaches should the CFPB consider? Please provide input on whether or how the CFPB should define "current."

[43] As discussed in part III.C.1.iii above, the CFPB understands that, with respect to many transactions displayed on a periodic statement or online financial account management portal, covered data providers receive and retain from the payment networks in which they participate certain data elements about the transactions that are not reflected on the periodic statement or portal. The CFPB is considering proposing that covered data providers would need to make these data elements available going as far back in time as for all the other data elements (discussed in part III.C above) subject to the CFPB's proposals under consideration.

[44] As noted above, for a prepaid account, as an alternative to a periodic statement, Regulation E permits a financial institution to provide a history of account transactions. *See* § 1005.18(c)(1). Where a financial institution chooses that alternative, Regulation E requires the financial institution to make available to a consumer a written history of the consumer's account transactions that covers at least 24 months. *See* § 1005.18(c)(1)(iii).

D. How and when information would need to be made available

In this section, the CFPB addresses proposals under consideration to define the methods and the circumstances in which a covered data provider would need to make information available with respect to direct and third-party access. Section 1033(a) of the Dodd-Frank Act states that a data provider shall make information available in an electronic form usable by consumers. Additionally, section 1033(d) states that "[t]he Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section." This part III.D describes the CFPB's proposals under consideration with respect to the implementation of these statutory provisions, as well as proposals under consideration related to other covered data provider obligations.

1. Direct access

With respect to requests for direct access, the CFPB is considering proposing that a covered data provider would be required to make available information if it has enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested.

The CFPB understands that many covered data providers currently provide their customers online financial account management portals to manage and obtain information about their accounts. Covered data providers typically authenticate the identity of consumers through their username and password, and online financial account management portals are designed to enable consumers to identify the information they are requesting.

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 (see part III.C above) is currently made available through these online financial account management portals. The CFPB is considering proposing that covered data providers would be required to make available all the information that would be covered by the proposals under consideration through online financial account management portals.

The CFPB further understands that many data providers that would be covered by the proposals under consideration currently provide consumers with the option to export account-related information in a number of file formats, including "human readable" and "machine readable" formats. For example, many data providers allow consumers to export a history of their transactions in file formats that present the information in a consumer-friendly display and file formats such that the file could be imported or read into a computer system for further processing (*e.g.*, a .CSV file format). Allowing consumers to export their information in electronic form would allow market participants to create new opportunities to innovate with the information, which would foster competition and help consumers obtain more value from their information. The CFPB is considering proposing that covered data providers would be required to allow consumers to export the information covered by the proposals under consideration in both human and machine readable formats.

Q39. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers if they have enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested. What alternative approaches should the CFPB consider?

Q40. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers through an online financial account management portal and to give consumers the option to export the information in both human and machine readable file formats. What alternatives should the CFPB consider?

Q41. Do covered data providers currently charge consumers specific fees (*i.e.*, fees other than periodic account maintenance fees) to access information through an online financial account management portal or to export information in a human or machine readable format? What would be the impact on covered data providers and consumers if covered data providers were restricted from charging specific fees?

Q42. If there are data elements that covered data providers are not currently making available to a consumer in electronic form through online financial account management portals, please describe any considerations that would weigh against requiring covered data providers to make such data elements available through such portals. For example, are certain types of information the CFPB is considering typically retained in records that are not easily made available in electronic form, such as paper or audio recordings? Are there any other considerations that impact the costs of requiring covered data providers to make such information available in electronic form through online financial account management portals?

Q43. Do covered data providers currently provide consumers with the ability to export account-related information? In what format or formats are consumers able to export account-related information?

Q44. Do covered data providers have policies and procedures in place to ensure that the information currently made available through online financial account management portals is not made inaccurate due to the way the portal operates or the way the information is transmitted to the consumer? If so, please describe these policies and procedures.

In general, the CFPB believes that online financial account management portals would facilitate compliance with the rule by automating the electronic delivery of the information, including the need to authenticate a consumer's identity and define the scope of the information requested. However, to the extent data elements are not generally accessible to a consumer through an online financial account management portal, the CFPB seeks information on alternative means by which covered data providers could satisfy their obligations under the rule. The CFPB understands that making information available through a means other than an online financial

account management portal may be burdensome for a covered data provider if the covered data provider is not permitted to limit the number or scope of requests it receives to make information available.

Q45. Through what channels other than an online financial account management portal do covered data providers make information available electronically to consumers?

Q46. How do covered data providers authenticate a consumer's identity when making information available other than through an online financial account management portal?

Q47. How do covered data providers define the scope of information requested by consumers through channels other than an online financial account management portal? Are there circumstances in which covered data providers encounter overly burdensome requests to make information available electronically? If so, how do covered data providers manage these situations?

The CFPB understands that consumers may be harmed if inaccurate information (*e.g.*, information that is the subject of a dispute that has not been resolved) were to be made available. The CFPB is considering whether covered data providers' obligation to make information available to third parties should apply when the covered data provider knows the information requested is inaccurate.

Q48. Please provide input on the approach the CFPB is considering with respect to whether to require covered data providers to make available information it knows is inaccurate. What alternative approaches should the CFPB consider? Are there circumstances under which the transmission of information that the covered data provider knows is inaccurate could nonetheless be beneficial to a consumer (*e.g.*, to address disputes)?

Q49. Please provide input on whether covered data providers have systems in place to both identify and withhold from transmission inaccurate information. Please provide input on the costs to covered data providers if such a system would need to be developed.

2. Third-party access

i. General obligation to make information available through a data portal

As described in part III.B.2, the CFPB is considering proposing that covered data providers would be required, upon request, to make information available to third parties authorized to access information on a consumer's behalf. The CFPB understands that there are generally two methods through which covered data providers make information available to third parties. One method is through authorized access that uses proprietary software to convert consumer data presented in the provider's online financial account management portal into standardized

machine readable data, generally on an automated basis (screen scraping), using a consumer's credentials. Another method is through a portal based on a data-sharing agreement that third parties can access without possessing or retaining a consumer's credentials. The CFPB also understands that information made available through such third-party access portals is generally structured, organized data.

The CFPB is also considering what role screen scraping should play in the context of a covered data provider's compliance with the rule. However, the CFPB is concerned that screen scraping presents some significant limitations and risks to consumers, data providers, and third parties, including risks related to possession of a consumer's credentials.

Making information available through a third-party access portal that does not rely on an authorized third party possessing or retaining consumer credentials to authenticate the authorized third party could enhance consumer privacy, data security, and data accuracy, and promote the development and use of standardized formats for information.

In light of the above, the CFPB is considering proposing that covered data providers would be required to establish and maintain a third-party portal that does not require the authorized third party to possess or retain consumer credentials. For purposes of this Outline, this is referred to as the CFPB's "third-party access portal proposal" under consideration. Specific aspects of this approach under consideration are described further below.

Q50. Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal. What alternative approaches should the CFPB consider?

Q51. Please provide input on how covered data providers' customers can share their account information with third parties today.

Q52. With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, should the CFPB require that they make information available to authorized third parties before they establish a third-party access portal? Would such a requirement necessitate covered data providers allowing authorized third parties to engage in screen scraping? Are there alternatives to screen scraping that a covered data provider could implement to make information available to authorized third parties in electronic form while establishing a third-party access portal?

Q53. Assuming the CFPB imposes staggered deadlines with respect to a requirement to establish a third-party access portal, please provide input on how the CFPB should do so. For example, how should the CFPB define different classes of covered data providers that would be subject to different implementation periods? Should the CFPB use asset size, activity level, or some other metric? What would be the appropriate thresholds? Would responses to these questions change if data providers relied on screen scraping to comply with an obligation to make information available before they establish a third-party access portal?

Q54. Assuming the CFPB imposes staggered implementation periods with respect to establishing a third-party access portal, please provide input on the appropriate time period that each class of covered data providers should have in order to come into compliance with the third-party access portal proposal under consideration. Would responses to these questions change if covered data providers were permitted to rely on screen scraping to comply with an obligation to make information available to authorized third parties before they establish a third-party access portal?

Q55. Should covered data providers be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption? What records could demonstrate that a service interruption to a third-party access portal has occurred? What alternatives to screen scraping should the CFPB consider to reduce interruptions to authorized third party information access when a third-party access portal experiences a service interruption?

Q56. To the extent screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? For example, should the CFPB require covered data providers to provide access tokens to authorized third parties to use to screen scrape so that third parties would not need a consumer's credentials to access the online financial account management portal? Alternatively, should authorized third parties be restricted from retaining consumer credentials indefinitely? For how long do authorized third parties need to retain consumer credentials? If the answer depends on the use case, please explain.

ii. Data portal requirements

As discussed below, the CFPB is considering various proposals related to the availability of information obtained through third-party access portals, the security of such portals, and the impacts of such portals on the accuracy of information accessed through them. The CFPB is aware that a number of large data providers, data aggregators, and large data recipients have been developing and implementing voluntary standards and guidelines related to third-party access portals. While industry-led standard-setting is a positive development, the CFPB is considering proposing requirements to promote the availability, security, and accuracy of information made available to authorized third parties, including by establishing a general framework under which industry-set standards and guidelines can further develop.

Q57. Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals?

Q58. How can the CFPB incentivize the establishment of industry-led mechanisms and fora through which disputes between ecosystem participants could be surfaced, adjudicated, and otherwise addressed?

a. Availability of information provided through third-party access portals

The CFPB is considering proposals that would regulate the availability of information provided through a third-party access portal described in part III.D.2.i above. Specifically, the CFPB is considering proposing that a covered data provider would not satisfy its obligations under the rule unless its third-party access portal meets certain availability requirements related to the following factors affecting the quality, timeliness, and usability of the information:

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

For the purpose of this Outline, the above factors are collectively referred to as "third party portal availability factors."

Q59. Please provide input on the third-party portal availability factors under consideration. Are there any other factors or alternative approaches the CFPB should consider?

Q60. Should the CFPB articulate similar availability factors with respect to the online management account portal proposal described above in part III.D.1?

The CFPB is considering how to ensure that third party data access portals are reliably available, as defined by the third party portal availability factors. This objective could be achieved by: (1) requiring the establishment and maintenance of reasonable policies and procedures to ensure availability, (2) establishing performance standards related to the third party portal availability factors, (3) prohibiting covered data provider conduct that would adversely affect the third-party portal availability factors, or (4) some combination of (1) through (3).

Q61. Please provide input on specific elements or standards that might be considered under these forms of regulation. For example, are there circumstances in which it would be appropriate for a performance standard to require 100 percent availability? What kind of policies and procedures would reasonably be required to ensure availability of information to authorized third parties?

Q62. Please provide input on whether certain third-party portal availability factors under consideration would be better suited to particular forms of regulation. Are there alternative approaches the CFPB should consider?

Q63. What would be the impact on covered data providers, authorized third parties, and consumers if covered data providers were or were not restricted from charging specific fees under the rule in order to access information through a third-party access portal?

Q64. How would covered data providers demonstrate compliance with performance standards regarding the availability factors under consideration? For example, what would be the costs of reporting information about such compliance to the CFPB and other regulators, as well as potentially to consumers or authorized third parties through a covered data provider's publicly facing website or through periodic third-party audits? Please provide input on alternative ways to demonstrate compliance.

Q65. What considerations disproportionately affecting small covered data providers should the CFPB be aware of as it seeks to determine how to regulate the third-party portal availability factors under consideration?

b. Accuracy of information transmitted through third-party access portals

Consumers could be harmed if the use of a third-party access portal introduces inaccuracies into the information transmitted through a third-party access portal. The CFPB is considering several different approaches to ensure that covered data providers transmit consumer information accurately, as follows: (1) require a covered data provider to implement reasonable policies and procedures to ensure that the transmission of information through the covered data provider's third-party access portal does not introduce inaccuracies; (2) establish performance standards relating to the accurate transmission of consumer information through third-party access portals; (3) prohibit covered data provider conduct that would adversely affect the accurate transmission of consumer information; or (4) require a combination of (1) through (3).

Q66. Please provide input on the approach the CFPB is considering with respect to ensuring that covered data providers transmit consumer information accurately. What alternative approaches should the CFPB consider?

Q67. Please provide input on specific elements or standards that might be considered under these forms of regulation. For example, are there circumstances in which it would be appropriate for a performance standard to require 100 percent accuracy in the transmission of consumer information? What kind of policies and procedures would reasonably be required to ensure accuracy?

Q68. For covered data providers: if you currently maintain a third-party access portal, what policies and procedures do you follow to ensure that the portal does not introduce inaccuracies into the information transmitted through it? What

were the costs associated with developing such policies and procedures? To what extent do existing policies and procedures address consumer disputes relating to the accuracy of information transmitted through third-party access portals, and what would be the costs associated with developing such policies and procedures?

c. Security of third-party access portals

The adequacy of the security of third-party access portals could significantly impact consumer interests related to the privacy and the security of their information and other sensitive information made available through such portals. The CFPB believes that nearly all—if not all—covered data providers must already comply with either the Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act (GLBA),[45] as well as the prohibition against unfair practices.[46] As such, the CFPB is considering not proposing new or additional data security standards with respect to a covered data provider's third-party access portal, other than with respect to the method of authenticating the authorized third party. As noted above in part III.D.2.i, the CFPB is considering a proposal in which the third-party access portal could not rely on an authorized third party possessing or retaining a consumer's credentials to authenticate the authorized third party.

Q69. Please provide input on the approach the CFPB is considering with respect to the security of a covered data provider's third-party access portal. What alternative approaches should the CFPB consider?

Q70. What methods of securely authenticating an authorized third party do not require consumers to share their credentials with the authorized third party? Should the CFPB consider proposals to articulate performance standards related to authentication? If so, how should the CFPB address such topics?

Q71. Are there additional data security requirements the CFPB should consider for third-party access portals that are not addressed by existing data security requirements or guidelines? Should the CFPB affirmatively require covered data providers to maintain procedures related to the authentication and ongoing fraud monitoring related to third-party access portals? What would be the costs associated with implementing these additional requirements?

iii. When covered data providers would be required to make information available to authorized third parties

Section 1033(a) of the Dodd-Frank Act generally provides that a data provider shall make available to a consumer, upon request, information concerning the consumer financial product or service that the consumer obtained from such data provider. As discussed in more detail below,

[45] Public Law 106-102, 138 Stat. 1338 (1999) (codified at 15 U.S.C. 6801 *et seq.*).

[46] *See* Bureau of Consumer Fin. Prot., *Consumer Financial Protection Circular 2022-04* (Aug. 11, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

the CFPB is considering proposing that a covered data provider would be required to make information available to a third party, upon request, when the covered data provider 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. The CFPB is seeking to ensure that third parties that do not meet these conditions are prevented from obtaining access to the information. The CFPB is considering how to address circumstances in which third parties could be prevented from getting access to information where they do not satisfy the conditions.

Q72. Please provide input on what steps the CFPB should take to prevent third parties that do not satisfy the conditions described above from obtaining information. Are there other conditions beyond what is described here that a third party should need to satisfy before a covered data provider is obligated to make information available? Are there circumstances in which third parties should be permitted to access information even if they do not satisfy the conditions the CFPB is considering proposing?

a. Evidence of third party's authority to access information on behalf of a consumer

As discussed in part III.B.2 above, the CFPB is considering proposing that, to be an authorized third party, a third party generally 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 regarding its collection, use, and retention of consumer information accessed under the rule. The CFPB is considering proposing that, where a covered data provider receives evidence that a third party has followed these steps to be authorized to access certain information on behalf of a consumer, a covered data provider generally would be required to make such consumer information available to the third party. Thus, third parties would be prevented from getting access to information where a consumer does not grant authorization or a third party's authorization lapses or is revoked, as discussed in part III.E below.

This proposal under consideration would ensure that covered data providers are only making information available to authorized third parties on the terms described in the authorization disclosure. This proposal under consideration might also reduce fraudulently obtained access. Further, this proposal under consideration would ensure that covered data providers have an objective way of verifying the third party's authority and the scope of information a covered data provider must make available, which could reduce costs to and promote accountability of covered data providers and third parties. Ensuring covered data providers have information necessary to identify the authorized third party would enable covered data providers to facilitate consumer revocation requests if data providers make revocation mechanisms available.

Q73. Please provide input on the approach the CFPB is considering. What alternative approaches should the CFPB consider? Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party? Is there additional information, besides the above-described evidence, that a covered data provider should

receive before a third party should be treated as authorized to access the consumer's information?

Q74. Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before they terminate access.

Q75. To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt (such as by providing consumers a copy of the evidence of authorization submitted by a third party), or be permitted to confirm with the consumer the authorization of a particular third party before making information available? To enable consumers to monitor third-party access to their account information, should covered data providers be required to inform consumers of which third parties are accessing information pursuant to a purported authorization?

b. Information sufficient to identify the scope of the information requested

The CFPB is considering proposing that covered data providers generally would be required to make available information as defined by the scope of the request, in terms of duration, frequency, and types of information, made by the authorized third party.[47] Thus, a covered data provider would be required to make available information on the durational terms and frequency requested by an authorized third party, unless the authorization has been revoked or has lapsed. As described in part III.D.2.i and ii above, the CFPB is considering proposing that a covered data provider would be required to make information available to an authorized third party through a dedicated third-party access portal and adhere to certain third-party data portal requirements. The CFPB believes covered data providers should be able to make information available, subject to such data portal requirements, based on the duration and frequency requested by authorized third parties.

Q76. Please provide input on the approach the CFPB is considering. Are there any alternative approaches the CFPB should consider?

As noted in part III.D.2.i above, the CFPB is considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

Q77. Please provide input on whether covered data providers have the technical capacity to make information available in terms of the frequency and duration sought by authorized third parties through screen scraping, including whether there are considerations particularly relevant to small entities.

[47] As described in part III.E, the CFPB is considering proposing that authorized third parties would be subject to limits on duration and frequency of access based on what is reasonably necessary to provide the product or service requested, subject to a maximum durational period.

Q78. Please provide input on whether covered data providers should be allowed to limit the frequency and duration of authorized third parties' access if covered data providers had to permit screen scraping in order to satisfy their obligations to make information available. How could they do so in a way that both minimizes their costs and does not interfere with a consumer's right to access information?

As discussed in part III.B.2, the CFPB is considering proposing that the authorization disclosure contain key scope terms, including the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access. In general, under the proposals the CFPB is considering, a covered data provider would be required to make available to the authorized third party the types of information requested, as defined in the authorization disclosure, provided the information is covered by the rule. (See also part III.C above.) In some circumstances, however, the scope of information requested by an authorized third party might be ambiguous. Thus, the CFPB is considering a proposal in which a covered data provider could seek to clarify the scope of an authorized third party's request with a consumer where a covered data provider does not have enough information to know how to respond to the request. For example, there might be circumstances in which a covered data provider could seek to clarify whether a consumer intended to consent to share information from particular accounts or particular types of information not specified in the consumer's third-party authorization.

Q79. Please provide input on the proposal the CFPB is considering. What alternative approaches should the CFPB consider?

c. Information sufficient to authenticate the third party's identity

In addition to determining that a third party is authorized to act on behalf of a consumer, a covered data provider may need to have information sufficient to authenticate the third party's identity. The CFPB understands that covered data providers have a legitimate interest in the secure handling and storage of their customers' information. To protect against fraudulent access attempts, the CFPB is considering proposing that a covered data provider would need to make information available to a third party, upon request, when it receives information sufficient to authenticate the identity of the third party, in addition to evidence of authorization (and information needed to identify the scope of information requested).

Q80. Please provide input on the approach the CFPB is considering with respect to authenticating the identity of the authorized third party. What alternative approaches should the CFPB consider? Is there other information that covered data providers might need before being obligated to make information available to a third party?

Q81. Please provide input on whether it would facilitate compliance or reduce costs to covered data providers and authorized third parties if covered data providers were required to follow certain specific procedures in authenticating an authorized third party's identity. Please provide input on what models the CFPB

could look to for prescribing such procedures. Do all covered data providers require a uniform set of information to authenticate an authorized third party's identity prior to making information available to the authorized third party?

iv. Issues related to data accuracy

Section 1033(a) of the Dodd-Frank Act generally requires covered data providers to make available information in their control or possession concerning the consumer financial product or service that the consumer obtained from such data provider, and that such information be made available in an electronic form usable by consumers. As described above in part III.D.2.ii.b, the CFPB is considering several different approaches to ensure that covered data providers transmit consumer information accurately. However, consumers may be harmed if information known to be inaccurate by the covered data provider were to be made available to authorized third parties, even if the third-party access portal does not introduce the inaccuracy. The CFPB is considering whether covered data providers should be required to make information available to third parties when the covered data provider knows the information requested is inaccurate.

Q82. Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate?

Q83. Do covered data providers have systems in place that have the capability to both identify information as inaccurate and then withhold such inaccurate information from transmission to an authorized third party? Please provide input on costs to covered data providers if such a system would need to be developed.

Q84. Are there circumstances under which the transmission to an authorized third party of information that the covered data provider knows is inaccurate could nonetheless be beneficial to a consumer (*e.g.*, to address disputes)?

3. Certain other covered data provider disclosure obligations

Section 1033(b) of the Dodd-Frank Act provides that covered data providers are not required to make information available under certain circumstances. The CFPB understands that there are concerns that some covered data providers might seek to use the exceptions in section 1033(b) as a pretext to not make information available to consumers or authorized third parties. The CFPB is considering whether it should require covered data providers to disclose to consumers or authorized third parties the reason information is not available pursuant to the section 1033(b) exceptions.

In addition, the CFPB is considering whether covered data providers should be required to disclose to consumers or third parties why access is prevented for reasons other than the section 1033(b) exceptions, including, for example, when a covered data provider lacks information described in part III.D.2.iii above (*e.g.*, evidence of the third party's authority or information needed to authenticate the third party's identity).

Q85. With respect to disclosing why access is prevented, should covered data providers be required to provide disclosures to third parties, consumers, or both? Does the answer depend on the reason access is prevented?

Q86. Please provide input on whether it would facilitate compliance or reduce costs to covered data providers if, rather than prescribe disclosures, they were required to implement reasonable policies and procedures with respect to explaining why information is withheld.

The CFPB is also considering whether and how covered data providers should be required to inform consumers of the rights afforded to them under the rule.

Q87. Please provide input on whether and how covered data providers should inform consumers of rights afforded to them pursuant to the rule.

E. Third party obligations

The CFPB is considering proposals under which third parties accessing consumer-authorized information would have certain obligations related to collection, use, and retention of that information. This section describes those third party obligations. The CFPB is requesting feedback on whether those obligations should apply to the data recipient, the data aggregator, or both parties in circumstances where a data recipient relies on a data aggregator to access the consumer's information.

1. Limiting the collection, use, and retention of consumer-authorized information

The CFPB is considering proposals under which third parties accessing consumer-authorized information would have to limit their collection, use, and retention of that information. The proposals under consideration would include collection limitations related to the duration and frequency of information accessed pursuant to consumer authorization, including requiring that authorized third parties provide consumers a simple way to revoke access. The proposals under consideration would also include limitations on uses of consumer-authorized information. Finally, the proposals under consideration would also include deletion requirements and limitations on retention of consumer-authorized information.

i. General limit on collection, use, and retention

This part III.E.1 describes proposals the CFPB is considering that would limit authorized third parties' collection, use, and retention of consumer information. Authorized third parties would not be permitted to collect, use, or retain consumer information beyond what is reasonably necessary to provide the product or service the consumer has requested (the limitation standard). This limitation standard would be aimed at reducing the risks of over-collection and retention of sensitive information, including risks associated with breaches of retained information, while allowing for uses of information needed to provide consumers with the products and services that

they requested. The standard also would be consistent with various State and international privacy regimes.[48]

Q88. Please provide input on the approach the CFPB is considering to limit third party collection, use, and retention of consumer-authorized information to what is reasonably necessary to provide the requested product or service. What alternative standards should the CFPB consider? In providing this input, please describe any guidance the CFPB should consider to clarify the applicability of the standard or any alternative standards the CFPB should consider.

ii. Limits on collection

The CFPB is considering proposals to limit authorized third parties' collection of consumer information to what is reasonably necessary to provide the product or service the consumer has requested. These proposals would include limitations on duration and frequency of information access and would also include requiring that third parties provide consumers a simple way to revoke a third party's authorization to access consumer information.

Q89. Please provide input on whether additional collection limitations are needed for potentially sensitive information that might cause particular harm to consumers if exposed (such as Social Security numbers). In providing this input, please explain why the general limitation standard described above is not sufficient for specific types of sensitive information.

Q90. If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties (see part III.D.2.i above), how would third parties using screen scraping comply with limits on collection? Would third parties employ filters or other technical solutions to limit collection?

a. Duration and frequency of third-party access

The CFPB is considering proposing that authorized third parties would be limited to accessing consumer-authorized information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. The CFPB is also considering proposing that the authorized duration would be limited to a maximum period, after which third parties would need to seek reauthorization for continued access. These proposals would seek to ensure the third party is not accessing information beyond what the consumer intended to authorize and ensure that third parties do not continue to access information for a product or service that the consumer no longer uses. Limiting duration and frequency in this way could ensure access for a variety of consumer-requested use cases and protect consumers from risks related to open-ended access.

[48] *See, e.g.*, Commission Regulation 2016/679 art. 5, General Data Protection Regulation, 2016 O.J. (L 119); Virginia Consumer Privacy Act, Va. Code Ann. § 59.1-578 § § A.1, 2 (effective Jan. 1, 2023); Colorado Privacy Act, Colo. Rev. Stat. § 59.1-578 § § A.1, A.2 (effective July 1, 2023).

Q91. Please provide input on the approach the CFPB is considering to limit duration and frequency according to what is reasonably necessary to provide the product or service the consumer has requested. What alternative approaches should the CFPB consider? How could the CFPB reduce costs and facilitate compliance for small entities?

Q92. Please provide input on the approach the CFPB is considering that would establish a maximum durational period for all use cases, along with any alternative approaches the CFPB should consider. Please provide input on the length of the maximum durational period, including whether certain use cases should have shorter or longer maximum durational periods.

Q93. If the rule were to require third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties? For example, should the CFPB consider proposals that would allow authorized third parties to:

- Seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses?
- Establish a presumption of reauthorization, subject to a consumer's ability to opt out of the presumption, based on the consumer's recent use of a product or service? If so, what should be considered "recent" use?
- Require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers?

b. Revoking third-party authorization

The CFPB is considering proposing that authorized third parties would be required to provide consumers with a simple way to revoke authorization at any point, consistent with the consumer's mode of authorization. For the purposes of this Outline, "revocation" is the mechanism by which the consumer withdraws consent from third parties they previously authorized to access their information. This proposal under consideration would seek to ensure that a consumer's consent is effective and meaningful.

Q94. Please provide input on the approach the CFPB is considering that would require authorized third parties to provide consumers with a mechanism through which they may revoke the third-party's access to their information. Please provide input on the costs associated with providing consumers a revocation mechanism. Please provide input on any alternative approaches the CFPB should consider, and how the CFPB could reduce costs and facilitate compliance for small entities.

Q95. Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization, and the costs and benefits of such an approach. Is it feasible to require covered data providers to provide revocation mechanisms where screen scraping is used?

Q96. Please provide input on whether authorized third parties should be required to report consumer revocation requests to covered data providers. What would be the challenges or costs anticipated from such a requirement?

Q97. How should the CFPB address consumers' potential desire to revoke access for certain, but not all, use cases, such as when the consumer might consent to two separate use cases but later want to revoke third-party access related to only one of those use cases? What would be the challenges or costs anticipated from such a requirement on third parties?

iii. Limits on secondary use of consumer-authorized information

The CFPB is considering proposals that would limit third parties' secondary use of consumer-authorized information. The CFPB is considering defining secondary use to mean a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including the third party's own use of consumer data and the sharing of data with downstream entities. The CFPB is considering various approaches to limiting third parties' secondary use of consumer-authorized information. General approaches the CFPB is considering include prohibiting (1) all secondary uses; (2) certain high risk secondary uses; (3) any secondary uses unless the consumer opts into those uses; and (4) any secondary use if the consumer opts out of those uses.

Q98. Please provide input on the standard the CFPB is considering for defining secondary use of consumer-authorized information. In providing this input, please describe any guidance the CFPB should consider to clarify the applicability of the standard to particular uses or any alternative standards the CFPB should consider.

Q99. Please provide input on the various approaches the CFPB is considering to limit third parties' secondary use of consumer-authorized information and any alternative approaches the CFPB should consider. For example:

- What specific protections could be included in an opt-in or opt-out approach to ensure that consumers are informed about their choices and the corresponding risks in a way that balances costs for third parties? Should the rule include requirements or restrictions on the timing and format of opt-in or opt-out requests to prevent the use of potentially misleading practices aimed at soliciting the consumer's consent, such as a prohibition on pre-populated opt-in requests?

- How could the CFPB design such approaches to facilitate compliance by small entities? Should the CFPB propose to include a standard for defining "high risk," or provide a specific list of uses that it deems to be "high risk," or both?

Q100. Please provide input on whether the rule should include a prohibition on third parties' use of consumer-authorized information that is not otherwise necessary to obtain the product or service requested by the consumer. Please provide input on the costs and benefits of that approach.

Q101. For third parties: please describe your current practices for using consumer-authorized information in ways that are not reasonably necessary to provide the consumer's requested product or service. Please describe your reasons for doing so.

Q102. Please provide input on whether the rule should allow consumer information that has been de-identified to be used by third parties beyond what is reasonably necessary to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"?

iv. Limits on retention

The CFPB is considering proposing that authorized third parties would be obligated to limit their retention of consumer-authorized information. Specifically, the CFPB is considering a proposal in which authorized third parties would be obligated to delete consumer information that is no longer reasonably necessary to provide the consumer's requested product or service, or upon the consumer's revocation of the third-party's authorization. The CFPB is also considering a limited exception to the deletion requirements for compliance with other laws. For the purposes of this Outline, "deletion" is the complete removal of previously collected consumer information. These proposals under consideration would seek to ensure authorized third parties do not retain information beyond what the consumer intended to authorize.

Q103. Please provide input on the approach the CFPB is considering that would require authorized third parties to delete consumer information that is no longer reasonably necessary for providing the consumer's requested product or service, the costs associated with this approach, and any potential alternatives the CFPB should consider. How could the CFPB reduce costs and facilitate compliance for small entities?

Q104. Should an authorized third party be required to delete consumer information upon receipt of the consumer's revocation request? Under what circumstances should an authorized third party be allowed to retain consumer information beyond receipt of the consumer's revocation request? For example, is retention of data after receipt of a revocation request necessary for compliance with other laws and regulations?

Q105. If retention is required to comply with other laws, should authorized third parties be required to disclose to consumers that the consumer-authorized information is being retained?

Q106. Should an authorized third party be permitted to ask consumers for permission to retain consumer-authorized information after receipt of a revocation request, and for what reasons?

Q107. Are there any use cases or services for which consumers might seek deletion of some consumer-authorized information that the authorized third party collected, but not want to revoke that third party's ongoing access to their information from a covered data provider?

Q108. Should deletion of consumer-authorized information be required when authorization lapses at the end of a durational period?

Q109. If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties (see part III.D.2.i above), what deletion requirements should be imposed on authorized third parties that utilize screen scraping and potentially collect more information than what is reasonably necessary to provide the product or service?

Q110. Should the CFPB consider more flexibilities related to retention beyond an exception for compliance with other laws? For example, should the CFPB consider allowing authorized third parties to retain de-identified consumer information? For what purposes might authorized third parties seek to retain de-identified consumer information, and by what standards should consumer information be de-identified?

2. Data security

The CFPB is considering a proposal to require authorized third parties to implement data security standards to prevent authorized third parties from exposing consumers to harms arising from inadequate data security.

The GLBA safeguards framework, implemented by the FTC in its Safeguards Rule and by the prudential regulators in the Safeguards Guidelines, applies to many types of financial institutions participating in the consumer-authorized financial data ecosystem.[49] The safeguards framework generally requires financial institutions to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institution's activities, and the sensitivity of the customer information at issue. These safeguards must include specific elements set forth in the regulations.

The CFPB believes that nearly all—if not all—covered data providers are subject to the GLBA safeguards framework. Although the CFPB believes authorized third parties that seek to access consumer-authorized information are also likely subject to this framework, the CFPB is

[49] 16 CFR part 314 (FTC Safeguards Rule); 12 CFR part 30, App. B (OCC Safeguards Guidelines); 12 CFR part 208, App. D-2 (Federal Reserve Board Safeguards Guidelines); 12 CFR part 364, App. B (FDIC Safeguards Guidelines); 12 CFR part 748, App. B (NCUA Safeguards Guidelines). The Securities and Exchange Commission and the Commodity Futures Trading Commission also have issued rules implementing GLBA data security standards with respect to the entities under their jurisdiction. *See* 17 CFR 248.30 and 17 CFR part 160. The safeguards framework is also described in Appendices B and C.

considering whether it should impose specific data security standards on authorized third parties under the rule.

General approaches the CFPB is considering include:

- Requiring authorized third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third party's size and complexity, and the volume and sensitivity of the consumer information at issue. This approach could be combined with a provision incorporating the Safeguards Rule or Safeguards Guidelines as a specific option for complying with any data security requirement under the CFPB's rule.
- Alternatively, requiring compliance with the Safeguards Rule or Safeguards Guidelines.

Q111. Please provide input on the approach the CFPB is considering regarding data security. What alternative approaches should the CFPB consider? Would a general requirement to develop, implement, and maintain a comprehensive written data security program appropriate to a third party's size and complexity, and the volume and sensitivity of the consumer information at issue, provide sufficient guidance? How could the CFPB reduce costs and facilitate compliance for small entities?

Q112. For third parties: what data security practices do you currently apply to consumer data? Do you tailor your information security approach to an existing legal or industry standard, such as the safeguards framework, and if so, which one(s)? Would you follow the Safeguards Rule or the Safeguards Guidelines if either were incorporated as an option for complying with any data security requirement under the CFPB's rule? Are there alternative data security standards that you believe adequately address data security, and how would implementation costs compare?

3. Data accuracy and dispute resolution

The CFPB is considering proposals related to data accuracy and dispute resolution. Authorized third parties could harm consumers if they collect or use inaccurate data in the course of providing the product or service the consumer has requested. Existing laws and regulations aim to protect against many of the most serious harms resulting from inaccurate data. Most notably, where applicable, FCRA and Regulation V impose accuracy requirements on the information furnished to and provided by consumer reporting agencies, EFTA and Regulation E protect consumers against unauthorized electronic fund transfers and other errors, and TILA and Regulation Z, and RESPA and Regulation X protect consumers against certain billing and servicing errors. But outside of specific contexts, no law creates general accuracy requirements regarding the collection of data by authorized third parties.[50] The CFPB is considering a

[50] At the Federal level, the United States takes a sectoral approach to privacy laws, and therefore has no general data privacy statute. General data privacy laws have been enacted in California, Colorado, and Virginia that give consumers the right to correct inaccurate personal information. *See* Cal. Civ. Code 1798.100(c) (effective Jan. 1, 2023); Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 (effective July 1, 2023); Virginia Consumer Privacy Act,

proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the information that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers.

Q113. Please provide input on the approach the CFPB is considering regarding data accuracy and dispute resolution. What alternative approaches should the CFPB consider? How could the CFPB reduce costs and facilitate compliance for small entities?

Q114. As an authorized third party, how do you currently resolve errors in consumer-authorized information, both when information is accessed through screen scraping and formal data-sharing agreements?

Q115. Are inaccuracies in consumer-authorized information used by authorized third parties more likely to come from errors in data made available by covered data providers or from errors in any manipulation, calculation, or subsequent transmission performed by authorized third parties? Could third-party policies and procedures address errors in data that were inaccurate when originally accessed from a covered data provider?

Q116. Should policies and procedures to ensure accuracy include addressing disputes submitted by consumers? When does addressing such disputes require an investigation and a response to the consumer?

4. Disclosures related to third party obligations

The CFPB is considering proposals related to disclosure requirements applicable to authorized third parties to enable consumers to make informed decisions about the ongoing collection, use, and retention of consumer-authorized information. For example, the CFPB is considering proposals that would require authorized third parties to periodically remind consumers how to revoke authorization. The CFPB is also considering proposing that authorized third parties would need to provide consumers with a mechanism to request information about the extent and purposes of the authorized third party's access. These disclosures, at a time prescribed by the rule or upon consumer request, could provide essential information while potentially avoiding negative impacts associated with numerous and irrelevant disclosures.

Q117. Please provide input on the approach the CFPB is considering with respect to periodic disclosures regarding an authorized third party's access to consumer information. What alternative approaches should the CFPB consider? What would be the costs associated with potential disclosures? How could the CFPB reduce costs and facilitate compliance for small entities?

Va. Code Ann. § 59.1-578 (effective Jan. 1, 2023). But Colorado and Virginia exempt financial institutions subject to the GLBA, while California exempts information subject to the GLBA.

Q118. What kinds of required disclosures, and at what points in time during authorized access, would be most helpful and effective for consumers? How could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties associated with irrelevant or unhelpful disclosures? For example, should the CFPB consider proposals related to:

- Timing and content requirements for key information to be shared with consumers?
- Periodic reminders of data-access terms, such as revocation?
- Disclosure requirements for covered data providers?

F. Record retention obligations

The CFPB is considering proposing record retention requirements for covered data providers and authorized third parties to demonstrate compliance with certain requirements of the rule. A record retention requirement would assist with the CFPB's ability to monitor compliance with the rule and therefore better protect consumers. A record retention requirement could also assist entities in assessing their compliance with the rule. The CFPB recognizes that imposing a record retention requirement would likely increase burden on covered data providers and authorized third parties (relative to how such entities currently operate).

Q119. Please provide input on the approach the CFPB is considering regarding a record retention requirement, along with any alternative approaches the CFPB should consider. Please provide input about the costs to covered data providers and authorized third parties that would be associated with such a requirement. What types of records would be relevant in assessing whether a data provider or authorized third party was complying with the rule? How could the CFPB reduce costs and facilitate compliance for small entities?

Q120. Should covered data providers and authorized third parties be required to maintain policies and procedures to comply with their obligations under the rule, beyond the areas already identified in this Outline? What costs would be associated with maintaining policies and procedures?

G. Implementation period

The CFPB seeks to ensure that consumers have the benefit of a final rule within a short timeframe, while also seeking to ensure that covered data providers and authorized third parties have sufficient time to implement the rule. As such, the CFPB is considering the proper implementation period for complying with the rule. As discussed above in part III.D.2.i, the CFPB is seeking feedback on whether certain covered data providers should not be subject to the third-party access portal requirement on the rule's compliance date and instead should be given additional time to build a compliant third-party access portal.

In order to assist industry with an efficient and effective implementation of the rule, the CFPB intends to provide guidance in the form of plain language compliance guides and aids, and by conducting meetings with stakeholders to discuss the rule and implementation issues.

Q121. Please provide input on an appropriate implementation period for complying with a final rule, other than the potential third-party access portal requirement.[51] What alternative approaches should the CFPB consider? Are there any aspects of the CFPB's proposals under consideration that could be particularly time consuming or costly for a covered data provider or a third party to implement? Are there any factors outside a covered data provider or authorized third party's control that would affect its ability to prepare for compliance?

Q122. The CFPB recognizes that small covered data providers and authorized third parties might not be able to comply with some of the proposals under consideration on the same timeframe as larger covered data providers and third parties. How much time would small entities need to implement the proposals under consideration, other than the third-party access portal proposal,[52] including updating policies, procedures, processes, and employee training programs?

IV. Potential Impacts on Small Entities

A. Overview

The RFA generally requires Federal agencies to consider the economic impact that rules will have on small entities.[53] In order to estimate the potential impact of the rule on small entities, the CFPB needs to ascertain the number of small entities that would be affected by the proposals under consideration and the costs that those entities would incur to comply with the proposals. Computing the number of affected small entities requires knowing the extent to which small entities would be affected by the proposals under consideration.

This part summarizes the CFPB's preliminary assessment of the impacts of the regulatory and operational proposals under consideration on affected small entities and the methods used to derive its assessment. The CFPB believes that this information will make it easier for SERs and others to offer the CFPB additional data and information regarding potential impacts. The CFPB encourages contributions of data and other factual information to inform its assessment of potential compliance costs and other impacts on small entities.

Part IV.B discusses which small entities may be covered by the proposals under consideration. Part IV.C reviews new compliance processes and costs associated with implementing the proposals under consideration. Part IV.D discusses additional impacts of the proposals under consideration. Part IV.E concludes with the impact on the cost and availability of credit to small entities.

[51] See part III.D.2.i above for questions about the implementation period with respect to the potential third-party access portal requirement.

[52] See the questions in part III.D.2.i above.

[53] 5 U.S.C. 601 *et seq.*

Generally, several types of small entities may be affected by the proposals under consideration. First, the CFPB estimates that over 8,000 small covered data providers are likely to be affected, including most small depositories and some nondepository institutions that meet the definition of covered data provider. Part IV.B details the relevant asset and revenue thresholds that define small entities by industry. The CFPB can reliably estimate the number of small depository institutions that would be covered data providers but lacks data on the number of small nondepositories that would be covered data providers. Second, small data recipients would be affected to varying degrees by the proposals under consideration. These include, for example, entities that use consumer-authorized information to underwrite loans, offer budgeting or personal financial management services, facilitate payments, and offer other services. Additionally, though fewer in number, small entities in the data aggregation business would also be affected by the proposals under consideration. Given the extent of available data, the CFPB is not able to reliably ascertain the total number of small entities that would be data recipients or data aggregators but expects that thousands of small entities likely meet the definition of "data recipient," plus a smaller number of small data aggregators. The CFPB also lacks data and information to quantify costs associated with complying with the proposals, and how much costs would vary across these small entities. The CFPB seeks feedback and information from the SERs about how proposals under consideration may change one-time and associated ongoing costs.

The CFPB's preliminary qualitative assessment is that the options under consideration would impact small entities via one-time costs and ongoing costs, as described below. The CFPB encourages contributions of data and other matters of fact to inform its assessment of potential compliance costs and other impacts on small entities. Specifically, the CFPB seeks feedback and information, including supporting data, from SERs on the questions in parts IV.C and IV.D below.

B. Small entities covered by the proposals under consideration

This part aims to quantify the number of small entities that may be affected by the proposals under consideration. Doing so requires determining whether an entity would be affected and whether it is small. First, potentially affected entities can be classified as data providers, data aggregators, and data recipients. At the same time, as noted in part I above, an entity could be both a data provider and a data recipient. Second, the CFPB adopts the SBA's industry-specific size standards for determining which entities are "small."

This part identifies industries of the entities that may be affected. Within each affected industry, this part estimates the number and share of entities that are small. The SBA classifies depository institutions[54] as small based on assets. With a single exception,[55] the SBA uses revenue thresholds for all other potentially affected industries. The CFPB estimates the number of small depositories using asset data from the Federal Financial Institutions Examination Council (FFIEC) and National Credit Union Administration (NCUA) Consolidated Reports of Condition

[54] The 2022 four-digit NAICS code for institutions in the "Depository Credit Intermediation" industry is 5221.

[55] Entities in the "Credit Card Issuing Non-Depository Credit Intermediation" industry are small according to an asset threshold.

and Income (Call Reports). The CFPB estimates the number of other potentially affected small entities using revenue information from summary tables derived from the 2017 Economic Census.

Covered data providers are primarily, but not exclusively, depository institutions. According to the SBA's criteria, entities in the "Depository Credit Intermediation" industry are small if they have less than $750 million in assets. The CFPB estimates that 82 percent of such entities are small.

Nondepository financial institutions and entities outside of the financial industry may also be affected if they are data providers, data recipients, or data aggregators. "Credit Card Issuing Non-Depositories"[56] are also considered small if they have less than $750 million in assets. However, the CFPB does not have asset data to quantify the number or share of such entities. Other nondepository financial institutions are subject to revenue criteria that vary by industry. The other types of nondepository financial institutions potentially affected by a rule include industries within Non-Depository Credit Intermediation,[57] Activities Related to Credit Intermediation,[58] and Securities and Commodity Contracts Intermediation and Brokerage,[59] though it is important to note that entities within these industries would only be subject to the proposals under consideration if they meet the definitions of data provider, data recipient, or data aggregator. Within those financial industry categories, the specific industries potentially affected include:

- Sales Financing companies;[60]
- Consumer Lending companies;[61]
- Real Estate Credit companies;[62]
- Financial Transactions Processing, Reserve, and Clearinghouse Activities;[63]
- Other Activities Related to Credit Intermediation;[64]
- Investment Banking and Securities Dealing;[65]

[56] The 2022 six-digit NAICS code for institutions in the "Credit Card Issuing Non-Depository Credit Intermediation" industry is 522220.

[57] The 2022 four-digit NAICS code for institutions in "Non-Depository Credit Intermediation" is 5222.

[58] The 2022 four-digit NAICS code for institutions in "Activities Related to Credit Intermediation" is 5223.

[59] The 2022 four-digit NAICS code for institutions in "Securities and Commodity Contracts Intermediation and Brokerage" is 5231.

[60] The 2022 six-digit NAICS code for institutions in the "Sales Financing" industry is 522220.

[61] The 2022 six-digit NAICS code for institutions in the "Consumer Lending" industry is 522291.

[62] The 2022 six-digit NAICS code for institutions in the "Real Estate Credit" industry is 522292.

[63] The 2022 six-digit NAICS code for institutions in the "Financial Transactions Processing, Reserve, and Clearinghouse Activities" industry is 522320.

[64] The 2022 six-digit NAICS code for institutions in "Other Activities Related to Credit Intermediation" is 522390.

[65] The 2022 six-digit NAICS code for institutions in the "Investment Banking and Securities Dealing" industry is 523110.

- Securities Brokerage;[66] and
- Commodities Contracts Brokerage.[67]

Across the industries described above, approximately 94 percent of entities are small (Table 1).

Potentially affected entities outside of the financial industry include:

- Software Publishers;[68]
- Data Processing, Hosting, and Related Services;[69]
- Payroll Services;[70]
- Custom Computer Programming Services;[71] and
- Credit Bureaus.[72]

Across these industries, approximately 96 percent of entities are small. Table 1 summarizes the number and share of entities across industries.

Table 1: Number and share of potentially affected entities

	Number of Entities	Percent of Entities
A. Small Depository Firms		
Commercial Banking (522110) and Savings Institutions (522120)	4,845	
< $750M (Assets)	3,581	73.9%
Credit Unions (522130)	4,976	
< $750M (Assets)	4,447	89.4%
B. Small Nondepository Firms		
Software Publishers (511210)	10,014	
< $40M (Revenue)	9,395	93.8%
< $50M (Revenue)	9,461	94.5%
Data Processing, Hosting, and Related Services (518210)	10,860	
< $35M (Revenue)	9,868	90.9%
Sales Financing (522220)	2,367	
< $40 M (Revenue)	2,112	89.2%

[66] The 2022 six-digit NAICS code for institutions in the "Securities Brokerage" industry is 523120.

[67] The 2022 six-digit NAICS code for institutions in the "Commodities Contracts Brokerage" industry is 523140.

[68] The 2022 six-digit NAICS code for institutions in the "Software Publishers" industry is 511210.

[69] The 2022 six-digit NAICS code for institutions in the "Data Processing, Hosting, and Related Services" industry is 518210.

[70] The 2022 six-digit NAICS code for institutions in the "Payroll Services" industry is 541214.

[71] The 2022 six-digit NAICS code for institutions in the "Custom Computer Programming Services" industry is 541511.

[72] The 2022 six-digit NAICS code for institutions in the "Credit Bureaus" industry is 561450.

	Number of Entities	Percent of Entities
< $50 M (Revenue)	2,124	89.7%
Consumer Lending (522291)	3,037	
< $40 M (Revenue)	2,905	95.7%
< $50 M (Revenue)	2,915	96.0%
Real Estate Credit (522292)	3,289	
< $40 M (Revenue)	2,872	87.3%
< $50 M (Revenue)	2,904	88.3%
Financial Transactions Processing, Reserve, and Clearinghouse Activities (522320)	3,068	
< $40 M (Revenue)	2,916	95.0%
< $50 M (Revenue)	2,928	95.4%
Other Activities Related to Credit Intermediation (522390)	3,772	
< $20 M (Revenue)	3,595	95.3%
< $25 M (Revenue)	3,610	95.7%
Investment Banking and Securities Dealing (523110)	2,394	
< $40 M (Revenue)	2,214	92.5%
< $50 M (Revenue)	2,227	93.0%
Securities Brokerage (523120)	6,919	
< $40 M (Revenue)	6,703	96.9%
< $50 M (Revenue)	6,717	97.1%
Commodities Contracts Brokerage (523140)	856	
< $40 M (Revenue)	825	96.4%
< $50 M (Revenue)	829	96.8%
Payroll Services (541214)	4,328	
< $30 M (Revenue)	4,097	94.7%
< $35 M (Revenue)	4,111	95.0%
Custom Computer Programming Services (541511)	62,205	
< $30 M (Revenue)	60,959	98.0%
Credit Bureaus (561450)	301	
< $35 M (Revenue)	279	92.7%
< $75 M (Revenue)	283	94.0%

Sources: Panel A: CFPB calculations based on March 2022 credit union and bank Call Report data. Panel B: U.S. Census Bureau, 2017 Economic Census, *The Number of Firms and Establishments, Employment, Annual Payroll, and Receipts by Industry and Enterprise Receipts Size: 2017* (May 28, 2021), https://www2.census.gov/programs-surveys/susb/tables/2017/us_6digitnaics_rcptsize_2017.xlsx. The tabulations and shares were computed according to available enterprise size cells.

Notably, not all entities within an industry may be affected by the rule. The CFPB is not able to estimate with precision what share of entities within an industry would be covered data providers, data aggregators, or data recipients. Nor is it able to estimate the share that would be subject to the rule. However, for purposes of this part of the Outline the CFPB assumes that most small depository institutions would be covered data providers subject to the rule. In contrast, the CFPB anticipates that only a limited share of small nondepository institutions would be covered data providers, data aggregators, or data recipients subject to the rule.

Q123. Please provide feedback on the CFPB's understanding of the industries that could be affected by the proposals under consideration.

C. CFPB review of implementation processes and costs

This analysis describes the implementation processes and costs that the proposals under consideration would impose. For clarity, these implementation costs are described separately for those that would apply to covered data providers and those that would apply to third parties, including data recipients and data aggregators that receive consumer-authorized information.[73] To the extent that any small entities are data aggregators or access consumer-authorized information without the use of a data aggregator, they would likely incur all costs described for third parties below.

As discussed elsewhere in this Outline, the CFPB understands that some covered data providers would also be data recipients for purposes of the proposals under consideration, and thus would need to meet both sets of obligations.

Q124. For covered data providers: does your business also participate in consumer-authorized information access as a data recipient? Would you expect to do so under the proposals under consideration?

1. Covered data providers

For covered data providers, the proposals under consideration would lead to one-time and ongoing compliance costs. These would stem from the potential requirements to provide both direct access and authorized third-party access to consumers. The CFPB expects that the largest costs would involve building and maintaining a third-party access portal. The CFPB expects that small entities would comply with the proposals under consideration by either contracting with a vendor (such as a core banking provider) to implement a third-party access portal, or by developing a third-party access portal in-house. While the proposals under consideration include a range of possible requirements for small entities, for the purposes of this part of the Outline the CFPB assumes all covered data providers would eventually need to implement a third-party access portal.

However, the CFPB understands that some small entities may already have some form of a third-party access portal. In these cases, small entities' existing portals may already satisfy the compliance requirements of the proposals under consideration, or they may be less costly to bring into compliance than implementing a new system from scratch. Similarly, if covered data providers already maintain existing third-party access portals, any additional ongoing compliance costs due to the proposals under consideration may be lower than those for covered data providers who do not yet have a third-party access portal. Small entities in these cases may

[73] The CFPB has considered both data recipients and data aggregators in analyzing the potential impacts of the proposals on third parties. In part III.B.2 above, the CFPB is requesting feedback on which authorization procedures and third party obligations should apply to the data recipient, the data aggregator, or both parties where a data recipient relies on a data aggregator to access consumer data from the covered data provider.

face some costs of renegotiating existing third-party access agreements to align with the requirements of the proposals under consideration.

Lacking direct data on costs associated with building or maintaining a compliant third-party access portal, the CFPB is limited to inferring estimated costs from alternative sources. These estimates may be inaccurate if building or maintaining a third-party access portal is more complex than the CFPB forecasts. In addition, certain aspects of the proposals under consideration, particularly the third-party portal availability factors described above in part III.D.2, may have large effects on the costs of building and maintaining a compliant portal.

To gauge costs associated with developing a third-party access portal, the CFPB conducted market research and spoke with industry participants. The CFPB anticipates that the structure of costs for small entities will differ substantially depending on whether they obtain a third-party access portal primarily through contracting with a vendor or primarily through an in-house build. The ongoing costs would likely be largest for contracting with a vendor, while upfront costs would be largest for a portal developed in-house. Small covered data providers' approaches are likely to be influenced by their size and their existing systems and connections with core banking providers. The analysis below estimates costs under these two alternatives, though covered data providers' approaches may reflect a combination of in-house development and contracted services.

Under the first approach, small covered data providers would primarily contract with a vendor for their third-party access portal. Many small covered data providers contract with core banking providers for transaction processing, online banking systems, or other key banking functions. Some core banking providers offer services to facilitate third-party access for covered data providers, often for an additional cost. These costs are likely to vary with the technology employed (*e.g.*, screen scraping or application programming interface) and the size of the data provider. Based on the CFPB's outreach, such added services have monthly costs that could range from several hundred dollars for the smallest covered data providers using the least burdensome technologies, to as high as $50,000 per month for the largest small covered data providers. For data providers taking this approach, the CFPB expects they would have limited additional upfront or ongoing costs, with the exception of the standard disclosures and record retention policies and procedures described below.

Under the second approach, small covered data providers would primarily build their third-party access portal in-house. The estimates below are based on the fully in-house development of a third-party access portal, though the CFPB anticipates that small covered data providers may be able to contract software providers for the initial development of their in-house portal at comparable or lower cost. Based on the CFPB's outreach, covered data providers would require approximately 2,600 to 5,200 hours of work by software developers or similar staff, equivalent to five full time employees over a period of three to six months. The CFPB assumes that these figures only apply to covered data providers that already provide consumers direct access to information through an online financial account management portal. The CFPB also assumes that these covered data providers possess and maintain electronic records in the ordinary course of their business for most or all of the data fields required by the proposals under consideration. As of the most recent available data from the Bureau of Labor Statistics (BLS), the mean hourly

wage for software developers is $58.17.[74] BLS data show that wages account for 70 percent of total compensation for private industry workers, so the CFPB assumes a total hourly compensation of $83.10.[75] The CFPB estimates the total upfront staffing cost to build a third-party access portal fully in-house ranges from $216,000 to $432,000.

In addition, small entities choosing the second, in-house approach would face ongoing staffing costs to maintain their third-party access portal. For such covered data providers, the CFPB estimates that maintaining and monitoring a third-party access portal would require approximately 500 to 1,000 hours per year of staff time. Similar to the assumption for one-time costs, this estimate assumes that covered data providers already have staff and resources dedicated to maintaining access to their online financial account management portal, and that the additional costs here are specific to maintaining the third-party access portal. If this work were performed by software developers, the total hourly compensation calculations above yield an estimate of $42,000 to $83,000 annually in ongoing staffing costs.

Small entities choosing the second, in-house approach would also likely incur upfront and ongoing computer hardware or service costs, but the CFPB estimates that these will be smaller than the staffing costs described above. Upfront hardware costs could include adding capacity to existing server networks, whether maintained on premises or rented from a vendor. Ongoing costs would include the costs of renting server or cloud computing capacity from a vendor or powering and maintaining servers added on premises. These costs stem not only from building and maintaining the third-party access portal, but also from changes in total network traffic that result from enabling third-party access. Though more third parties may access the network through the portal (or may access it more often), there may be an offsetting reduction in screen scraping traffic.

The proposals under consideration include several disclosure and recordkeeping requirements for all covered data providers related to consumer-authorized information access. These include requirements to inform third parties why access was not permitted under certain circumstances, and to inform consumers of their rights under the proposals under consideration. The requirements to inform third parties when and why access was not permitted would likely be built into a covered data provider's third-party access portal, as automated responses to third-party data access requests. Similarly, the requirements to retain records to demonstrate compliance with certain requirements of the proposals under consideration would likely be built into a covered data provider's third-party access portal. As a result, under both the vendor and in-house build approaches, the CFPB considers the costs of implementing these systems as part of the overall costs described above of implementing a compliant third-party access portal.

In contrast, the CFPB expects the periodic disclosures to inform consumers of their rights would be provided directly to consumers through electronic means outside of the third-party access portal, such as email or an online financial account management portal. The CFPB expects that covered data providers already provide other standard (*i.e.*, not tailored to specific consumers)

[74] Bureau of Labor Stat., *Occupational Employment and Wages—May 2021, 15-1252 Software Developers* (May 2021), https://www.bls.gov/oes/current/oes151252.htm.

[75] Bureau of Labor Stat., *Employer Costs for Employee Compensation—March 2022*, https://www.bls.gov/news.release/archives/ecec_06162022.pdf.

disclosures and terms of service to consumers through similar means. The CFPB considers the costs of developing these disclosures as part of the overall cost to develop and update policies and procedures described below. Once developed, the CFPB expects the cost of providing the disclosures to be negligible.

In addition to the costs related to implementing a third-party access portal, covered data providers would incur some costs to comply with the direct access requirements of the proposals under consideration. For these estimates, the CFPB assumes that all covered data providers have an online financial account management portal, either provided by a vendor or maintained in-house. The added costs would stem from making additional required information available that is not currently provided through the portal, and only for those covered data providers that do not already make all required information available. Covered data providers who contract a vendor to provide their online financial account management portal would likely rely on their vendor to add the additional information, with potentially limited added costs. Covered data providers who maintain their portal in-house would require approximately 250 to 500 hours of work by software developers or similar staff to add the required information to their online financial account management portal, representing a one-time cost of $21,000 to $42,000. Finally, to comply with the proposals under consideration, covered data providers would need to develop or update their standard disclosures and record retention policies and procedures and review compliance with the proposals as a whole. In other consumer financial markets, the CFPB has estimated that small depository institutions would face a one-time cost of $2,500 to $4,100 to develop policies and procedures and a one-time cost of $3,000 to $7,600 for a legal and compliance review.[76] Assuming comparable costs for the requirements of the proposals under consideration yields a total cost of roughly $5,500 to $11,700 for developing and implementing compliant procedures.

Q125. For data providers: do you have a third-party access portal or comparable system? If so, was the system built primarily in-house or provided primarily by a software provider pursuant to a contract?

Q126. For covered data providers with a third-party access portal or comparable system that was built primarily in-house:

i. What were your upfront staffing costs to build the portal or system?

ii. What are your ongoing staffing costs to maintain the portal or system?

iii. What were your upfront hardware or data processing costs to build the portal or system?

iv. What are your ongoing costs to maintain the hardware and provide the data processing capabilities?

v. Were you able to use existing hardware or data processing systems?

[76] 86 FR 56356, 56556 (Oct. 8, 2021).

vi. Has the portal or system worked effectively?

Q127. For covered data providers with a third-party access portal or comparable system that was built or provided primarily by a software provider pursuant to a contract:

i. What were the upfront costs to create the portal?

ii. What are the ongoing costs to maintain the portal? Do these costs scale with the number of consumers or accounts connected?

Q128. For covered data providers without a third-party access portal or comparable system: under the proposals under consideration, would you expect that you would develop a third-party access portal in-house or procure one from a software provider?

i. If you would procure a portal from a software provider, would you expect to use the core banking provider of your other technology services?

Q129. For covered data providers who have implemented a third-party access portal or comparable system: were there any unexpected costs or difficulties in building the portal or system? Were there any additional costs not captured above? Are the overall costs lower or higher than the CFPB's estimates?

Q130. For covered data providers who have built an in-house data portal or comparable system: what is the portal's target reliability goal, in terms of the expected number of downtime hours per year? What costs were considered when setting that reliability goal? How were those costs accounted for among staff versus technology investments?

Q131. For covered data providers who have contracted a software provider for a third-party access portal or comparable system: what are the portal's target standards for latency, uptime, and error response time? What access caps are in place? How many hours per year does the portal undergo planned and unplanned outages? What costs were incurred to contract for those standards, and were there lower or higher reliability standards available for contracts at different costs?

Q132. For covered data providers who have implemented a third-party access portal or comparable system: how did total network traffic change?

Q133. For covered data providers who have an online financial account management portal for direct access by consumers: is there any information that you do not currently provide through your online financial account management portal, but that you would need to provide under the proposals under consideration? What costs would you incur to provide this information through your online financial account management portal?

Q134. For covered data providers who do not have an online financial account management portal for direct access by consumers: what costs would you expect to incur to create an online financial account management portal?

Q135. For covered data providers: what legal fees or other compliance costs did you incur or would you expect to incur in developing a third-party access portal?

Q136. For covered data providers: what training costs, if any, would you expect to incur in implementing a third-party access portal?

2. Third parties

For third parties, the proposals under consideration may require modifications to existing systems or procedures to meet the conditions required for consumer-authorized information access, such as providing the authorization disclosure and certification statement; implementing the limitations on data collection, use, and retention; mechanisms for revocation of authorization and deletion; potentially providing ongoing disclosures and opportunities to reauthorize access; and record retention requirements.

The CFPB understands that most data recipients who are small entities partner with larger data aggregators to facilitate linking consumers' financial accounts to the data recipients' systems. The CFPB expects that data aggregators would modify their existing systems to meet many of the conditions required for consumer-authorized information access. Some conditions would likely require modifications to existing systems or procedures for all third parties receiving consumer-authorized information, including both data recipients and data aggregators.

The CFPB expects that in many cases, data aggregators would likely provide the required authorization disclosure and certification statement on behalf of the third parties involved. Based on cost estimates from requirements for tailored disclosures provided at service initiation in other consumer financial markets, the CFPB estimates that each data aggregator will require approximately 1,000 hours of work by software developers or similar staff to incorporate the authorization disclosure and certification statement into their existing systems.[77] Based on total compensation hourly costs described above, this results in a one-time cost for data aggregators of $83,000. However, even if costs are passed through to third parties, because relatively few large data aggregators would spread costs to relatively many third parties—only some of which are small entities—the CFPB expects the burden of these requirements for small third parties to be small.

The CFPB is considering proposals that would require third parties to build and maintain systems that could receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revocation or authorization lapses. These systems would also need to retain records as required by the proposals under consideration. Third parties that operate in the state of California and have gross annual revenues greater than $25 million may already have such systems if they are subject to the California Consumer Privacy Act (CCPA),[78]

[77] 82 FR 54472, 54823 (Nov. 17, 2017).

[78] Cal. Civ. Code § 1798.198(a) (2018).

which requires that businesses delete consumer personal data upon consumer request. These third parties would likely need to modify their systems, incorporate authorization duration limits, and process more data deletion requests, but they would likely have lower costs than third parties that must build such a system from scratch. The CFPB estimates that building and maintaining an appropriate data system would cost up to $75,000 based on analysis of the Standardized Regulatory Impact Assessment for the CCPA.[79] The CFPB is interested in receiving feedback on the estimated cost of implementing access revocation or deletion systems and maintaining records of consumer data and revocation requests.

To implement the proposals under consideration, third parties would need to develop and maintain policies and procedures in several distinct areas. These include (1) a comprehensive written data security program appropriate to their size and complexity as described in part III.E.2,[80] (2) reasonable policies and procedures to ensure the accuracy of the information that they collect, as described in part III.E.3, (3) policies governing the limits on collection, use, and retention of consumer-authorized information, and (4) record retention requirements for third parties to demonstrate adherence to certain requirements of the rule. In other consumer financial markets, the CFPB has estimated that small nondepository institutions would face a one-time cost of $4,300 to develop new policies and procedures and a one-time cost of $3,900 for a legal/compliance review.[81] Assuming comparable costs for the requirements of the proposals under consideration yields a total cost of roughly $8,200 for developing and implementing necessary procedures. The CFPB requests information on the cost of developing policies and procedures regarding such practices from third parties that have already done so. Maintaining the policies and procedures once initially implemented is likely to involve limited ongoing costs.

Q137. For third parties: do you currently provide disclosures or other information to consumers within your own platform? What would be the expected costs to modify these systems to satisfy the proposals under consideration?

Q138. For third parties: do you have written policies and procedures in place regarding the collection, use, and retention of consumer-authorized data; data security; data accuracy and dispute resolution; and record retention? If so, how many staff-hours did you commit to develop these procedures? How many staff-hours do you expect it would take to develop policies and procedures to implement the proposals under consideration?

[79] The Standardized Regulatory Impact Assessment for the CCPA estimated that the average technology cost would be $75,000. However, the CFPB estimates that the cost for most of the small businesses considered in this Outline would be lower, as the CCPA figure was based on a survey of the top 1 percent of California businesses by size (those with more than 500 employees), and the CCPA has more requirements than the CFPB's considered proposals. *See* Off. of the Att'y Gen., Cal. Dep't of Justice, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), https://dof.ca.gov/wp-content/uploads/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf.

[80] Alternatively, they could satisfy these requirements by complying with the Safeguards Rule or Safeguards Guidelines.

[81] 86 FR 56356, 56556 (Oct. 8, 2021).

Q139. For third parties: do you have consumer-facing tools for access revocation and deletion? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you expect it would take to develop these tools to implement the proposals under consideration?

Q140. For third parties: what training costs, if any, would you expect to incur in satisfying the third party obligations and record retention obligations of the proposals under consideration?

D. Additional impacts of proposals under consideration

In addition to the implementation processes and costs described above, the proposals under consideration would likely have additional effects on covered data providers and third parties, including small entities. These additional effects would depend on the baseline structure of how consumer-authorized information is shared and handled by covered data providers and third parties in the current market. Based on market research and engagement with industry participants, the CFPB understands that a substantial and growing share of consumer-authorized information access occurs through third-party access portals under agreements between covered data providers and third parties. However, access through such portals primarily occurs among very large covered data providers, while access through screen scraping or other credential-based systems is more common for small covered data providers. The CFPB anticipates that the share of small covered data providers providing consumer-authorized data access through third-party access portals will increase, particularly as core banking software providers adopt the technology for their covered data provider customers.

1. Covered data providers

The proposals under consideration would lead to increased integration between covered data providers and third parties. The CFPB expects that most existing consumer-authorized data access that occurs through screen scraping would transition to new third-party access portals, and additional consumer-authorized data sharing may be facilitated if the proposals under consideration lower the barriers to establishing third-party connections. However, some existing consumer-authorized data access may cease if the requirements and conditions on data collection, use, and retention for third parties make certain business models or use cases unprofitable. As discussed further below, these additional effects of the proposals under consideration may include both costs and benefits for small covered data providers, depending on the specifics of their institution and their desire to provide consumer-authorized information access.

Absent the proposals under consideration, establishing an agreement between a covered data provider and a third party on the terms of consumer-authorized information access requires substantial negotiation, with the negotiating leverage of the parties dependent in part on their size, technical capabilities, and desire to facilitate such data access. The CFPB anticipates that the proposals under consideration would reduce the set of negotiable terms in such agreements, as these terms would be largely determined by the proposals, if finalized. Depending on the covered data providers' desired terms of access, these changes may reflect an additional benefit or cost of the proposals under consideration.

Some third-party products and services derived from consumer-authorized data sharing can be complementary to the services offered by covered data providers, while other uses compete with covered data providers' internal products and services. For example, third-party payment services and personal financial management products may enhance the functionality of consumers' financial data and accounts, increasing their utility from their covered data provider account. But consumer-authorized cash advance and underwriting use cases offer consumers credit products that may compete with covered data providers' own products.

The proposals under consideration, if finalized, may require covered data providers to make available additional data fields relative to the status quo. This may enable certain third-party products or services. The proposals may also reduce the data fields available to third parties when those fields are not reasonably necessary for the third party's products or services. This may make certain third-party products or use cases which rely on secondary data unprofitable. Depending on whether such products are complementary to or compete with the covered data providers' own products, this may represent an additional cost or benefit of the proposals under consideration.

The CFPB understands that, in general, consumer-authorized data access that occurs through third-party access portals involves substantially lower traffic loads than screen scraping. The transition to third-party access portals is therefore likely to reduce total traffic. Similarly, proposals under consideration related to the collection, use, and retention limitation standard are likely to reduce total traffic, particularly for use cases that do not require large data fields such as detailed transaction information.

The CFPB is aware that many covered data providers impose access caps, such as limiting the number of allowable data calls, total traffic, or the frequency at which authorized third parties can access consumer data. The CFPB is considering proposals that would create requirements for these access caps. All else equal, this is likely to increase total traffic and may therefore increase costs for covered data providers. The CFPB is also considering proposals that would create requirements for third-party access portals' uptime, latency, planned and unplanned outages, and error response. To the extent that covered data providers do not currently meet these requirements, the proposals may impose costs related to increasing reliability.

By relaxing access caps and increasing the reliability of third-party data access, the proposals under consideration may improve the quality of third-party products or services. This may reflect an additional cost or benefit to covered data providers depending on whether such third-party products or services are complementary to or compete with covered data providers' own products and services.

Covered data providers may be differentiated by their current data access policies. For example, a covered data provider may attract customers by offering better integration with complementary third-party applications than its competitors. The proposals under consideration are likely to result in more uniform terms of access, which will reduce the competitive advantages covered data providers currently gain from differentiation.

To the extent that covered data providers generate revenue by selling or otherwise capturing value from data on their customers, the value derived from these data could be reduced by greater data availability through consumer-authorized access.

Finally, the transition away from credential-based authorized information access would likely reduce the risk of data breaches and resulting potential costs for covered data providers.

Q141. For covered data providers who have negotiated or attempted to negotiate third-party access agreements: would you expect the proposals under consideration to reduce the costs of negotiating such agreements?

Q142. Does existing consumer-authorized information access generally complement or compete with your own products and services? Has such data access led to changes in consumers' use of your own products or services? Has such data access led you to develop new products and services due to changing consumer expectations?

Q143. Are there significant differences in consumer-authorized information access policies between covered data providers? Are there certain use cases enabled or prohibited by existing consumer-authorized information access which would lead a consumer to choose one covered data providers' products or services over another's?

2. Third parties

Some of the proposals under consideration would place limits on third parties' use and retention of consumer financial data, which could impede certain products or business models that third parties use to generate revenue. One large potential impact of the proposals under consideration in this regard would be the required deletion of consumer's financial data when authorization lapses or is revoked. If third parties rely on such data to develop new products or services (such as underwriting models based on transaction histories), the proposals under consideration could hinder these use cases.

The CFPB estimates that a majority of third-party screen scraping traffic comes from user-not-present personal financial management services. These services rely on frequent monitoring of balances and transactions to alert consumers when an account balance falls below a predetermined amount, or when an unusually large transaction is posted, for example. These services may become more limited if the CFPB requires periodic reauthorization, as third parties will be unable to collect account data if a consumer fails to reauthorize access. However, these services may be improved by increasing the availability of relevant data elements.

The CFPB anticipates that the proposals under consideration will enable third parties to obtain more data elements from covered data providers relative to the status quo. The CFPB is also considering proposals that would regulate the availability of these data elements and may make them available more often by creating requirements for third-party access portals' uptime, latency, planned and unplanned outages, error response, and access caps. These changes may improve the quality of services offered by third parties, and these services may better compete

with (or complement) covered data providers' own services. This may be particularly salient when the covered data provider's product makes use of data that was not shared with third parties prior to the rulemaking, but under the rulemaking will be required to be shared.

Q144. Would the proposals requiring the deletion of consumer data when consumer authorization lapses or is revoked impede products or business models used by third parties?

Q145. Would the proposals restricting certain secondary uses of consumer data impede products or business models used by third parties?

Q146. Would any limitations created by the data availability standards impede products or business models used by third parties?

Q147. Would periodic reauthorization requirements lead to reduced customer retention for products or business models used by third parties?

Q148. For third parties who have negotiated or attempted to negotiate third-party access agreements: would you expect the proposals under consideration to reduce the costs of negotiating such agreements? Would you expect the proposals to lead to more favorable or less favorable terms of access for third parties?

E. Impact on the cost and availability of credit to small entities

Section 603(d) of the RFA requires the CFPB to consult with small entities regarding the potential impact of the proposals under consideration on the cost of credit for small entities. The CFPB expects that the proposals under consideration may have some limited impact on the cost or availability of credit for small entities but does not expect that the impact would be substantial.

The CFPB expects there are several ways the proposals under consideration could potentially impact the cost or availability of credit to small entities. First, the proposals could impact the availability of credit to small entities if small businesses are using loans from lenders (either covered data providers or third parties) affected by the proposals and the proposals lead to a contraction of the market. Second, the proposals could potentially increase the cost of credit for small businesses if the costs of implementing the proposals are passed through in the form of higher prices on loans from lenders. Third, for small businesses that use consumer-authorized data to qualify for or access credit, the proposals could potentially increase credit availability or lower costs for small entities by facilitating increased data access.

Q149. Would the proposals under consideration affect the cost and availability of credit to small entities? Are there additional channels beyond those described above that could affect the cost and availability of credit to small entities?

Appendix A: Section 1033 of the Dodd-Frank Act

12 USC 5533.

SEC. 1033. CONSUMER RIGHTS TO ACCESS INFORMATION.

(a) IN GENERAL.—Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

(b) EXCEPTIONS.—A covered person may not be required by this section to make available to the consumer—

(1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;

(2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;

(3) any information required to be kept confidential by any other provision of law; or

(4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

(c) NO DUTY TO MAINTAIN RECORDS.—Nothing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer.

(d) STANDARDIZED FORMATS FOR DATA.—The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.

(e) CONSULTATION.—The Bureau shall, when prescribing any rule under this section, consult with the Federal banking agencies and the Federal Trade Commission to ensure, to the extent appropriate, that the rules—

(1) impose substantively similar requirements on covered persons;

(2) take into account conditions under which covered persons do business both in the United States and in other countries; and

(3) do not require or promote the use of any particular technology in order to develop systems for compliance.

Appendix B: Glossary

The CFPB is seeking feedback and information from SERs as to the clarity of these terms, which the CFPB is considering including in a proposed rule.

Account means a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes.

Administrator means the appointed head of the Small Business Administration.

Authorization disclosure means a disclosure that would be provided by a third party as a condition to be an authorized third party, as described in part III.B.2.

Authorized third party means a third party who has followed the procedures for authorization described in part III.B.2.

Calls means electronic requests from a third party to a data provider to make information available through a portal.

Card issuer has the meaning provided in Regulation Z. It refers to a person that issues a credit card or that person's agent with respect to the card (12 CFR 1026.2(a)(7)).

Consumer means an individual who obtained the consumer financial product or service from a covered data provider.

Consumer-authorized information means third-party access to consumer financial information pursuant to the relevant consumer's authorization.

Covered account(s) means asset account(s) (see account definition) and credit card account(s) (any open-end credit account that is accessed by a credit card).

Covered data provider means a financial institution, as defined in Regulation E (EFTA), or a card issuer, as defined in Regulation Z (TILA), who is a data provider.

Credit card has the meaning provided in Regulation Z. It refers to any card, plate, or other single credit device that may be used from time to time to obtain credit (12 CFR 1026.2(a)(15)(i)).

Data aggregator (or **aggregator**) means an entity that supports data recipients and data providers in enabling consumer-authorized information access.

Data provider means a covered person, as defined under the Dodd-Frank Act (12 U.S.C. 5481(6)), with control or possession of consumer financial information.

Data recipient means a third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer.

Deletion is the complete removal of previously collected consumer information.

Depository institution means any bank or savings association defined by the Federal Deposit Insurance Act, 12 U.S.C. 1813(c)(1), or credit union defined pursuant to the Federal Credit Union Act, as implemented by 12 CFR 700.2.

Direct access refers to covered data providers making information available, upon request, directly to a consumer.

Dodd-Frank Act means the Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, 124 Stat. 1376 (2010). Section 1033 of the Dodd-Frank Act provides the CFPB with the authority to promulgate rules related to the proposals under consideration.

EFT means electronic fund transfer, as defined in Regulation E. The term refers to any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to (i) point-of-sale transfers, (ii) automated teller machine transfers, (iii) direct deposits or withdrawals of funds, (iv) transfers initiated by telephone, and (v) transfers resulting from debit card transactions, whether or not initiated through an electronic terminal (12 CFR 1005.3(b)(1)).

EFTA and **Regulation E** refer to the Electronic Fund Transfer Act (15 U.S.C. 1693 *et seq.*), and the CFPB's implementing regulation, Regulation E (12 CFR part 1005).

FCRA and **Regulation V** refer to the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*), and the CFPB's implementing regulation, Regulation V (12 CFR part 1022).

Financial institution means a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services (12 CFR 1005.2(i)).

GLBA refers to the Gramm-Leach-Bliley Act, Public Law 106-102, 138 Stat. 1338 (1999) (15 U.S.C. 6801 *et seq.*).

Online financial account management portal means an online portal that a data provider makes available for consumers to directly access information, often using a consumer username and password, about the consumer financial product or service that the consumer obtained from the data provider.

Regulatory Flexibility Act or **RFA**, Public Law 96-354, 94 Stat.1164 (1980) (5 U.S.C. 601 *et seq.*), refers to the statute that established the principle of regulatory issuance that agencies shall endeavor, consistent with the objectives of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the businesses, organizations, and governmental jurisdictions subject to that regulation.

RESPA and **Regulation X** refer to the Real Estate Settlement Procedures Act of 1974 (12 U.S.C. 2601 *et seq.*), and the CFPB's implementing regulation, Regulation X (12 CFR part 1024).

Revocation means the mechanism by which the consumer withdraws consent from third parties they previously authorized to access their information.

Safeguards Rule and **Safeguards Guidelines** refer to the rules issued by the Federal Trade Commission and the guidelines issued by the prudential regulators that generally implement the GLBA's data security safeguards framework, pursuant to sections 501 (15 U.S.C. 6801) and 505 (15 U.S.C. 6805) of the GLBA.

Screen scraping means authorized access that uses proprietary software to convert consumer data presented in the provider's online financial account management portal into standardized machine readable data, generally on an automated basis.[82]

Secondary use means a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including a third party's own use of consumer information and the sharing of information with downstream entities.

Small Business Regulatory Enforcement Fairness Act of 1996 or **SBREFA**, Public Law 104-121, tit. II, 110 Stat. 857 (1996), refers to the statute that establishes the Small Business Review Panel process for certain CFPB, Environmental Protection Agency, and Occupational Health and Safety Administration rulemakings. SBREFA amended the RFA.

Small Business Review Panel or **Panel** means a panel formed of representatives from the CFPB, the Chief Counsel for Advocacy of the Small Business Administration, and the Office of Information and Regulatory Affairs in the Office of Management and Budget. A Panel is convened in accordance with SBREFA when a rule under development may have a significant economic impact on a substantial number of small entities. The Panel for the CFPB's rulemaking on Personal Financial Data Rights will prepare a report of its recommendations after discussing the proposals and alternatives under consideration with the SERs.

Small entity means a small business, small organization, or a small governmental jurisdiction as defined by the Regulatory Flexibility Act. The size standards for determining a business as small vary by industry and are established by the Small Business Administration.

Small Entity Representative or **SER** means a representative of a small entity who participates in the SBREFA process to provide input on costs and benefits of the proposals under consideration in a rulemaking.

Third party refers, generally, to data recipients or data aggregators.

Third-party access refers to covered data providers making information available, upon request, to authorized third parties.

[82] Screen scraping is often used to refer to screen scraping using *credential-based access*, which is a particular form of authorized access that uses the consumer's user ID and password or like credentials to log into the data provider's online financial account management portal, generally on an automated basis. However, credential-based access is not the only form of access used by screen scraping.

Third-party access portal means a portal that a data provider makes available for third parties authorized by consumers to access information about the consumer financial product or service that the consumer obtained from the data provider based on standardized information formats and other terms agreed upon by the data provider and third party.

Third-party portal availability factors or **availability factors** refer to the factors the CFPB is considering proposing to assess the availability of information provided through a data provider's third-party access portal. These factors are listed in part III.D.2.ii.

TILA and **Regulation Z** refer to the Truth in Lending Act, codified at 15 U.S.C. 1601 *et seq.*, and the CFPB's implementing regulation, Regulation Z (12 CFR part 1026).

TISA and **Regulation DD** refer to the Truth in Savings Act, codified at 12 U.S.C. 4301 *et seq.*, and the CFPB's implementing regulation, Regulation DD (12 CFR part 1030).

Appendix C: Closely related Federal statutes and regulations

The CFPB has identified other Federal statutes and regulations that have potentially overlapping or conflicting requirements in order to avoid duplication or conflict with implementing section 1033. The CFPB has identified the following Federal statutes and regulations as closely related to section 1033.

The Electronic Fund Transfer Act (EFTA)[83] and the CFPB's implementing regulation, Regulation E (12 CFR part 1005), establish a basic framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems. Among other requirements, EFTA and Regulation E prescribe requirements applicable to electronic fund transfers, including disclosures, error resolution, and rules related to unauthorized electronic fund transfers.

The Fair Credit Reporting Act (FCRA)[84] and the CFPB's implementing regulation, Regulation V (12 CFR part 1022), govern the collection, assembly, and use of consumer report information and provide the framework for the credit reporting system in the United States. They also promote the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. They also include limitations on the use of certain types of consumer information, limitations on the disclosure of such information to third parties, as well as certain requirements related to accuracy and dispute resolution.

The Gramm-Leach-Bliley Act (GLBA)[85] and the CFPB's implementing regulation, Regulation P (12 CFR part 1016), require financial institutions subject to the CFPB's jurisdiction to provide their customers with notices concerning their privacy policies and practices, among other things. They also place certain limitations on the disclosure of nonpublic personal information to nonaffiliated third parties, and on the redisclosure and reuse of such information. Other parts of the GLBA, as implemented by regulations and guidelines of certain other Federal agencies (*e.g.*, the Federal Trade Commission's Safeguards Rule and the prudential regulators' Safeguards Guidelines), set forth standards for administrative, technical, and physical safeguards with respect to financial institutions' customer information. These standards generally apply to the security and confidentiality of customer records and information, anticipated threats or hazards to the security or integrity of such records, and unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

The Truth in Lending Act (TILA)[86] and the CFPB's implementing regulation, Regulation Z (12 CFR part 1026), impose requirements on creditors and include special provisions for credit offered by credit card issuers. Among other requirements, TILA and Regulation Z prescribe requirements applicable to credit cards, including disclosures, error resolution, and rules related to unauthorized credit card use.

[83] 15 U.S.C. 1693 *et seq.*

[84] 15 U.S.C. 1681 *et seq.*

[85] 15 U.S.C. 6801 *et seq.*

[86] 15 U.S.C. 1601 *et seq.*

The Truth in Savings Act (TISA)[87] and the CFPB's implementing regulation, Regulation DD (12 CFR part 1030), apply to depository institutions; TISA and Part 707 of the National Credit Union Administration Rules and Regulations apply to credit unions. Among other things, TISA and Regulation DD prescribe requirements applicable to deposit accounts, including disclosure requirements.

The Real Estate Settlement Procedures Act of 1974 (RESPA)[88] and the CFPB's implementing regulation, Regulation X (12 CFR part 1024), include requirements applicable to mortgage servicers that seek to protect borrowers against certain billing and servicing errors.

[87] 12 U.S.C. 4301 *et seq.*

[88] 12 U.S.C. 2601 *et seq.*

APPENDIX E: HIGH-LEVEL SUMMARY AND DISCUSSION GUIDE OF OUTLINE OF PROPOSALS AND ALTERNATIVES UNDER CONSIDERATION FOR SBREFA: REQUIRED RULEMAKING ON PERSONAL FINANCIAL DATA RIGHTS

See attached.

October 27, 2022

High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights

In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Section 1033(a) of the Dodd-Frank Act authorizes the Consumer Financial Protection Bureau (CFPB) to prescribe rules requiring "a covered person [to] make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[1]

The Bureau is now in the process of writing regulations to implement section 1033. Under the process established by Congress in the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), the Bureau is required to consult with representatives of small entities likely to be affected directly by the regulations the Bureau is considering proposing and to obtain feedback on the likely impacts the rules the Bureau is considering would have on small entities.

[1] Dodd-Frank Act section 1033, 124 Stat. 2008 (codified at 12 U.S.C. 5533(a)). The term "covered person" is defined at section 1002(6) of the Dodd-Frank Act. *See* 12 U.S.C. 5481(6).

This document provides a high-level summary of the regulatory provisions the CFPB is considering proposing, as described more fully in its Outline of Proposals and Alternatives Under Consideration (Outline). These proposals address the following topics:

- Coverage of data providers who would be subject to the proposals under consideration;[2]
- Recipients of information, including consumers and authorized third parties;[3]
- The types of information that would need to be made available;
- How and when information would need to be made available, including when information made available to consumers directly and to third parties authorized to access information on their behalf;
- Third party obligations;
- Record retention obligations; and
- Implementation period.

The Appendix illustrates how the CFPB's proposals under consideration would apply to a hypothetical transaction involving data access to an authorized third party.

Discussion questions. This summary includes questions drawn from the Outline, selected to solicit feedback from small entity representatives on specific topics. However, the CFPB is interested in input from SERs on all aspects of the proposals under consideration and any alternatives the CFPB should consider.

[2] For purposes of the Outline, a "data provider" means a covered person with control or possession of consumer financial data.

[3] For purposes of the Outline, "third party" refers, generally, to data recipients or data aggregators. "Data recipient" means a third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer, or (2) services used by entities that provide products or services to the authorizing consumer. "Data aggregator" means an entity that supports data recipients and data providers in enabling consumer-authorized information access. The term "authorized third party" means a third party who has followed certain procedures for authorization described in part III.B.2 of the Outline and summarized below under section B (Recipients of information).

The following questions apply to all the proposals under consideration discussed below.

- *Do you believe any of the statutes or regulations identified in Appendix C of the Outline,*[4] *or other statutes or regulations, duplicate, overlap, or conflict with the CFPB's proposals under consideration? (See Outline Q1-2.)*

- *What factors disproportionately affecting small entities should the CFPB be aware of when evaluating the proposals under consideration? For example, would a small entity's reliance on a core processor or other service provider affect the costs or burdens associated with any of the proposals under consideration? Would any of the proposals under consideration provide unique benefits to small entities? What training costs, if any, would small entities expect to incur in implementing the proposals? (See Outline Q3, 136, 140.)*

- *Please provide input on any costs or challenges you foresee with the enforcement or supervision of the proposals under consideration. In particular, please provide input on whether enforcement or supervision of the proposals under consideration may be impractical in certain circumstances and how the CFPB could address those concerns. (See Outline Q4.)*

- *Would the proposals under consideration affect the cost and availability of credit to small entities? Are there additional channels beyond those described above that could affect the cost and availability of credit to small entities? (See Outline Q149.)*

A. Coverage of data providers subject to the proposals under consideration (Outline part III.A)

Covered data providers. The CFPB is considering proposals that, if finalized, would require a defined subset of Dodd-Frank Act covered persons (*see* 12 U.S.C. 5481(6)) that are data providers to make consumer financial information available to a consumer or an authorized third party. This subset of data providers would be entities that meet the definition of "financial institution" as set forth in § 1005.2(i) of the CFPB's Regulation E (12 CFR part 1005) or "card issuer" as set forth in § 1026.2(a)(7) of the CFPB's Regulation Z (12 CFR part 1026). The data

[4] Appendix C of the Outline lists the Electronic Fund Transfer Act (EFTA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Truth in Lending Act (TILA), the Truth in Savings Act (TISA), and the Real Estate Settlement Procedures Act of 1974 (RESPA), and the CFPB's implementing regulations of those statutes.

providers that would be directly affected by the proposals under consideration include depository and non-depository financial institutions that provide consumer funds-holding accounts or that otherwise meet the Regulation E definition of financial institution, as well as depository and non-depository institutions that provide credit cards or otherwise meet the Regulation Z definition of card issuer. The Outline refers to financial institutions and card issuers collectively as "covered data providers."

It is important to note that a financial institution would be a covered data provider if it issues an "access device" (as the term is defined in Regulation E § 1005.2(a)(1)), such as a digital credential storage wallet, and provides EFT services, even if it does not hold consumer accounts. Likewise, a card issuer would be a covered data provider if it issues a "credit card" (as the term is defined in Regulation Z § 1026.2(a)(15)(i)), such as by issuing digital credential storage wallets, even if it does not hold consumer credit accounts.

- *Please provide input on the approach the CFPB is considering with respect to the coverage of data providers. What alternative approaches should the CFPB consider? For example, should the CFPB also consider covering payment account providers that are not Regulation E financial institutions as presently defined, such as providers of government benefit accounts used to distribute needs-based benefits programs? Should the CFPB consider covering any providers of credit products that are not Regulation Z credit cards? How could the CFPB clarify coverage of the proposals under consideration? (See Outline Q5.)*

Covered accounts. Under the proposals the CFPB is considering, a Regulation E financial institution would be a covered data provider with respect to information that pertains to an "account," as that term is defined in Regulation E § 1005.2(b), and a Regulation Z card issuer would be a covered data provider with respect to information that pertains to a "credit card account under an open-end (not home-secured) consumer credit plan" as that term is defined in Regulation Z § 1026.2(a)(15)(ii). The Outline refers to these accounts collectively as "covered accounts."

Potential exemptions for certain covered data providers. The CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers. However, in determining if exemptions would be appropriate, the CFPB is interested in whether there are ways to design the proposals described in this Outline to reduce impact on covered data providers.

- *Should the CFPB exempt certain covered data providers from any particular proposals under consideration? For which covered data providers would such exemptions be appropriate, and why? Which proposals should such data providers be exempt from, and why? (See Outline Q6.)*

B. Recipients of information (Outline part III.B)

Consumers and third parties. The CFPB is considering proposals that would address a covered data provider's obligation to make information available upon request directly to a consumer (direct access) and to authorized third parties (third-party access).

Third-party authorization procedures—in general. Under the proposals the CFPB is considering, to be an authorized third party, the third party must: (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.

- *Please provide input on the approach the CFPB is considering with respect to the authorization procedures, described in more detail in part III.B.2 of the Outline. In providing input, please describe the authorization procedures that third parties and/or covered data providers currently employ and the benefits and drawbacks of those procedures in comparison to the procedures the CFPB is considering. What costs would third parties or covered data providers face with respect to the authorization procedures under consideration? (See Outline Q12.)*

- *What alternative approaches should the CFPB consider? Please describe any additional authorization procedures or any suggested changes to the procedures the CFPB is contemplating. (See Outline Q13.)*

- *Where a data recipient relies on a data aggregator to access consumer data from the covered data provider, which authorization procedures and third party obligations should apply to the data recipient, the data aggregator, or both parties? For example, should the data recipient or the data aggregator be responsible for providing the authorization disclosure to the consumer? What obligations, if any, should apply to parties other than a data recipient or an aggregator who receive consumer data? (See Outline Q14.)*

Third-party authorization procedures—authorization disclosure. The CFPB is considering proposing that the authorization disclosure would contain key scope and use terms.

Key scope terms might include the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access. Key use terms might include the identity of intended data recipients (including any downstream parties and data aggregators to whom the information may be disclosed), and the purpose for accessing the information. The CFPB is also considering proposing that the authorization disclosure include a reference to the third party's certification to certain obligations regarding collection, use, and retention of the consumer's information, which are described in part III.E of the Outline and summarized below in section E. The authorization disclosure would also contain a request for consent to access the consumer's information.

- *Please describe any additional content that should be included in the authorization disclosure or whether there are circumstances in which more limited disclosures would be appropriate. In providing input, please describe the extent to which third parties currently inform consumers about the scope and use of data when obtaining authorization. (See Outline Q17.)*

- *Please provide input on whether the full certification statement regarding an authorized third party's obligations with respect to the collection, use, and retention of consumer information should be included in the authorization disclosure? (See Outline Q21.)*

The CFPB is considering proposing that the authorization disclosure would need to be provided close in time to when the third party would need the consumer-authorized information to provide the product or service requested by the consumer. The CFPB is also considering proposing that the authorization disclosure would need to be clear and conspicuous and segregated from other material.

- *Please provide input on whether the CFPB should include any particular requirements or restrictions on the timing and format of the authorization disclosure to prevent the use of potentially misleading practices aimed at soliciting consent, such as a prohibition on pre-populated consent requests. (See Outline Q19.)*

C. The types of information a covered data provider would be required to make available (Outline part III.C)

Scope of information with respect to covered accounts. Dodd-Frank Act section 1033(a) authorizes the CFPB to require a data provider to make available information

"concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data." The Outline sets forth six categories of information the CFPB is considering requiring covered data providers to make available with respect to covered accounts:

- Periodic statement information regarding transactions and deposits that have settled,[5] including fees, account terms and conditions, and the annual percentage yield of an asset account or the annual percentage rate of a credit card account;
- Information regarding prior transactions and deposits that have not yet settled;
- Information about prior transactions not typically shown on periodic statements or online financial account management portals;
- Online banking transactions that the consumer has set up but that have not yet occurred;
- Account identity information; and
- Other information, including consumer reports obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer; fees that the covered data provider assesses on its consumer accounts; bonuses, rewards, discounts, or other incentives that the covered data provider gives to consumers; and information about security breaches that exposed a consumer's identity or financial information.

- *Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make available the above information to a consumer or an authorized third party. What alternative approaches should the CFPB consider? (See Outline Q22-29)*

Exceptions. Dodd-Frank Act section 1033(b) sets forth the following four exceptions to the section 1033(a) requirement to make information available. Specifically, under the statute, a data provider may not be required by section 1033 to make available:

[5] This information generally appears on periodic statements that covered data providers are currently required to provide for asset accounts under Regulation E § 1005.9(b) and § 1030.6(a) of the CFPB's Regulation DD (12 CFR part 1030) and for credit card accounts under Regulation Z §§ 1026.7(b) and 1026.8

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

- *How should the CFPB interpret these exceptions? Which data elements should be covered under the exceptions? (See Outline Q30-37.)*

Current and historical information. The CFPB is considering proposing that a covered data provider would need to make available the most current information that the covered data provider has in its control or possession at the time of a request for current information. With respect to historical information that may be requested, as noted above, Dodd-Frank Act section 1033(c) states that section 1033 shall not be construed to impose a duty on a data provider to maintain or keep any information about a consumer. In light of section 1033(c), the CFPB is considering proposals under which a covered data provider would be required only to make available information going as far back in time as that covered data provider makes transaction history available directly to consumers, such as, but not limited to, through the covered data provider's online financial account management portal.

D. How and when information would need to be made available (Outline part III.D)

The CFPB is considering proposals to define the methods and the circumstances in which a covered data provider would need to make information available with respect to both direct access (where a consumer directly obtains data about their own account from the covered data provider), and third-party access (where a consumer authorizes a third party to access data on their behalf).

- *Do covered data providers currently charge consumers or third parties specific fees (i.e., fees other than periodic account maintenance fees) to access information, such as through an online financial account management portal, a third-party access portal, or to export information in a human or machine readable format? What would be the impact on covered data providers, consumers, and authorized third parties if covered*

data providers were or were not restricted from charging specific fees? (See Outline Q41, 63.)

- *Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate? (See Outline Q82.)*

Direct access. With respect to requests for direct access, the CFPB is considering proposing that a covered data provider would be required to make information available if it has enough information from the consumer to reasonably authenticate the consumer's identity and reasonably identify the information requested. The CFPB is also considering proposing that covered data providers would be required to make available all the information that would be covered by the proposals under consideration through online financial account management portals, and to allow consumers to export the information in both human and machine readable formats. For example, many data providers allow consumers to export a history of their transactions in file formats that present the information in a consumer-friendly display and file formats such that the file could be imported or read into a computer system for further processing (*e.g.*, a .CSV file format).

- *Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers through an online financial account management portal and by giving consumers the option to export the information in both human and machine readable file formats. What alternatives should the CFPB consider? (See Outline Q40.)*

Third-party access. With respect to third-party access, the CFPB is considering proposing that covered data providers must establish and maintain a third-party access portal that does not require the authorized third party to possess or retain consumer credentials. The CFPB is also considering what role screen scraping should play in the context of a covered data provider's compliance with the rule. Specific aspects of this approach under consideration are described further below.

- *Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal, along with any alternative approaches the CFPB should consider. (See Outline Q50.)*

- *Please provide input on how covered data providers' customers can share their account information with third parties today. (See Outline Q51.)*

- *For covered data providers with a third-party access portal or comparable system that was built primarily in-house:*
    - *What were your upfront staffing costs to build the portal or system?*
    - *What are your ongoing staffing costs to maintain the portal or system?*
    - *What were your upfront hardware or data processing costs to build the portal or system?*
    - *What are your ongoing costs to maintain the hardware and provide the data processing capabilities?*
    - *Were you able to use existing hardware or data processing systems?*
    - *Has the portal or system worked effectively?*

      (See Outline Q126.)
- *For covered data providers with a third-party access portal or comparable system that was built or provided primarily by a software provider pursuant to a contract:*
    - *What were the upfront costs to create the portal?*
    - *What are the ongoing costs to maintain the portal? Do these costs scale with the number of consumers or accounts connected?*

      (See Outline Q127.)
- *For covered data providers without a third-party access portal or comparable system, under the proposals under consideration: would you expect you would need to develop a third-party access portal in-house or procure one from a software provider? If you would procure a portal from a software provider, would you expect to use the core banking provider of your other technology services? (See Outline Q128.)*
- *With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, should the CFPB require that they make information available to authorized third parties before they establish a third-party access portal? Would such a requirement necessitate covered data providers allowing authorized third parties to engage in screen scraping? Are there alternatives to screen scraping that a covered data provider could implement to make information available to authorized third parties in electronic form while establishing a third-party access portal? (See Outline Q52.)*

- *Assuming the CFPB imposes staggered deadlines with respect to a requirement to establish a third-party access portal, please provide input on how the CFPB should do so. For example, how should the CFPB define different classes of covered data providers that would be subject to different implementation periods? Should the CFPB use asset size, activity level, or some other metric? What would be the appropriate thresholds? Would responses to these questions change if data providers relied on screen scraping to comply with an obligation to make information available before they establish a third-party access portal? (See Outline Q53.)*

- *Assuming the CFPB imposes staggered implementation periods with respect to establishing a third-party access portal, please provide input on the appropriate time period that each class of covered data providers should have in order to come into compliance with the third-party access portal proposal under consideration. Would responses to this question change if data providers were permitted to rely on screen scraping to comply with an obligation to make information available to authorized third parties before they establish a third-party access portal? (See Outline Q54.)*

- *Should covered data providers be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption? What records could demonstrate that a service interruption to a third-party access portal has occurred? What alternatives to screen scraping should the CFPB consider to reduce interruptions to authorized third-party information access when a third-party access portal experiences a service interruption? (See Outline Q55.)*

- *To the extent screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? For example, should the CFPB require covered data providers to provide access tokens to authorized third parties to use to screen scrape so that third parties would not need a consumer's credentials to access the online financial account management portal? Alternatively, should authorized third parties be restricted from retaining consumer credentials indefinitely? For how long do authorized third parties need to retain consumer credentials? If the answer depends on the use case, please explain. (See Outline Q56.)*

The CFPB is considering various proposals related to the availability of information obtained through such third-party access portals, the security of such portals, and the impacts of such portals on the accuracy of information accessed through them.

- *Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the*

regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals? (See Outline Q57.)

- *How can the CFPB incentivize the establishment of industry-led mechanisms and fora through which disputes between ecosystem participants could be surfaced, adjudicated, and otherwise addressed? (See Outline Q58.)*

With respect to the availability of information provided through a third-party access portal, the CFPB is considering proposing that a covered data provider would not satisfy its obligations under the rule unless its portal meets certain availability requirements related to the following factors affecting the quality, timeliness, and usability of the information:

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

To ensure third-party access portals are reliably available, as defined by the above factors, the CFPB is considering proposals that would: require the establishment and maintenance of reasonable policies and procedures to ensure availability, establish performance standards related to the third-party portal availability factors, prohibit covered data provider conduct that would adversely affect the third-party portal availability factors, or some combination of the above.

Similarly, to ensure that data providers transmit consumer information accurately through third-party access portals, the CFPB is also considering proposals for covered data providers to implement reasonable policies and procedures to ensure data accuracy, establish performance

standards, and prohibit covered data provider conduct that would adversely affect the accurate transmission of consumer information, or some combination of the above.

With respect to the security of third-party access portals, the CFPB believes that nearly all—if not all—covered data providers must already comply with either the Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act (GLBA), as well as the prohibition against unfair practices. However, as noted above, the CFPB is considering a proposal in which a third-party access portal could not rely on an authorized third party possessing or retaining a consumer's credentials to authenticate the authorized third party.

- *What methods of securely authenticating an authorized third party do not require consumers to share their credentials with the authorized third party? Should the CFPB consider proposals to articulate performance standards related to authentication? If so, how should the CFPB address such topics? (See Outline Q70.)*

The CFPB is considering proposing that a covered data provider generally would be required to make information available to a third party, upon request, when the covered data provider has received certain 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,[6] and information sufficient to authenticate the third party's identity. The CFPB is seeking to ensure that third parties that do not meet these conditions are prevented from obtaining access to the information. The CFPB is considering how to address circumstances in which third parties could be prevented from getting access to information where they do not satisfy the conditions. The CFPB is also considering whether it should require covered data providers to disclose to consumers or third parties when information is not available and the reason it is not available.

- *Please provide input on the approach the CFPB is considering. What alternative approaches should the CFPB consider? Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party? Is there additional information, besides the above-described evidence,*

[6] In some circumstances the scope of information requested by an authorized third party might be ambiguous. Thus, the CFPB is considering a proposal in which a covered data provider could seek to clarify the scope of an authorized third party's request with a consumer where a covered data provider does not have enough information to know how to respond to the request.

that a covered data provider should receive before a third party should be treated as authorized to access the consumer's information? (See Outline Q73.)

- *Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before they terminate access. (See Outline Q74.)*

- *To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt (such as by providing consumers a copy of the evidence of authorization submitted by a third party), or be permitted to confirm with the consumer the authorization of a particular third party before making information available? To enable consumers to monitor third-party access to their account information, should covered data providers be required to inform consumers of which third parties are accessing information pursuant to a purported authorization? (See Outline Q75.)*

- *Please provide input on whether it would facilitate compliance or reduce costs to covered data providers and authorized third parties if covered data providers were required to follow certain specific procedures in authenticating an authorized third party's identity. Please provide input on what models the CFPB could look to for prescribing such procedures. Do all covered data providers require a uniform set of information to authenticate an authorized third party's identity prior to making information available to the authorized third party? (See Outline Q81.)*

As noted above, the CFPB is considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

- *Please provide input on whether covered data providers have the technical capacity to make information available in terms of the frequency and duration sought by authorized third parties through screen scraping, including whether there are considerations particularly relevant to small entities. (See Outline Q77.)*

- *Please provide input on whether covered data providers should be allowed to limit the frequency and duration of authorized third parties' access if covered data providers had to permit screen scraping in order to satisfy their obligations to make information available. How could they do so in a way that both minimizes their costs and does not interfere with a consumer's right to access information? (See Outline Q78.)*

E. Third party obligations (Outline part III.E)

Collection, use, and retention limits. The CFPB is considering proposals under which authorized third parties would have to limit their collection, use, and retention of consumer information to what is reasonably necessary to provide the product or service the consumer has requested.

- *Please provide input on the standard the CFPB is considering to limit third party collection, use, and retention of consumer information to what is reasonably necessary to provide the requested product or service. In providing this input, please describe any guidance the CFPB should consider to clarify the applicability of the standard or any alternative standards the CFPB should consider. (See Outline Q88.)*

Limits on collection. The CFPB is considering proposals to limit third parties' collection of consumer information to what is reasonably necessary to provide the product or service the consumer has requested. The CFPB is considering proposing that third parties would be limited to collecting consumer information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. The CFPB is also considering proposing that authorized duration would be limited by a maximum period, after which third parties would need to seek reauthorization for continued access.

- *If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties (see Outline part III.D.2.i), how would third parties using screen scraping comply with limits on collection? Would third parties employ filters or other technical solutions to limit collection? (See Outline Q90.)*

- *Please provide input on the approach the CFPB is considering that would establish a maximum durational period for all use cases, along with any alternative approaches the CFPB should consider. Please provide input on the length of the maximum durational period, including whether certain use cases should have shorter or longer maximum durational periods. (See Outline Q92.)*

- *In requiring third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties? For example, should the CFPB consider proposals that would allow third parties to:*

- *Seek reauthorization, either before authorization lapses, or within a grace period after authorization lapses?*
- *Establish a presumption of reauthorization, subject to a consumer's ability to opt out of the presumption, based on the consumer's recent use of a product or service? If so, what should be considered "recent" use?*
- *Require all authorized third parties to obtain reauthorization on the same day or during the same month each year, for all consumers?*

  (See Outline Q93.)

The CFPB is considering proposing that authorized third parties would be required to provide consumers with a simple way to revoke authorization at any point, consistent with the consumer's mode of authorization. For the purposes of the Outline, "revocation" is the mechanism by which the consumer withdraws consent from third parties they previously authorized to access their information.

- *Please provide input on the approach the CFPB is considering that would require authorized third parties to provide consumers with a mechanism through which consumers may revoke access to their information, along with costs associated with providing consumers a revocation mechanism. Please provide input on any alternative approaches the CFPB should consider, and how it could reduce costs and facilitate compliance for small entities. (See Outline Q94.)*
- *Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization, and the costs and benefits of such an approach. Is it feasible to require covered data providers to provide revocation mechanisms where screen scraping is used? (See Outline Q95.)*
- *Please provide input on whether authorized third parties should be required to report consumer revocation requests to covered data providers. What challenges or costs would be anticipated from such a requirement? (See Outline Q96.)*
- *For third parties: do you have consumer-facing tools for access revocation? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you expect it would take to develop these tools to implement the proposals under consideration? (See Outline Q139.)*

Limits on use. The CFPB is considering proposals that would limit third parties' secondary use of consumer-authorized information. The Bureau is considering defining secondary use to

mean a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including the third party's own use of consumer data and the sharing of data with downstream entities. The CFPB is considering various approaches to limiting third parties' secondary use of consumer information. General approaches the CFPB is considering include:

- Prohibiting all secondary uses.
- Prohibiting certain high risk secondary uses.
- Prohibiting any secondary uses unless the consumer opts in to those uses.
- Prohibiting any secondary use if the consumer opts out of those uses.

- *Please provide input on the various approaches the CFPB is considering to limit authorized third parties' use of consumer information and any alternative approaches the CFPB should consider. How could the CFPB design such approaches to facilitate compliance by small entities? Should the CFPB propose to include a standard for defining "high risk," or provide a specific list of uses that it deems to be "high risk," or both? (See Outline Q99.)*

- *Would the conditions restricting certain secondary uses of consumer data impede products or business models used by third parties? (See Outline Q144.)*

- *Please provide input on whether the rule should allow consumer information that has been de-identified to be used by third parties beyond what is reasonably necessary to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"? (See Outline Q102.)*

Limits on retention. The CFPB is considering proposing that authorized third parties would need to limit their retention of consumer-authorized information. Specifically, the CFPB is considering a proposal in which authorized third parties would need to delete consumer information that is no longer reasonably necessary to provide the consumer's requested product or service, or upon the consumer's revocation of the third-party's authorization. The CFPB is also considering a limited exception to the deletion requirements for compliance with other laws. For the purposes of the Outline, "deletion" is the complete removal of previously collected consumer information.

- *For third parties: do you have consumer-facing tools for deletion? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you*

expect it would take to develop these tools to implement the proposals under consideration? (See Outline Q138.)

- *Should an authorized third party be required to delete information upon receipt of the consumer's revocation request? Under what circumstances should a third party be allowed to retain information beyond receipt of the consumer's revocation request? For example, is retention of data after receipt of a revocation request necessary for compliance with other laws and regulations? (See Outline Q104).*

- *Are there any use cases or services for which consumers might seek deletion of some consumer-authorized information that the authorized third party collected, but not want to revoke that third party's ongoing access to their information from a covered data provider? Should deletion of consumer-authorized information be required when authorization lapses at the end of a durational period? (See Outline Q107-108.)*

- *Would the proposals requiring the deletion of consumer data when consumer authorization lapses or is revoked impede products or business models used by third parties? (See Outline Q143.)*

- *If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties, what deletion requirements should be imposed on authorized third parties that utilize screen scraping and potentially collect more information than what is reasonably necessary to provide the product or service? (See Outline Q109.)*

- *Should the CFPB consider more flexibilities related to retention beyond an exception for compliance with other laws? For example, should the CFPB consider allowing authorized third parties to retain de-identified consumer information? For what purposes might authorized third parties seek to retain de-identified consumer information, and by what standards should consumer information be de-identified? (See Outline Q110.)*

Data security requirements. The CFPB is considering a proposal to require authorized third parties to implement data security standards. Although the CFPB believes that authorized third

parties are likely subject to the GLBA safeguards framework,[7] the CFPB is considering whether it should impose specific data security standards on authorized third parties under the rule. General approaches the CFPB is considering include:

- Requiring authorized third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third parties' size and complexity, and the volume and sensitivity of the consumer information at issue. This approach could be combined with a provision incorporating the Safeguards Rule or Guidelines as a specific option for complying with any data security requirement under the CFPB's rule.
- Alternatively, requiring compliance with the Safeguards Rule or Guidelines.

- *For third parties: what data security practices do you currently apply to consumer data? Do you tailor your information security approach to an existing legal or industry standard, such as the safeguards framework, and if so, which one(s)? Would you follow the Safeguards Rule or the Safeguards Guidelines if either were incorporated as an option for complying with any data security requirement under the CFPB's rule? (See Outline Q112.)*

Data accuracy and dispute resolution requirements. The CFPB is considering a proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the data that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers.

- *Are inaccuracies in consumer-authorized information used by authorized third parties more likely to come from errors in data made available by covered data providers or from errors in any manipulation, calculation, or subsequent transmission performed by third parties? Could third-party policies and procedures address errors in data that were inaccurate when originally accessed from a covered data provider? (See Outline Q115.)*

[7] The safeguards framework generally requires financial institutions to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institutions' activities, and the sensitivity of the customer information at issue. These safeguards must include specific elements set forth in the regulations.

- *Should policies and procedures to ensure accuracy include addressing disputes submitted by consumers? When does addressing such disputes require an investigation and a response to the consumer? (See Outline Q116.)*

Disclosure obligations. The CFPB is considering proposals related to disclosure requirements applicable to authorized third parties' ongoing collection, use, and retention of consumer-authorized information. The CFPB is also considering proposing that authorized third parties would need to provide consumers with a mechanism to request information about the extent and purposes of the authorized third party's access.

F. Record retention obligations (Outline part III.F)

The CFPB is considering proposing record retention requirements for covered data providers and authorized third parties to demonstrate compliance with certain requirements of the rule.

- *Should the rule require covered data providers and authorized third parties to maintain policies and procedures to comply with their obligations under the rule, beyond the areas already identified in this Outline? What costs would be associated with maintaining policies and procedures? (See Outline Q120.)*

G. Implementation period (Outline part III.G)

The CFPB seeks to ensure that consumers have the benefit of a final rule within a short timeframe, while also ensuring that covered data providers and authorized third parties have sufficient time to implement the rule. The CFPB is also seeking feedback on whether certain covered data providers should not be subject to a third-party access portal requirement on the compliance date of the final rule, and instead should be given additional time to build a compliant third-party access portal.

- *Please provide input on an appropriate implementation period for complying with a final rule other than a potential third-party access portal requirement.*[8] *What alternative approaches should the CFPB consider? Are there any aspects of the CFPB's proposals under consideration that could be particularly time consuming or costly for*

[8] See section D above for questions about the implementation period with respect to the potential third-party access portal requirement.

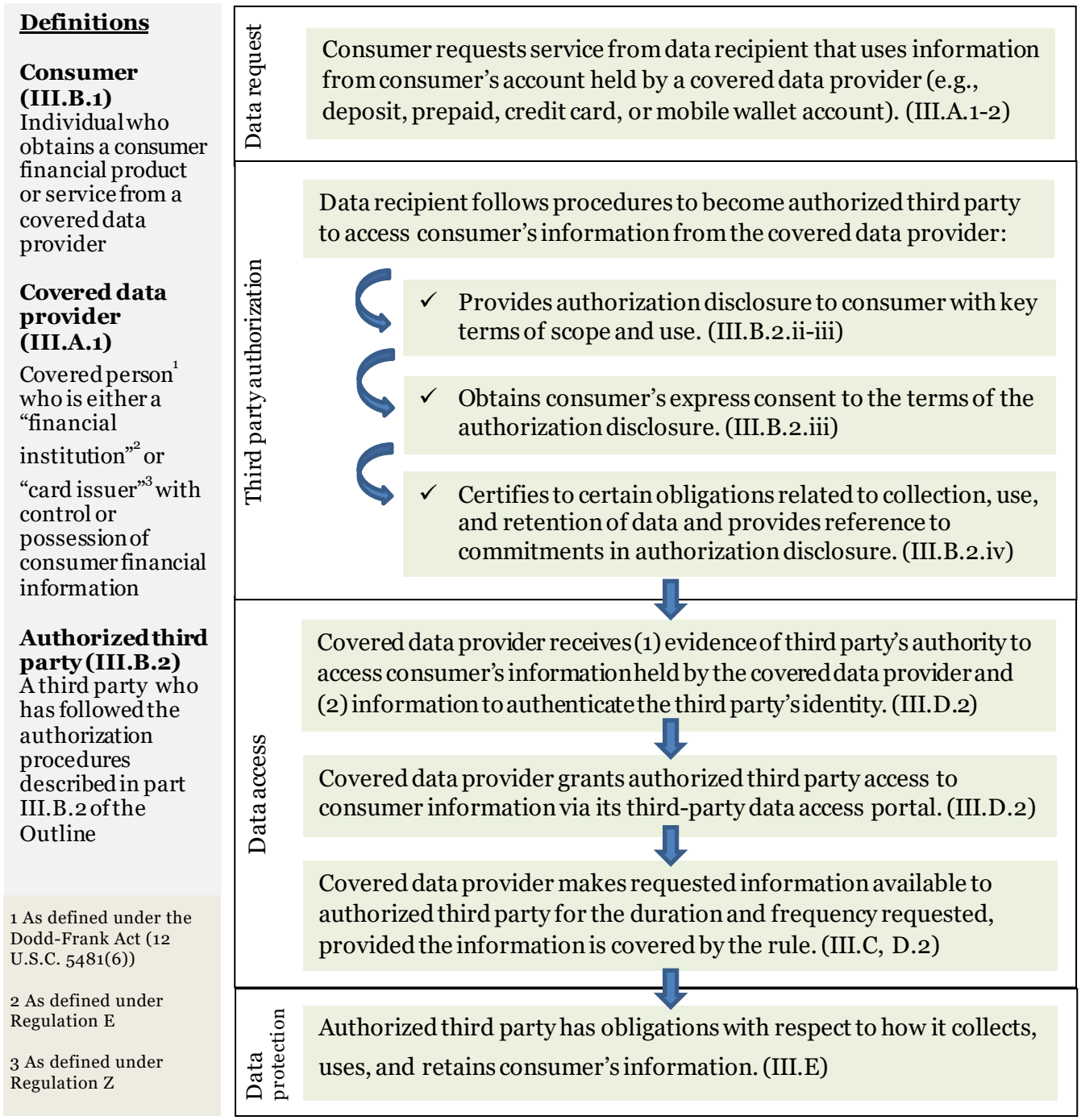
a covered data provider or a third party to implement? Are there any factors outside a covered data provider's or authorized third party's control that would affect its ability to prepare for compliance? (See Outline Q121.)

- *The CFPB recognizes that small covered data providers and authorized third parties might not be able to comply with some of the proposals under consideration on the same timeframe as larger covered data providers and authorized third parties. How much time would small entities need to implement the proposals under consideration, other than the third-party access portal proposal,[9] including updating policies, procedures, processes, and employee training programs? (See Outline Q122.)*

[9] See the questions in section D above.

Appendix: Illustration of Interaction of Proposals Under Consideration (Third-Party Access)

The graphic below illustrates how the CFPB's proposals under consideration described in the Outline would apply to a hypothetical transaction involving consumer-authorized information access through a third-party data access portal. See references to sections of the Outline (in parentheses) to read the proposals under consideration in greater detail.



APPENDIX F: PANEL OUTREACH MEETINGS PRESENTATION MATERIALS

See attached.

Required Rulemaking on Personal Financial Data Rights: SBREFA Panel Meetings

Panel Meeting #1 | February 1, 2023

Panel Meeting #2 | February 2, 2023

Consumer Financial Protection Bureau

Disclaimer

This presentation is being made by a Consumer Financial Protection Bureau representative on behalf of the Bureau. It does not constitute legal interpretation, guidance, or advice of the Consumer Financial Protection Bureau. Any opinions or views stated by the presenter are the presenter's own and may not represent the Bureau's views.

Privacy Act Statement (5 U.S.C. 552a(e)(3))

The information you provide the Consumer Financial Protection Bureau (Bureau) during this session will facilitate a discussion related to the 1033 rulemaking.

The information you provide to the Consumer Financial Protection Bureau (CFPB) will be used to register you for events sponsored by the CFPB and to keep you updated on our work. The CFPB may collect personally identifiable information (PII) such as your name, email address, company, and information about any necessary accommodations. Information collected will be treated in accordance with the System of Records Notice (SORN), CFPB.013 External Contact Database. The event recording may be shared with CFPB staff. Although the CFPB does not anticipate further disclosing the information provided, it may be disclosed as indicated in the Routine Uses described in the SORN. Direct identifying information will only be used by the CFPB to facilitate the event and will be kept Private except as required by law. This collection of information is authorized by Public Law 111-203, Title X, sections 1011, 1012, 1021, codified at 12 U.S.C. 5491, 5492, 5511.

Please note that the session will be recorded, and the recording may capture your name, webcam image, and voice. You may keep your webcam and microphone off if you do not wish for your image or voice to be recorded.

Participation in this event is voluntary. However, if you do not consent to the recordings, you will not be able to participate in the session.

cfpb Consumer Financial Protection Bureau

SBREFA Meeting Logistics

Connecting audio

- Use your computer for audio with a headset to reduce background noise. Or have WebEx call your phone.
- If you prefer to connect to audio only:
  US Toll for Call
  +1-xxx-xxx-xxxx
  Access code xxxx
  Passcode xxxxx
- If you experience audio problems, click the "Audio & Video" button in the top toolbar.

Mute

All **attendees are automatically muted** upon entry.

Manage your view

- Click on "Layout" located to the left of the Participants view to change your view.

Speakers

If you are a presenter or panelist and are not speaking, **please mute and turn off your camera.**

Closed Captions

If you need closed captioning, the access link will be posted in the Chat box, located in the lower right side of the screen.

Technical Issues

If you are having technical difficulties, please send a Chat to the "Host" or email XXX.

Ask a question

During the session if you would like to ask a question, please raise your hand. The raised hand function can be found on the right-hand side of your screen. Your question will be answered in the order in which your hand was raised. Please **turn off your raised hand** once your question has been answered.

If you do not want to raise your hand you can ask your question using the **Chat bubble**. It can be found on the lower right-hand side of the screen. Please address your question to "All Panelists".

cfpb Consumer Financial Protection Bureau

Day 1

Day 1: Agenda

Time (Eastern)	Session
12:00 – 12:30 PM	Welcome
12:30 – 12:45 PM	Segment 1: Overview of the proposals under consideration
12:45 – 1:15 PM	Segment 2: Coverage of data providers
1:15 – 2:00 PM	Segment 3: Recipients of information
2:00 – 2:45 PM	Segment 4: Types of information that would need to be made available
2:45 – 3:30 PM	Mid-session break #1
3:30 – 4:30 PM	Segment 5: How and when information would need to be made available, part 1
4:30 – 4:40 PM	Mid-session break #2
4:40 – 5:25 PM	Segment 5: How and when information would need to be made available, part 2
5:25 – 5:30 PM	Closing remarks

Segment 1: Overview of the proposals under consideration

Consumer Financial Protection Bureau

Overview of proposals under consideration

- Issues with consumer data access
- Dodd-Frank Act section 1033

Hypothetical illustration of interaction of proposals under consideration (Third-Party Access)

Definitions

Consumer (III.B.1)
Individual who obtains a consumer financial product or service from a covered data provider

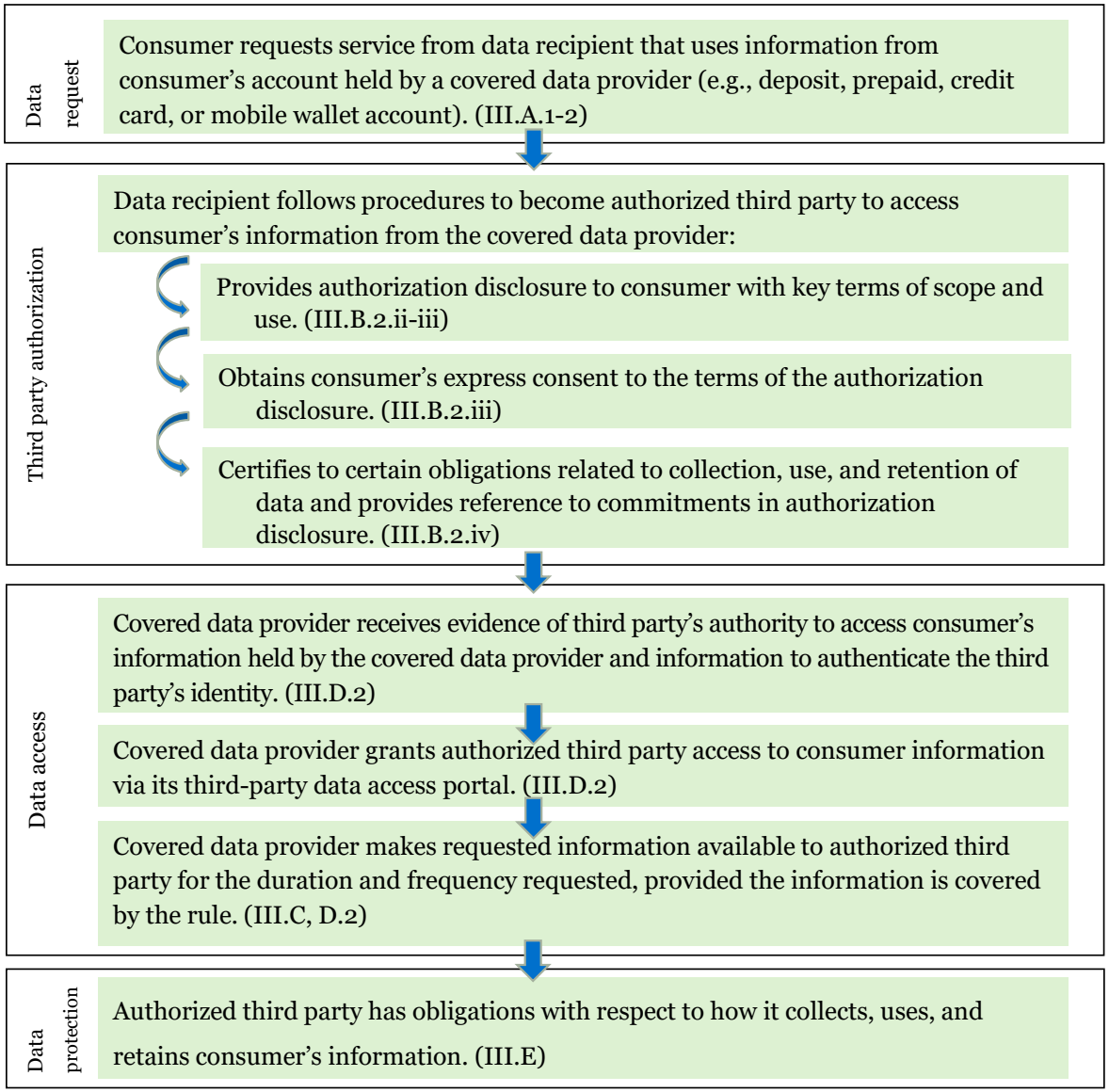
Covered data provider (III.A.1)
Covered person[1] who is either a "financial institution"[2] or "card issuer"[3] with control or possession of consumer financial information

Authorized third party (III.B.2)
A third party who has followed the authorization procedures described in part III.B.2 of the Outline

[1] As defined under the Dodd-Frank Act (12 U.S.C. 5481(6))

[2] As defined under Regulation E

[3] As defined under Regulation Z



General questions

The following apply to all the CFPB's proposals under consideration:

- *Do any statutes or regulations, duplicate, overlap, or conflict with the proposals under consideration? (Outline Q1-2)*
- *What factors disproportionately affecting small entities should the CFPB be aware of when evaluating the proposals under consideration? (Outline Q3, 136, 140)*
- *Please provide input on the approaches the CFPB is considering* ***and any alternatives*** *the CFPB should consider.*
- *Please provide input on any costs or challenges you foresee with the enforcement or supervision of the proposals under consideration. (Outline Q4)*
- *Would the proposals under consideration affect the cost and availability of credit to small entities? (Outline Q149)*

Segment 2: Coverage of data providers (Outline part III.A)

Covered data providers

Entity	Definition	Examples
Financial institution	§ 1005.2(i) of Regulation E (12 CFR part 1005)	• Banks and credit unions that directly or indirectly hold a consumer asset account (incl. a prepaid account) • Other persons that directly or indirectly hold an asset account • Persons that issue an access device and agree with a consumer to provide EFT services
Card issuer	§ 1026.2(a)(7) of Regulation Z (12 CFR part 1026)	• Persons that issue a credit card and those persons' agents with respect to the card

Covered accounts

Under the proposals the CFPB is considering:

- Regulation E "financial institutions" would be covered data providers with respect to information that pertains to an "account" as defined in Regulation E § 1005.2(b).
- Regulation Z "card issuers" would be covered data providers with respect to information that pertains to a "credit card account under an open-end (not home-secured) consumer credit plan" as defined in Regulation Z § 1026.2(a)(15)(ii).

Discussion questions

- *How could the CFPB clarify coverage of the proposals under consideration? (Outline Q5)*

Potential exemptions

- The CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers.
- The CFPB is interested in whether there are ways to design the proposals described in this Outline to reduce impact on covered data providers.

Discussion questions

- *Should the CFPB exempt certain covered data providers from any particular proposals under consideration? (Outline Q6)*
- *For which covered data providers would such exemptions be appropriate, and why? (Outline Q6)*
- *Which proposals should such data providers be exempt from, and why? (Outline Q6)*

Segment 3: Recipients of information (Outline part III.B)

Consumers and third parties

- The CFPB is considering proposals that would address a covered data provider's obligation to make information available upon request directly to a consumer (direct access) and to authorized third parties (third-party access).

Third-party authorization procedures

- Under the proposals the CFPB is considering, to be an authorized third party, the third party would need to:
  1. Provide an "authorization disclosure" to inform the consumer of key terms of access;
  2. Obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and
  3. Certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.

Third-party authorization procedures – authorization disclosure

- The CFPB is considering proposing that the authorization disclosure would contain:
  - Key scope and use terms;
  - A reference to the third party's certification to certain obligations regarding collection, use, and retention of the consumer's information; and
  - A request for consent to access the consumer's information
- The CFPB is also considering proposing timing and formatting requirements for the authorization disclosure.
  - Close in time
  - Clear and conspicuous and segregated from other material

Discussion questions

- *How do the proposals under consideration compare to the authorization procedures that third parties and/or covered data providers currently employ? (See Outline Q12)*
- *Where a data recipient relies on a data aggregator to access consumer data from the covered data provider, what authorization procedures should apply to the data recipient, the data aggregator, or both parties? (Outline Q14)*

Discussion questions

- *Please describe any additional content that should be included in the authorization disclosure or whether there are circumstances in which more limited disclosures would be appropriate. (Outline Q17)*
- *Please provide input on whether the full certification statement should be included in the authorization disclosure. (Outline Q21)*
- *Please provide input on whether the CFPB should include any particular requirements or restrictions on the timing and format of the authorization disclosure. (Outline Q19)*

Segment 4: Types of information that would need to be made available (Outline part III.C)

Scope of information

- The Outline sets forth six categories of information the CFPB is considering proposing that covered data providers would need to make available with respect to covered accounts.

Scope of information

Category of information	Examples of data elements	Generally provided on an online account management portal?
Periodic statement information for settled transactions and deposits (Reg E, Reg DD, and Reg Z)	• Payment information • Fee information • Interest credited or charged • APY/APR • Account balance • Account number	Yes
Information regarding prior transactions and deposits that have not yet settled	• See above	Yes
Other information about prior transactions not typically shown on periodic statements or portals	• The bank into which a card, ACH, check, or other transaction was deposited by a merchant or other payee • Name and account number at the bank of the merchant or other payee that deposited the payment transaction	No

Scope of information

Category of information	Examples of data elements	Generally provided on an online account management portal?
Online banking transactions that the consumer has set up but that have not yet occurred	• 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" or "identification" number with a biller • Amounts of bills and dates on which the consumer would like payments to be transferred	Yes
Account identity information	• Name, age, gender, marital status, number of dependents • Race, ethnicity, citizenship or immigration status • Address, phone number, email address • Date of birth • Social Security number	Some yes and some no

Scope of information

Category of information	Examples of data elements	Generally provided on an online account management portal?
Other information	• Consumer reports from consumer reporting agencies used in deciding whether to provide a financial product or service to a consumer • Fees that may be assessed in connection with covered accounts • Bonuses, rewards, discounts, incentives that may be provided • Information about breaches that exposed a consumer's information	Some yes and some no

Exceptions

- Dodd-Frank Act section 1033(b) sets forth four exceptions to the section 1033(a) requirement to make information available:
  - Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
  - Any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
  - Any information required to be kept confidential by any other provision of law; or
  - Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

Current and historical information

- The CFPB is considering proposing that a covered data provider would need to make available the most current information that the covered data provider has in its control or possession at the time of a request for current information.
- The CFPB is also considering proposals under which a covered data provider would be required only to make available information going as far back in time as that covered data provider makes transaction history available directly to consumers.

Discussion questions

- *How should the CFPB interpret the exceptions set forth in Dodd Frank Act section 1033(b)? (Outline Q30-37)*
- *Which data elements should be covered under the exceptions? (Outline Q30-37)*

Mid-session break #1 (45 mins.)

Segment 5: How and when information would need to be made available (Outline part III.D)

General proposals

- The CFPB is considering proposals to define the methods and the circumstances in which a covered data provider would need to make information available with respect to both:
  - Direct access (where a consumer directly obtains data about their own account from the covered data provider), and
  - Third-party access (where a third party accesses data from the covered data provider on the consumer's behalf).

Direct access

- For direct access, the CFPB is considering proposing that a covered data provider would be required to:
  - Make information available if it has enough information from the consumer to reasonably authenticate the consumer's identity and reasonably identify the information requested.
  - Make available all the information that would be covered by the proposals under consideration through online financial account management portals.
  - Allow consumers to export the information in both human and machine readable formats.

Direct access – export in machine readable format

- For example,
  - Many data providers allow consumers to export a history of their transactions in file formats that present the information in a consumer-friendly display and file formats such that the file could be imported or read into a computer system for further processing (e.g., a .CSV file format).

Third-party access

- The CFPB is considering proposing that a covered data provider generally would be required to make information available to a third party, upon request, when the covered data provider has received:
  - Certain 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.

Discussion questions

- *Do covered data providers currently charge consumers or third parties specific fees to access information or export information in a human or machine readable format? What would be the impact if covered data providers were or were not restricted from charging fees? (Outline Q41, Q63)*
- *Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate? (Outline Q82)*

Discussion questions

- *Please provide input on what steps the CFPB should take to prevent third parties that do not satisfy the conditions described above from obtaining information. (Outline Q72)*
- *Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party? (Outline Q73)*
- *Is there additional information, besides the above-described evidence, that a covered data provider should receive before a third party should be treated as authorized to access the consumer's information? (Outline Q73)*

Discussion questions

- *Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before terminating the third party's access. (Outline Q74)*
- *To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt, or be permitted to confirm with the consumer the authorization of a particular third party before making information available? (Outline Q75)*
- *To enable consumers to monitor third-party access to their account information, should covered data providers be required to inform consumers of which third parties are accessing information pursuant to a purported authorization? (Outline Q75)*

Third-party access portals

- The CFPB is considering proposing that a covered data provider would need to establish and maintain a third-party access portal that does not require the authorized third party to possess or retain consumer credentials.

Discussion questions

- *Please provide input on how covered data providers' customers can share their account information with third parties today. (Outline Q51)*
- *With respect to covered data providers with a third-party access portal or comparable system that was built primarily in-house or by a software provider pursuant to a contract, what are the upfront and ongoing costs? (Outline Q126, 127)*
- *With respect to covered data providers without a third-party access portal or comparable system, would a third-party access portal need to be developed in-house or be procured from a software provider? (Outline Q128)*
- *With respect to covered data providers that have not yet established a third-party access portal, should the CFPB require that they make information available to authorized third parties before they establish such a portal? Would this require that they permit screen scraping? (Outline Q52)*

Mid-session break #2 (10 mins.)

Third-party access portals – screen scraping

- The CFPB is considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

Discussion questions

- *Should covered data providers be required to permit screen scraping when their third-party access portal experiences a service interruption? (Outline Q55)*
- *If screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? (Outline Q56)*
- *Are there alternatives to screen scraping that a covered data provider could implement to make information available to authorized third parties in electronic form? (Outline Q52)*

Discussion questions

- *Please provide input on whether covered data providers have the technical capacity to make information available in terms of the frequency and duration sought by authorized third parties through screen scraping. (Outline Q77)*
- *Please provide input on whether covered data providers should be allowed to limit the frequency and duration of authorized third parties' access if covered data providers had to permit screen scraping in order to satisfy their obligations to make information available. (Outline Q78)*

Third-party access portals – portal standards

- Regarding the third-party access portals, the CFPB is considering various proposals related to the:
  - Availability of information obtained through such portals;
  - Impacts of such portals on the accuracy of information accessed through them; and
  - Security of such portals.

Third-party access portals – portal standards

	CFPB proposals under consideration
Availability of information obtained through a third-party access portal	A covered data provider would not satisfy its obligations unless its portal meets certain availability requirements related to these factors: • The general reliability of a third-party access portal in response to electronic requests to the portal for information by an authorized third party (uptime); • The length of time between the submission of a call to a third-party access portal and a response (latency); • System maintenance and development that involve both planned interruptions of data availability (planned outages) and responses to unplanned interruptions (unplanned outages); • Responses to notifications of errors from an authorized third party (error response); and • Limitations or restrictions on fulfilling a call from an authorized third party even when data are otherwise available (access caps).

Third-party access portals – portal standards

	CFPB proposals under consideration
Availability and accuracy of information accessed through a third-party access portal	• Reasonable policies and procedures; • Performance standards; • Prohibitions on covered data provider conduct; • Or some combination of the above.
Security of a third-party access portal	A third-party access portal could not rely on an authorized third party possessing or retaining a consumer's credentials to authenticate the authorized third party.

Discussion questions

- *Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. (Outline Q57)*
- *How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals? (Outline Q57)*
- *How can the CFPB incentivize the establishment of industry-led mechanisms and fora through which disputes between ecosystem participants could be surfaced, adjudicated, and otherwise addressed? (Outline Q58)*

Closing remarks

Welcome

Consumer Financial Protection Bureau

Day 2: Agenda

Time (Eastern)	Session
12:00 – 12:10 PM	Welcome
12:10 – 1:00 PM	Segment 6: Third party obligations, part 1
1:00 - 1:10 PM	Mid-session break #1
1:10 – 2:00 PM	Segment 6: Third party obligations, part 2
2:00 – 2:45 PM	Segment 7: Record retention obligations and implementation period
2:45 – 3:30 PM	Mid-session break #2
3:30 – 5:00 PM	Segment 8: Potential impacts on small entities
5:00 – 5:30 PM	Closing remarks

Segment 6: Third party obligations (Outline part III.E)

Limits on collection, use, and retention

- The CFPB is considering proposals under which authorized third parties would have to limit their collection, use, and retention of consumer information to what is reasonably necessary to provide the product or service the consumer has requested.
- The CFPB is requesting feedback on whether those obligations should apply to the data recipient, the data aggregator, or both parties in circumstances where a data recipient relies on a data aggregator to access the consumer's information.

Limits on collection

	CFPB proposals under consideration
Limits on collection	• Third parties would be limited to collecting consumer information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. • Authorized duration would be limited by a maximum period, after which third parties would need to seek reauthorization for continued access. • Authorized third parties would be required to provide consumers with a simple way to revoke authorization at any point, consistent with the consumer's mode of authorization.

Discussion questions

- *If screen scraping were a method by which covered data providers could satisfy their obligation to make information available to authorized third parties, how would third parties using screen scraping comply with limits on collection? (Outline Q90)*
- *In requiring third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties? (Outline Q93)*
- *Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization. Is it feasible to require covered data providers to provide revocation mechanisms where screen scraping is used? (Outline Q95)*

Limits on use

	CFPB proposals under consideration

Limits on use	• Defining secondary use to mean a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including the third party's own use of consumer data and the sharing of data with downstream entities.
	• General approaches to limiting third parties' secondary use of consumer information may include:
	  • Prohibiting all secondary uses.
	  • Prohibiting certain high risk secondary uses.
	  • Prohibiting any secondary uses unless the consumer opts into those uses.
	  • Prohibiting any secondary use if the consumer opts out of those uses.

Discussion questions

- *Regarding the proposal under consideration for secondary use, should the CFPB propose to include a standard for defining "high risk," or provide a specific list of uses that it deems to be "high risk," or both? (Outline Q99)*
- *Would the conditions restricting certain secondary uses of consumer data impede products or business models used by third parties? (Outline Q144)*
- *Please provide input on whether the rule should allow consumer information that has been de-identified to be used by third parties beyond what is reasonably necessary to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"? (Outline Q102)*

Limits on retention

	CFPB proposals under consideration
Limits on retention	• Authorized third parties would need to delete consumer information that is no longer reasonably necessary to provide the consumer's requested product or service, or upon the consumer's revocation of the third-party's authorization. • The CFPB is also considering a limited exception to the deletion requirements for compliance with other laws.

Discussion questions

- *Should an authorized third party be required to delete information upon receipt of the consumer's revocation request? Under what circumstances should a third party be allowed to retain information beyond receipt of the consumer's revocation request? (Outline Q104)*
- *Would the proposals requiring the deletion of consumer data when consumer authorization lapses or is revoked impede products or business models used by third parties? (Outline Q143)*
- *If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties, what deletion requirements should be imposed on authorized third parties? (Outline Q109)*
- *Should the CFPB consider allowing authorized third parties to retain de-identified consumer information? (Outline Q110)*

Mid-session break #1 (10 mins.)

Data security requirements

- The CFPB is considering requiring authorized third parties to implement data security standards.
- Authorized third parties are likely subject to the GLBA safeguards framework; however, the CFPB is considering whether it should impose specific data security standards on authorized third parties. For example,
  - Requiring authorized third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third parties' size and complexity, and the volume and sensitivity of the consumer information at issue.
  - Alternatively, requiring compliance with the Safeguards Rule or Guidelines.

Discussion questions

- *What data security practices do third parties currently apply to consumer data? (Outline Q112)*
- *Do third parties tailor their information security approach to an existing legal or industry standard, such as the safeguards framework, and if so, which one(s)? (Outline Q112)*
- *Would third parties follow the Safeguards Rule or the Safeguards Guidelines if either were incorporated as an option for complying with any data security requirement under the CFPB's rule? (Outline Q112)*

Data accuracy and dispute resolution requirements

- The CFPB is considering requiring authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the data that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers.

Discussion questions

- *Are inaccuracies in consumer-authorized information used by authorized third parties more likely to come from errors in data made available by covered data providers or from errors in any manipulation, calculation, or subsequent transmission performed by third parties? (Outline Q115)*
- *Could third-party policies and procedures address errors in data that were inaccurate when originally accessed from a covered data provider? (Outline Q115)*
- *Should policies and procedures to ensure accuracy include addressing disputes submitted by consumers? When does addressing such disputes require an investigation and a response to the consumer? (Outline Q116)*

Disclosure obligations

- The CFPB is considering proposals related to disclosure requirements applicable to authorized third parties' ongoing collection, use, and retention of consumer-authorized information.
- The CFPB is also considering proposing that authorized third parties would need to provide consumers with a mechanism to request information about the extent and purposes of the authorized third party's access.

Segment 7: Record retention obligations and implementation period (Outline part III.F and G)

Record retention obligations

- The CFPB is considering proposing record retention requirements for covered data providers and authorized third parties to demonstrate compliance with certain requirements of the rule.

Discussion questions

- *Should the rule require covered data providers and authorized third parties to maintain policies and procedures to comply with their obligations under the rule, beyond the areas already identified in this Outline? What costs would be associated with maintaining policies and procedures? (Outline Q120)*

Implementation period

- The CFPB is seeking to ensure that consumers have the benefit of a final rule within a short timeframe, while also ensuring that covered data providers and authorized third parties have sufficient time to implement the rule.
- In addition to considering a general implementation for a final rule, the CFPB is seeking feedback on whether certain covered data providers should not be subject to a third-party access portal requirement on the compliance date of the final rule, and instead should be given additional time to build a compliant third-party access portal.

Discussion questions

- *Are there any aspects of the CFPB's proposals under consideration that could be particularly time consuming or costly for a covered data provider or a third party to implement? (Outline Q121)*
- *How much time would small entities need to implement the proposals under consideration, other than the third-party access portal proposal, including updating policies, procedures, processes, and employee training programs? (Outline Q122)*

Mid-session break #2 (45 mins.)

Segment 8: Potential impacts on small entities (Outline part IV)

Data providers and third parties

- Discuss costs separately for:
  - Covered data providers
  - Third parties (data recipients or data aggregators)
- Focus on largest direct implementation costs, some discussion of additional impacts
- Limited data on costs – estimates based on market research and discussions with industry participants
  - Open to feedback or data on all estimates

Implementation processes and costs – covered data providers

- Largest expected costs: building and maintaining third-party access portal
  - Either primarily obtain from a vendor (e.g., core banking provider) or primarily develop in-house
  - Assume data providers already have a consumer-facing portal, electronic records
- Outline assumes all covered data providers would *eventually* need to implement a third-party access portal and direct access through consumer-facing portal

Implementation processes and costs – covered data providers' third-party access portal

- Approach #1: Primarily contract with a vendor

Expense	Considerations	Upfront costs	Ongoing costs
Ongoing, monthly contract with vendor	Likely to scale with number of accounts (*e.g.*, XX cents per account per month)		<$1,000 to $50,000 per month
Update standard disclosures, policies and procedures	Est. from prior rules	$2,500 to $4,100	
Legal and compliance review	Est. from prior rules	$3,000 to $7,600	

- Additional costs covered by main contract – recordkeeping and providing disclosures

Implementation processes and costs – covered data providers' third-party access portal

- Approach #2: Primarily build portal in-house

Expense	Considerations	Upfront costs	Ongoing costs
Staffing to build third-party access portal	Assume 2,600 to 5,200 hours of work by software developers or similar staff @ hourly total comp. of $83.10	$216,000 to $432,000	
Staffing to maintain third-party access portal	Assume 500 to 1,000 hours annually by software developers or similar staff		$42,000 to $83,000 per year
Computer hardware and service costs	Depends on whether implemented on premises, renting servers, or w/ cloud computing services	Less than staffing costs, developing further estimates	Less than staffing costs, developing further estimates
Update standard disclosures, policies and procedures	Est. from prior rules	$2,500 to $4,100	
Legal and compliance review	Est. from prior rules	$3,000 to $7,600	

  - Additional costs covered by building/maintaining portal – recordkeeping and providing disclosures

Discussion questions – covered data providers

- For covered data providers without a third-party access portal or comparable system:
  - *Under the proposals under consideration, would you expect that you would develop a third-party access portal in-house or procure one from a software provider?* (Outline Q128)
  - *If you would procure a portal from a software provider, would you expect to use the core banking provider of your other technology services?*
- For covered data providers who have implemented a third-party access portal or comparable system:
  - *What were your costs to implement the portal?* (Outline Q126, Q127)
  - *Were there any unexpected costs or difficulties in building the portal or system? Were there any additional costs not captured above? Are the overall costs lower or higher than the CFPB's estimates?* (Outline Q129)
  - *What is the portal's target uptime or reliability standard? What costs were incurred to meet that standard?* (Outline Q130, Q131)

Implementation processes and costs – third parties

- The proposals under consideration may require third parties to modify existing systems to meet the conditions required for consumer-authorized access, such as:
  - Providing authorization disclosure and certification statement
  - Mechanisms for revocation of authorization and deletion
  - Implementing limitations on data collection, use, and retention
  - Potentially providing ongoing disclosures and reauthorization
  - Record retention

Implementation processes and costs – third parties

- Where data aggregators facilitate consumer-authorized access, some costs may be borne by data aggregators rather than data recipients
  - For example, data aggregators may provide the authorization disclosure and certification statement on behalf of the data recipient
- Third parties already in compliance with the California Consumer Privacy Act (CCPA) or international data privacy laws may have lower implementation costs if requirements overlap

Implementation processes and costs – third parties

- Potential implementation costs

Expense	Considerations	Upfront costs	Ongoing costs
Staffing to develop authorization disclosure and certification statement	Assume 1,000 hours of work by software developers or similar staff @ hourly total comp. of $83.10	$83,000	
Build and maintain systems for revocation requests, authorization duration tracking, deletion, and record retention	Est. based on Regulatory Impact Assessment of CCPA	Up to $75,000	Less than upfront, developing further estimates
Update policies and procedures	Est. from prior rules	$4,300	
Legal and compliance review	Est. from prior rules	$3,900	

Cost and availability of credit

- Do not expect substantial impacts on cost or availability of credit for small entities
  - Impacts possible through cost pass-through, market contraction, increased data access for underwriting business credit
- Are there additional channels that could affect the cost and availability of credit to small entities?

Discussion questions – third parties

- For third parties:
  - *Do you currently provide disclosures or other information to consumers within your own platform? What would be the expected costs to modify these systems to satisfy the proposals under consideration?* (Outline Q137)
  - *Do you have consumer-facing tools for access revocation and data deletion? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you expect it would take to develop these tools to implement the proposals under consideration?* (Outline Q139)

Discussion questions on additional impacts

- For data providers:
  - *Does existing consumer-authorized access generally complement or compete with your own products and services? Has such data access led to change in consumers' use of your own products and services? Has such data access led you to develop new products or services due to changing consumer expectations?* (Outline Q142)
- For third parties:
  - *Would any of your products or business models be impeded by the proposals under consideration due to (a) deletion requirements, (b) restrictions on certain secondary uses, (c) limitations on data availability, or (d) periodic reauthorization?* (Outline Q144-Q147)

Closing remarks

Submitting written feedback

- SERs are encouraged to submit written feedback.
- Your feedback will help inform the written SBREFA Panel Report.
- Deadline for submission is **February 15, 2023**, in order to be considered and incorporated into the Panel Report.
- Send feedback to: Financial_Data_Rights_SBREFA@cfpb.gov
- Written feedback from SERs will be appended to the SBREFA panel report, which will be made part of the public rulemaking docket.
  - If you are considering submitting proprietary or confidential business information, please contact us in advance to discuss whether and how that information should be provided.
  - Written feedback will be shared with SBA OA and OIRA.

Thank you!

Consumer Financial Protection Bureau