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.*