Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

October 27, 2022

# High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights

In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Section 1033(a) of the Dodd-Frank Act authorizes the Consumer Financial Protection Bureau (CFPB) to prescribe rules requiring "a covered person [to] make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[1]

The Bureau is now in the process of writing regulations to implement section 1033. Under the process established by Congress in the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), the Bureau is required to consult with representatives of small entities likely to be affected directly by the regulations the Bureau is considering proposing and to obtain feedback on the likely impacts the rules the Bureau is considering would have on small entities.

[1] Dodd-Frank Act section 1033, 124 Stat. 2008 (codified at 12 U.S.C. 5533(a)). The term "covered person" is defined at section 1002(6) of the Dodd-Frank Act. *See* 12 U.S.C. 5481(6).

This document provides a high-level summary of the regulatory provisions the CFPB is considering proposing, as described more fully in its Outline of Proposals and Alternatives Under Consideration (Outline). These proposals address the following topics:

- Coverage of data providers who would be subject to the proposals under consideration;[2]
- Recipients of information, including consumers and authorized third parties;[3]
- The types of information that would need to be made available;
- How and when information would need to be made available, including when information made available to consumers directly and to third parties authorized to access information on their behalf;
- Third party obligations;
- Record retention obligations; and
- Implementation period.

The Appendix illustrates how the CFPB's proposals under consideration would apply to a hypothetical transaction involving data access to an authorized third party.

**Discussion questions.** This summary includes questions drawn from the Outline, selected to solicit feedback from small entity representatives on specific topics. However, the CFPB is interested in input from SERs on all aspects of the proposals under consideration and any alternatives the CFPB should consider.

---

[2] For purposes of the Outline, a "data provider" means a covered person with control or possession of consumer financial data.

[3] For purposes of the Outline, "third party" refers, generally, to data recipients or data aggregators. "Data recipient" means a third party that uses consumer-authorized information access to provide (1) products or services to the authorizing consumer, or (2) services used by entities that provide products or services to the authorizing consumer. "Data aggregator" means an entity that supports data recipients and data providers in enabling consumer-authorized information access. The term "authorized third party" means a third party who has followed certain procedures for authorization described in part III.B.2 of the Outline and summarized below under section B (Recipients of information).

The following questions apply to all the proposals under consideration discussed below.

- *Do you believe any of the statutes or regulations identified in Appendix C of the Outline,*[4] *or other statutes or regulations, duplicate, overlap, or conflict with the CFPB's proposals under consideration? (See Outline Q1-2.)*

- *What factors disproportionately affecting small entities should the CFPB be aware of when evaluating the proposals under consideration? For example, would a small entity's reliance on a core processor or other service provider affect the costs or burdens associated with any of the proposals under consideration? Would any of the proposals under consideration provide unique benefits to small entities? What training costs, if any, would small entities expect to incur in implementing the proposals? (See Outline Q3, 136, 140.)*

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

- *Would the proposals under consideration affect the cost and availability of credit to small entities? Are there additional channels beyond those described above that could affect the cost and availability of credit to small entities? (See Outline Q149.)*

### *A. Coverage of data providers subject to the proposals under consideration (Outline part III.A)*

**Covered data providers**. The CFPB is considering proposals that, if finalized, would require a defined subset of Dodd-Frank Act covered persons (*see* 12 U.S.C. 5481(6)) that are data providers to make consumer financial information available to a consumer or an authorized third party. This subset of data providers would be entities that meet the definition of "financial institution" as set forth in § 1005.2(i) of the CFPB's Regulation E (12 CFR part 1005) or "card issuer" as set forth in § 1026.2(a)(7) of the CFPB's Regulation Z (12 CFR part 1026). The data

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

providers that would be directly affected by the proposals under consideration include depository and non-depository financial institutions that provide consumer funds-holding accounts or that otherwise meet the Regulation E definition of financial institution, as well as depository and non-depository institutions that provide credit cards or otherwise meet the Regulation Z definition of card issuer. The Outline refers to financial institutions and card issuers collectively as "covered data providers."

It is important to note that a financial institution would be a covered data provider if it issues an "access device" (as the term is defined in Regulation E § 1005.2(a)(1)), such as a digital credential storage wallet, and provides EFT services, even if it does not hold consumer accounts. Likewise, a card issuer would be a covered data provider if it issues a "credit card" (as the term is defined in Regulation Z § 1026.2(a)(15)(i)), such as by issuing digital credential storage wallets, even if it does not hold consumer credit accounts.

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

**Covered accounts**. Under the proposals the CFPB is considering, a Regulation E financial institution would be a covered data provider with respect to information that pertains to an "account," as that term is defined in Regulation E § 1005.2(b), and a Regulation Z card issuer would be a covered data provider with respect to information that pertains to a "credit card account under an open-end (not home-secured) consumer credit plan" as that term is defined in Regulation Z § 1026.2(a)(15)(ii). The Outline refers to these accounts collectively as "covered accounts."

**Potential exemptions for certain covered data providers**. The CFPB is considering whether exemptions from the proposals under consideration would be appropriate for any data providers that would otherwise be covered data providers. However, in determining if exemptions would be appropriate, the CFPB is interested in whether there are ways to design the proposals described in this Outline to reduce impact on covered data providers.

- *Should the CFPB exempt certain covered data providers from any particular proposals under consideration? For which covered data providers would such exemptions be appropriate, and why? Which proposals should such data providers be exempt from, and why? (See Outline Q6.)*

### *B. Recipients of information (Outline part III.B)*

**Consumers and third parties**. The CFPB is considering proposals that would address a covered data provider's obligation to make information available upon request directly to a consumer (direct access) and to authorized third parties (third-party access).

**Third-party authorization procedures—in general**. Under the proposals the CFPB is considering, to be an authorized third party, the third party must: (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.

- *Please provide input on the approach the CFPB is considering with respect to the authorization procedures, described in more detail in part III.B.2 of the Outline. In providing input, please describe the authorization procedures that third parties and/or covered data providers currently employ and the benefits and drawbacks of those procedures in comparison to the procedures the CFPB is considering. What costs would third parties or covered data providers face with respect to the authorization procedures under consideration? (See Outline Q12.)*

- *What alternative approaches should the CFPB consider? Please describe any additional authorization procedures or any suggested changes to the procedures the CFPB is contemplating. (See Outline Q13.)*

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

**Third-party authorization procedures—authorization disclosure**. The CFPB is considering proposing that the authorization disclosure would contain key scope and use terms.

Key scope terms might include the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access. Key use terms might include the identity of intended data recipients (including any downstream parties and data aggregators to whom the information may be disclosed), and the purpose for accessing the information. The CFPB is also considering proposing that the authorization disclosure include a reference to the third party's certification to certain obligations regarding collection, use, and retention of the consumer's information, which are described in part III.E of the Outline and summarized below in section E. The authorization disclosure would also contain a request for consent to access the consumer's information.

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

- *Please provide input on whether the full certification statement regarding an authorized third party's obligations with respect to the collection, use, and retention of consumer information should be included in the authorization disclosure? (See Outline Q21.)*

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

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

### *C. The types of information a covered data provider would be required to make available (Outline part III.C)*

**Scope of information with respect to covered accounts**. Dodd-Frank Act section 1033(a) authorizes the CFPB to require a data provider to make available information

"concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data." The Outline sets forth six categories of information the CFPB is considering requiring covered data providers to make available with respect to covered accounts:

- Periodic statement information regarding transactions and deposits that have settled,[5] including fees, account terms and conditions, and the annual percentage yield of an asset account or the annual percentage rate of a credit card account;
- Information regarding prior transactions and deposits that have not yet settled;
- Information about prior transactions not typically shown on periodic statements or online financial account management portals;
- Online banking transactions that the consumer has set up but that have not yet occurred;
- Account identity information; and
- Other information, including consumer reports obtained and used by the covered data provider in deciding whether to provide an account or other financial product or service to a consumer; fees that the covered data provider assesses on its consumer accounts; bonuses, rewards, discounts, or other incentives that the covered data provider gives to consumers; and information about security breaches that exposed a consumer's identity or financial information.

- *Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make available the above information to a consumer or an authorized third party. What alternative approaches should the CFPB consider? (See Outline Q22-29)*

**Exceptions.** Dodd-Frank Act section 1033(b) sets forth the following four exceptions to the section 1033(a) requirement to make information available. Specifically, under the statute, a data provider may not be required by section 1033 to make available:

---

[5] This information generally appears on periodic statements that covered data providers are currently required to provide for asset accounts under Regulation E § 1005.9(b) and § 1030.6(a) of the CFPB's Regulation DD (12 CFR part 1030) and for credit card accounts under Regulation Z §§ 1026.7(b) and 1026.8

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

- *How should the CFPB interpret these exceptions? Which data elements should be covered under the exceptions? (See Outline Q30-37.)*

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

### *D. How and when information would need to be made available (Outline part III.D)*

The CFPB is considering proposals to define the methods and the circumstances in which a covered data provider would need to make information available with respect to both direct access (where a consumer directly obtains data about their own account from the covered data provider), and third-party access (where a consumer authorizes a third party to access data on their behalf).

- *Do covered data providers currently charge consumers or third parties specific fees (i.e., fees other than periodic account maintenance fees) to access information, such as through an online financial account management portal, a third-party access portal, or to export information in a human or machine readable format? What would be the impact on covered data providers, consumers, and authorized third parties if covered*

*data providers were or were not restricted from charging specific fees? (See Outline Q41, 63.)*

- *Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate? (See Outline Q82.)*

**Direct access**. With respect to requests for direct access, the CFPB is considering proposing that a covered data provider would be required to make information available if it has enough information from the consumer to reasonably authenticate the consumer's identity and reasonably identify the information requested. The CFPB is also considering proposing that covered data providers would be required to make available all the information that would be covered by the proposals under consideration through online financial account management portals, and to allow consumers to export the information in both human and machine readable formats. For example, many data providers allow consumers to export a history of their transactions in file formats that present the information in a consumer-friendly display and file formats such that the file could be imported or read into a computer system for further processing (*e.g.*, a .CSV file format).

- *Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers through an online financial account management portal and by giving consumers the option to export the information in both human and machine readable file formats. What alternatives should the CFPB consider? (See Outline Q40.)*

**Third-party access**. With respect to third-party access, the CFPB is considering proposing that covered data providers must establish and maintain a third-party access portal that does not require the authorized third party to possess or retain consumer credentials. The CFPB is also considering what role screen scraping should play in the context of a covered data provider's compliance with the rule. Specific aspects of this approach under consideration are described further below.

- *Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal, along with any alternative approaches the CFPB should consider. (See Outline Q50.)*

- *Please provide input on how covered data providers' customers can share their account information with third parties today. (See Outline Q51.)*

- *For covered data providers with a third-party access portal or comparable system that was built primarily in-house:*
    - *What were your upfront staffing costs to build the portal or system?*
    - *What are your ongoing staffing costs to maintain the portal or system?*
    - *What were your upfront hardware or data processing costs to build the portal or system?*
    - *What are your ongoing costs to maintain the hardware and provide the data processing capabilities?*
    - *Were you able to use existing hardware or data processing systems?*
    - *Has the portal or system worked effectively?*

      *(See Outline Q126.)*
- *For covered data providers with a third-party access portal or comparable system that was built or provided primarily by a software provider pursuant to a contract:*
    - *What were the upfront costs to create the portal?*
    - *What are the ongoing costs to maintain the portal? Do these costs scale with the number of consumers or accounts connected?*

      *(See Outline Q127.)*
- *For covered data providers without a third-party access portal or comparable system, under the proposals under consideration: would you expect you would need to develop a third-party access portal in-house or procure one from a software provider? If you would procure a portal from a software provider, would you expect to use the core banking provider of your other technology services? (See Outline Q128.)*

- *With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, should the CFPB require that they make information available to authorized third parties before they establish a third-party access portal? Would such a requirement necessitate covered data providers allowing authorized third parties to engage in screen scraping? Are there alternatives to screen scraping that a covered data provider could implement to make information available to authorized third parties in electronic form while establishing a third-party access portal? (See Outline Q52.)*

- *Assuming the CFPB imposes staggered deadlines with respect to a requirement to establish a third-party access portal, please provide input on how the CFPB should do so. For example, how should the CFPB define different classes of covered data providers that would be subject to different implementation periods? Should the CFPB use asset size, activity level, or some other metric? What would be the appropriate thresholds? Would responses to these questions change if data providers relied on screen scraping to comply with an obligation to make information available before they establish a third-party access portal? (See Outline Q53.)*

- *Assuming the CFPB imposes staggered implementation periods with respect to establishing a third-party access portal, please provide input on the appropriate time period that each class of covered data providers should have in order to come into compliance with the third-party access portal proposal under consideration. Would responses to this question change if data providers were permitted to rely on screen scraping to comply with an obligation to make information available to authorized third parties before they establish a third-party access portal? (See Outline Q54.)*

- *Should covered data providers be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption? What records could demonstrate that a service interruption to a third-party access portal has occurred? What alternatives to screen scraping should the CFPB consider to reduce interruptions to authorized third-party information access when a third-party access portal experiences a service interruption? (See Outline Q55.)*

- *To the extent screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? For example, should the CFPB require covered data providers to provide access tokens to authorized third parties to use to screen scrape so that third parties would not need a consumer's credentials to access the online financial account management portal? Alternatively, should authorized third parties be restricted from retaining consumer credentials indefinitely? For how long do authorized third parties need to retain consumer credentials? If the answer depends on the use case, please explain. (See Outline Q56.)*

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

- *Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the*

*regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals? (See Outline Q57.)*

- *How can the CFPB incentivize the establishment of industry-led mechanisms and fora through which disputes between ecosystem participants could be surfaced, adjudicated, and otherwise addressed? (See Outline Q58.)*

With respect to the availability of information provided through a third-party access portal, the CFPB is considering proposing that a covered data provider would not satisfy its obligations under the rule unless its portal meets certain availability requirements related to the following factors affecting the quality, timeliness, and usability of the information:

- The general reliability of a third-party access portal in response to electronic requests to the portal for information by an authorized third party (uptime);
- The length of time between the submission of a call to a third-party access portal and a response (latency);
- System maintenance and development that involve both planned interruptions of data availability (planned outages) and responses to unplanned interruptions (unplanned outages);
- Responses to notifications of errors from an authorized third party (error response); and
- Limitations or restrictions on fulfilling a call from an authorized third party even when data are otherwise available (access caps).

To ensure third-party access portals are reliably available, as defined by the above factors, the CFPB is considering proposals that would: require the establishment and maintenance of reasonable policies and procedures to ensure availability, establish performance standards related to the third-party portal availability factors, prohibit covered data provider conduct that would adversely affect the third-party portal availability factors, or some combination of the above.

Similarly, to ensure that data providers transmit consumer information accurately through third-party access portals, the CFPB is also considering proposals for covered data providers to implement reasonable policies and procedures to ensure data accuracy, establish performance

standards, and prohibit covered data provider conduct that would adversely affect the accurate transmission of consumer information, or some combination of the above.

With respect to the security of third-party access portals, the CFPB believes that nearly all—if not all—covered data providers must already comply with either the Safeguards Rule or Guidelines issued under the Gramm-Leach-Bliley Act (GLBA), as well as the prohibition against unfair practices. However, as noted above, the CFPB is considering a proposal in which a third-party access portal could not rely on an authorized third party possessing or retaining a consumer's credentials to authenticate the authorized third party.

- *What methods of securely authenticating an authorized third party do not require consumers to share their credentials with the authorized third party? Should the CFPB consider proposals to articulate performance standards related to authentication? If so, how should the CFPB address such topics? (See Outline Q70.)*

The CFPB is considering proposing that a covered data provider generally would be required to make information available to a third party, upon request, when the covered data provider has received certain evidence of a third party's authority to access information on behalf of a consumer, information sufficient to identify the scope of the information requested,[6] and information sufficient to authenticate the third party's identity. The CFPB is seeking to ensure that third parties that do not meet these conditions are prevented from obtaining access to the information. The CFPB is considering how to address circumstances in which third parties could be prevented from getting access to information where they do not satisfy the conditions. The CFPB is also considering whether it should require covered data providers to disclose to consumers or third parties when information is not available and the reason it is not available.

- *Please provide input on the approach the CFPB is considering. What alternative approaches should the CFPB consider? Should covered data providers be able to obtain evidence of authorization directly from a consumer, rather than through an authorized third party? Is there additional information, besides the above-described evidence,*

[6] In some circumstances the scope of information requested by an authorized third party might be ambiguous. Thus, the CFPB is considering a proposal in which a covered data provider could seek to clarify the scope of an authorized third party's request with a consumer where a covered data provider does not have enough information to know how to respond to the request.

*that a covered data provider should receive before a third party should be treated as authorized to access the consumer's information? (See Outline Q73.)*

- *Please provide input on what type of evidence of revocation of a third party's authorization a covered data provider should be required to receive before they terminate access. (See Outline Q74.)*

- *To reduce the risk of potentially fraudulently obtained authorizations, should a covered data provider be required to notify a consumer of a third party's initial access attempt (such as by providing consumers a copy of the evidence of authorization submitted by a third party), or be permitted to confirm with the consumer the authorization of a particular third party before making information available? To enable consumers to monitor third-party access to their account information, should covered data providers be required to inform consumers of which third parties are accessing information pursuant to a purported authorization? (See Outline Q75.)*

- *Please provide input on whether it would facilitate compliance or reduce costs to covered data providers and authorized third parties if covered data providers were required to follow certain specific procedures in authenticating an authorized third party's identity. Please provide input on what models the CFPB could look to for prescribing such procedures. Do all covered data providers require a uniform set of information to authenticate an authorized third party's identity prior to making information available to the authorized third party? (See Outline Q81.)*

As noted above, the CFPB is considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

- *Please provide input on whether covered data providers have the technical capacity to make information available in terms of the frequency and duration sought by authorized third parties through screen scraping, including whether there are considerations particularly relevant to small entities. (See Outline Q77.)*

- *Please provide input on whether covered data providers should be allowed to limit the frequency and duration of authorized third parties' access if covered data providers had to permit screen scraping in order to satisfy their obligations to make information available. How could they do so in a way that both minimizes their costs and does not interfere with a consumer's right to access information? (See Outline Q78.)*

### *E. Third party obligations (Outline part III.E)*

**Collection, use, and retention limits**. The CFPB is considering proposals under which authorized third parties would have to limit their collection, use, and retention of consumer information to what is reasonably necessary to provide the product or service the consumer has requested.

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

**Limits on collection**. The CFPB is considering proposals to limit third parties' collection of consumer information to what is reasonably necessary to provide the product or service the consumer has requested. The CFPB is considering proposing that third parties would be limited to collecting consumer information for only as long (duration) and as often (frequency) as would be reasonably necessary to provide the product or service the consumer has requested. The CFPB is also considering proposing that authorized duration would be limited by a maximum period, after which third parties would need to seek reauthorization for continued access.

- *If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties (see Outline part III.D.2.i), how would third parties using screen scraping comply with limits on collection? Would third parties employ filters or other technical solutions to limit collection? (See Outline Q90.)*

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

- *In requiring third parties to obtain reauthorization after a durational period has lapsed, how could the CFPB reduce negative impacts on consumers and unnecessary costs on authorized third parties? For example, should the CFPB consider proposals that would allow third parties to:*

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

*(See Outline Q93.)*

The CFPB is considering proposing that authorized third parties would be required to provide consumers with a simple way to revoke authorization at any point, consistent with the consumer's mode of authorization. For the purposes of the Outline, "revocation" is the mechanism by which the consumer withdraws consent from third parties they previously authorized to access their information.

- *Please provide input on the approach the CFPB is considering that would require authorized third parties to provide consumers with a mechanism through which consumers may revoke access to their information, along with costs associated with providing consumers a revocation mechanism. Please provide input on any alternative approaches the CFPB should consider, and how it could reduce costs and facilitate compliance for small entities. (See Outline Q94.)*
- *Please provide input on whether covered data providers should also be required to provide consumers with a mechanism by which they may revoke third-party authorization, and the costs and benefits of such an approach. Is it feasible to require covered data providers to provide revocation mechanisms where screen scraping is used? (See Outline Q95.)*
- *Please provide input on whether authorized third parties should be required to report consumer revocation requests to covered data providers. What challenges or costs would be anticipated from such a requirement? (See Outline Q96.)*
- *For third parties: do you have consumer-facing tools for access revocation? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you expect it would take to develop these tools to implement the proposals under consideration? (See Outline Q139.)*

**Limits on use**. The CFPB is considering proposals that would limit third parties' secondary use of consumer-authorized information. The Bureau is considering defining secondary use to

mean a third party's use of consumer-authorized information beyond what is reasonably necessary to provide the product or service that the consumer has requested, including the third party's own use of consumer data and the sharing of data with downstream entities. The CFPB is considering various approaches to limiting third parties' secondary use of consumer information. General approaches the CFPB is considering include:

- Prohibiting all secondary uses.
- Prohibiting certain high risk secondary uses.
- Prohibiting any secondary uses unless the consumer opts in to those uses.
- Prohibiting any secondary use if the consumer opts out of those uses.

- *Please provide input on the various approaches the CFPB is considering to limit authorized third parties' use of consumer information and any alternative approaches the CFPB should consider. How could the CFPB design such approaches to facilitate compliance by small entities? Should the CFPB propose to include a standard for defining "high risk," or provide a specific list of uses that it deems to be "high risk," or both? (See Outline Q99.)*

- *Would the conditions restricting certain secondary uses of consumer data impede products or business models used by third parties? (See Outline Q144.)*

- *Please provide input on whether the rule should allow consumer information that has been de-identified to be used by third parties beyond what is reasonably necessary to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"? (See Outline Q102.)*

**Limits on retention**. The CFPB is considering proposing that authorized third parties would need to limit their retention of consumer-authorized information. Specifically, the CFPB is considering a proposal in which authorized third parties would need to delete consumer information that is no longer reasonably necessary to provide the consumer's requested product or service, or upon the consumer's revocation of the third-party's authorization. The CFPB is also considering a limited exception to the deletion requirements for compliance with other laws. For the purposes of the Outline, "deletion" is the complete removal of previously collected consumer information.

- *For third parties: do you have consumer-facing tools for deletion? If so, how many staff-hours did you commit to develop those tools? How many staff-hours do you*

*expect it would take to develop these tools to implement the proposals under consideration? (See Outline Q138.)*

- *Should an authorized third party be required to delete information upon receipt of the consumer's revocation request? Under what circumstances should a third party be allowed to retain information beyond receipt of the consumer's revocation request? For example, is retention of data after receipt of a revocation request necessary for compliance with other laws and regulations? (See Outline Q104).*

- *Are there any use cases or services for which consumers might seek deletion of some consumer-authorized information that the authorized third party collected, but not want to revoke that third party's ongoing access to their information from a covered data provider? Should deletion of consumer-authorized information be required when authorization lapses at the end of a durational period? (See Outline Q107-108.)*

- *Would the proposals requiring the deletion of consumer data when consumer authorization lapses or is revoked impede products or business models used by third parties? (See Outline Q143.)*

- *If screen scraping were a method by which data providers could satisfy their obligation to make information available to authorized third parties, what deletion requirements should be imposed on authorized third parties that utilize screen scraping and potentially collect more information than what is reasonably necessary to provide the product or service? (See Outline Q109.)*

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

**Data security requirements**. The CFPB is considering a proposal to require authorized third parties to implement data security standards. Although the CFPB believes that authorized third

parties are likely subject to the GLBA safeguards framework,[7] the CFPB is considering whether it should impose specific data security standards on authorized third parties under the rule. General approaches the CFPB is considering include:

  - Requiring authorized third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third parties' size and complexity, and the volume and sensitivity of the consumer information at issue. This approach could be combined with a provision incorporating the Safeguards Rule or Guidelines as a specific option for complying with any data security requirement under the CFPB's rule.

  - Alternatively, requiring compliance with the Safeguards Rule or Guidelines.

- *For third parties: what data security practices do you currently apply to consumer data? Do you tailor your information security approach to an existing legal or industry standard, such as the safeguards framework, and if so, which one(s)? Would you follow the Safeguards Rule or the Safeguards Guidelines if either were incorporated as an option for complying with any data security requirement under the CFPB's rule? (See Outline Q112.)*

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

- *Are inaccuracies in consumer-authorized information used by authorized third parties more likely to come from errors in data made available by covered data providers or from errors in any manipulation, calculation, or subsequent transmission performed by third parties? Could third-party policies and procedures address errors in data that were inaccurate when originally accessed from a covered data provider? (See Outline Q115.)*

---

[7] The safeguards framework generally requires financial institutions to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institutions' activities, and the sensitivity of the customer information at issue. These safeguards must include specific elements set forth in the regulations.

- *Should policies and procedures to ensure accuracy include addressing disputes submitted by consumers? When does addressing such disputes require an investigation and a response to the consumer? (See Outline Q116.)*

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

### *F. Record retention obligations (Outline part III.F)*

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

- *Should the rule require covered data providers and authorized third parties to maintain policies and procedures to comply with their obligations under the rule, beyond the areas already identified in this Outline? What costs would be associated with maintaining policies and procedures? (See Outline Q120.)*

### *G. Implementation period (Outline part III.G)*

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

- *Please provide input on an appropriate implementation period for complying with a final rule other than a potential third-party access portal requirement.*[8] *What alternative approaches should the CFPB consider? Are there any aspects of the CFPB's proposals under consideration that could be particularly time consuming or costly for*

[8] See section D above for questions about the implementation period with respect to the potential third-party access portal requirement.

*a covered data provider or a third party to implement? Are there any factors outside a covered data provider's or authorized third party's control that would affect its ability to prepare for compliance? (See Outline Q121.)*

- *The CFPB recognizes that small covered data providers and authorized third parties might not be able to comply with some of the proposals under consideration on the same timeframe as larger covered data providers and authorized third parties. How much time would small entities need to implement the proposals under consideration, other than the third-party access portal proposal,[9] including updating policies, procedures, processes, and employee training programs? (See Outline Q122.)*

[9] See the questions in section D above.

## Appendix: Illustration of Interaction of Proposals Under Consideration (Third-Party Access)

The graphic below illustrates how the CFPB's proposals under consideration described in the Outline would apply to a hypothetical transaction involving consumer-authorized information access through a third-party data access portal. See references to sections of the Outline (in parentheses) to read the proposals under consideration in greater detail.

**Definitions**

**Consumer (III.B.1)**
Individual who obtains a consumer financial product or service from a covered data provider

**Covered data provider (III.A.1)**
Covered person[1] who is either a "financial institution"[2] or "card issuer"[3] with control or possession of consumer financial information

**Authorized third party (III.B.2)**
A third party who has followed the authorization procedures described in part III.B.2 of the Outline

1 As defined under the Dodd-Frank Act (12 U.S.C. 5481(6))

2 As defined under Regulation E

3 As defined under Regulation Z