PLAID

January 25, 2023
The Honorable Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G St. NW
Washington, DC 20552

SENT VIA ELECTRONIC MAIL TO Financial_Data_Rights_SBREFA@cfpb.gov.
Re: Outline of Proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights

Director Chopra and Bureau Staff,

Plaid appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (the "Bureau's") outline (the "Proposal") for its Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights. Plaid is a financial data aggregator enabling consumers to programmatically share their own financial data, so that they can benefit from greater competition and choice in their use of critical financial products and services.

Plaid develops digital infrastructure to transmit consumer-permissioned financial data to consumers' chosen data recipients, which in turn are able to offer consumers innovative and essential financial services. We serve over 7,000 data recipient customers, including large and small banks, credit unions, and diverse, large and small for-profit and nonprofit digital financial service providers. As part of our efforts to build trust in the open finance ecosystem through consumer control and appropriate data and security practices, we have signed data access agreements with many of the largest data providers (both banks and nonbanks), actively participated in technical standards development with the Financial Data Exchange ("FDX"),[1] and shifted most of our traffic to data providers' third-party access portals.

Consumer demand, technological innovation, and industry collaboration have led to significant advances in the United States' consumer-permissioned data sharing ecosystem, with millions of consumers able to access and share their own financial information so that they can easily use their chosen services.[2] The rulemaking is critical to consumers fully realizing the consumer empowerment goal that underpins §1033, and to achieving a fair, transparent, and competitive financial services marketplace. It will propel the financial services industry to better serve consumers by bolstering the consumer right to access and share their own financial data, and mitigate privacy, security, and anticompetitive risks.

[1] "Financial Data Exchange (FDX) is a North American non-profit industry standards body dedicated to unifying the financial services ecosystem around a common, interoperable, and royalty-free technical standard for consumer-permissioned financial data sharing, aptly named the FDX API."
"About-FDX - Our Mission." About FDX. Accessed January 24, 2023.
https://financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6
[2] Financial Data and Technology Association (FDATA). 2019. "Opportunities in Open Banking,"
https://fdata.global/north-america/wp-content/uploads/sites/3/2019/04/FDATA-Open-Banking-in-North-America-US-version.pdf

The Bureau's outlined proposal is a positive step toward this goal. By affirming the strong consumer rights established in §1033 and setting out the obligations of all covered parties involved in consumer-permissioned data sharing under §1033, the Proposal lays a strong foundation for rulemaking. Its emphasis on effective authorization and obligations regarding authorized third parties collection, use, and retention of the consumer's information appropriately aligns consumers' interests with covered party obligations. In the interest of further defining strong consumer protections and rights, our comments focus on five overarching elements of the Proposal:

1. **Ensure consumers have equivalent "direct" and "third-party"[3] access to the data they need to manage their finances, now and in the future:** Consumers need reliable access to a wide range of their own financial data – both directly and via authorized third parties, at parity – to fully benefit from a data access rights regime. As a principle, there should be no distinction between what data is available to consumers directly and what they can share via an authorized third party, because many digital financial services will work more effectively – and often only – with consumer-permissioned access for a third party. The Proposal covers a significant part of the data consumers already choose to share, but would leave millions of consumers who today share their investments, mortgage, auto, student and personal loans, government benefits, and payroll information, outside of the rule's protection. If those data categories are not addressed, then consumers could lose access to the tools they already use to manage their finances. The §1033 rulemaking should cover all products the Bureau regulates, including mortgage, auto, and student loans, which are central to financial planning and management for consumers. The Bureau also should signal its intent to work with other agencies to expand coverage to all consumer financial data. If the Bureau decides not to expand the scope of this rule to include these additional categories, then, at a minimum, the Bureau should make explicit in the rule that its scope is not intended to otherwise limit the full scope of potential applicability of §1033, and that a regulation issued pursuant to §1033 is not necessary for enforcement of the statutory mandate.

2. **Support the ecosystem's shift away from credential sharing, while protecting consumer access:** Consumers' ability to benefit from data sharing via a third party historically required them to share their banking credentials with that third party (or another third party, like a data aggregator), as part of the process in which they permissioned the third party to access data on their behalf. Over time, multiple methods have been developed to eliminate the need for consumers to share their credentials with third parties. Many of the largest data providers have already built dedicated third-party access portals that reduce or eliminate credential sharing. However, not all data providers (including small covered data providers) have such technology currently available for their consumers. The Bureau must protect access for the millions of

[3] As defined in the Proposal: (1) "Direct access refers to covered data providers making information available, upon request, directly to a consumer;" and (2) "Third-party access refers to covered data providers making information available, upon request, to authorized third parties."

consumers who already rely on data access from these data providers, while permitting these data providers a transition period to build their own third-party access portals, or to work with another provider offering such technology. The Bureau also should make clear that it is not acceptable for consumer access via data providers' third-party access portals to be interrupted due to technical issues and should explicitly recognize that, if such failures take place, consumers and authorized third parties may use alternative means as a fallback to maintain access that may in some instances require credential sharing. The shift away from credential sharing will be advanced by a mandate from the Bureau that prescribes its expectations for third-party access portals.

3. **Require modern disclosures and privacy controls across financial services providers and back them up with oversight:** To meaningfully exercise their data access rights, consumers need a fair, transparent, and competitive marketplace where they can expect consistent disclosures and controls across all consumer finance service providers. The Bureau should set standards for disclosures and protections that support consumers' decisions to share their data and provide the information they need to meaningfully control their own data and benefit from continued innovation. The Bureau can help prevent inconsistent consumer data sharing experiences across the ecosystem by assigning roles and responsibilities to data providers and authorized third parties, and by harmonizing different expectations under the Gramm-Leach-Bliley Act ("GLBA") and §1033.

4. **Prevent anticompetitive practices that interfere with consumer choice and cause consumer harm:** When consumers can easily and securely share their own financial data, they are able to seek and obtain innovative financial services that may compete with those provided by the data provider. The Bureau should protect against anticompetitive conduct designed to interfere with a consumer's right to share their own data. Data providers may seek to prevent or introduce barriers to consumer data sharing, or otherwise improperly persuade consumers not to share their data through materials and communications suggesting data sharing is inherently risky.[4] The Bureau should recognize that such efforts may materially interfere with the ability of a consumer to understand a term or condition of a consumer financial product or service, or to comprehend the risks or benefits of data sharing. The Bureau's rulemaking should protect consumers from such anticompetitive practices.

5. **Supervise third-party authorization managers like Plaid to ensure they act responsibly, and allow them to enhance the safety and security of ecosystem:** The Proposal makes clear that authorization is the cornerstone of consumers exercising their financial data access rights, and that consumer control and choice will be served by transparency in, and adherence to, authorization disclosures and data collection, use,

[4] Levitin, Adam J. "Consumers - Not Banks - Should Control Access to Personal Financial Data." The Hill. The Hill, July 6, 2021. https://thehill.com/opinion/finance/561645-consumers-not-banks-should-control-access-to-personal-financial-data/.

and retention obligations. Third-party authorization is what consumers and third parties must communicate about in order to effectuate the consumer's decision to share data and use new consumer finance providers. Therefore, the Bureau rules and its oversight approach should focus on making authorization and access as effective as possible for the consumer, including by recognizing that there are security, fraud prevention, authentication, and consumer convenience benefits when authorization management providers can enhance their services. For these reasons, the Bureau should set clear standards in its rule that can be a basis for supervising Plaid and all the third parties that handle consumer authorization and effectuate data access under this rule. The Bureau should also use its existing authorities to ensure that data providers do not anticompetitively bar access by interfering with authorization.

In summary, in order to bolster consumers' rights to use their own personal financial information to improve their ability to manage their financial lives and get the benefit of innovation from providers that they choose, and to ensure a fair, transparent, and competitive marketplace, we recommend that the Bureau issue a rule that: requires data providers to implement policies that enhance consumer access to information; ensures third parties have appropriate authorization management, privacy, and security policies; and prohibits anticompetitive conduct that interferes with consumer and authorized third-party access. In combination, this model will provide the Bureau with substantial tools to oversee and enforce consumer financial data rights, set forth clear requirements for industry that allow continued innovation, and ensure consumers benefit from competitive marketplaces that can deploy the latest technology.

Sincerely,

John Pitts
Global Head of Policy

Ben White
Policy & Technical Standards

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? What challenges or costs would you anticipate in complying with those statutes and regulations (if applicable) and the CFPB's proposals under consideration?

Yes, a certain subset of the Bureau's proposals appear to overlap with already-existing statutes and regulations. Because the purposes of §1033 are different than the closely related statutes and regulations, the overlapping provisions are not always adequate direct substitutes for each other and could potentially create confusion in the market.

Where regulations overlap with this Proposal, we believe provisions in this Proposal should be maintained if they meet the following criteria: (i) the overlapping requirements further §1033's purpose of protecting and enabling consumers' access to their financial data, whereas the closely related statutes and regulations do not; and (ii) the overlapping requirements do not create redundancies or conflicts likely to cause consumer confusion, nor does their cost of compliance outweigh the benefits received by the consumer.

If these criteria are applied in the rulemaking, then the industry will be able to operationalize compliance with both §1033 and overlapping obligations. For clarity, the Bureau should be explicit about when §1033 rules overlap with existing requirements and when §1033 rules add new obligations. To further aid compliance, the Bureau should be clear that, when there are overlapping requirements, compliance with either §1033 or the overlapping regulation constitutes compliance with both requirements.

Examples

FCRA: The FCRA, 15 U.S.C. §§ 1681, et seq., exists to ensure that consumers are properly served by entities that, largely without the consumers' knowledge or consent, collect and share their data for certain permissible purposes. This data collection and transmission has historically occurred without consumers' involvement, and the data (in the form of a consumer report) is often transmitted when consumers apply for many financial products and services.

Consumers today, however, have the ability to manage the digital submission of data they select for these purposes, through direct access, permission to access granted to a third-party data recipient, or by relying on data aggregators to facilitate collection and transmission of their data. In such circumstances, data aggregators, unlike consumer reporting agencies (CRAs), collect and transmit consumer information as an intermediary acting on behalf of the consumer.

Congress enacted the FCRA, in part, because of the "need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[5] From this original motivation to the most recent amendments, Congress has repeatedly updated the FCRA to combat consumer harms arising from a

[5] 15 U.S.C. § 1681(a)(4).

consumer reporting system that was not built for consumers even though it has a direct impact on their individual financial lives, including entities investigating and collecting information unbeknownst to consumers, sometimes including inaccuracies, and then selling the information to financial services providers.

These FCRA-regulated practices bear little resemblance to the consumer-permissioned ecosystem made possible by §1033. In particular, direct access and consumer-permissioned access generally enable consumers to control what data about them is accessed, and with whom and for what purpose such data is shared. Under this consumer-permissioned model, data aggregators do not transmit a "consumer report" of pooled data from various sources to a third party.[6]

Critically, unlike in the consumer reporting system, where anyone with a "permissible purpose" can access consumer reports, no one has access to the consumer's financial data through data aggregators unless the consumer authorizes such access.[7] Instead, in their role of providing financial data on behalf of a consumer to third parties, data aggregators are in essence an intermediary for the consumer, and only acting to further the consumer's desired actions.

While the FCRA is intended to provide protections to consumers in circumstances when they do not have transparency and control over the data collected and transmitted about them, the statutory terms do not contemplate situations where entities collect and transmit data at the consumer's direction and with transparency. Moreover, while there is some overlap, the major consumer risks that exist in the §1033 regime are not identical to the major consumer risks that exist in FCRA-regulated activity.

The §1033 regime was designed to benefit the consumer making choices, whereas the credit reporting system traditionally has been in service of the lenders, landlords, and employers who wanted to check into the consumer's finances. Thus, the FCRA and enforcement of its requirements focuses on the particular risks experienced in consumer reporting. Section 1033 is a shift from the traditional worldview, where a business decides whom it will do business with, to one where the consumer compares their options and selects their best provider. Consumer-permissioned access and sharing thus has introduced new risks associated with secure consumer authorization, reliable access, and risk of anticompetitive conduct by businesses that want to hold on to their customers.

In this §1033 rulemaking, the Bureau can address the requirements for a consumer-centered ecosystem by clarifying that the FCRA does not apply in the context of consumer-permissioned data pursuant to §1033 — that such data is not a "consumer report" and the data aggregators that facilitate consumer data access are not "consumer reporting agencies."[8]

By doing this, the Bureau can help resolve regulatory uncertainty that has created resistance to

[6] 15 U.S.C. § 1681a(d).
[7] 15 U.S.C. § 1681b(a)(3)(B).
[8] 12 C.F.R. § 1022.41(c).

data sharing by some data providers. One example of the uncertainty that data providers have been concerned about is being considered "furnishers" of data when they act on their consumer's direction and allow access to data. A second uncertainty is whether a consumer who permissions access to their data for inclusion by the data recipient in a consumer report causes the data provider or a data aggregator that may have been involved in the transmission to be considered a "furnisher" of information. Regulation V, which implements the FCRA, defines a "furnisher" as "an entity that furnishes information relating to consumers to one or more consumer reporting agencies for inclusion in a consumer report,"[9] but explicitly excludes a consumer from the definition of "furnisher."[10] Thus, to be clear, it is our view that when data providers or data aggregators, acting as an agent on behalf of a consumer, transmit data from the financial institution to a third-party recipient, including a CRA, the data provider and data aggregator should not be considered furnishers.

The Bureau should specifically clarify that the FCRA does not apply when data aggregators access and transmit consumer data by consumer permission pursuant to §1033. The applicability of either the FCRA or any §1033 regulatory framework should be determined by whether the consumer does or does not control the collection, use, and disclosure of their data. Further, the Bureau should clarify that §1033 applies to situations where the consumer acts through a data aggregator to select their data source(s) and the recipient(s) of their data, and also has visibility into the particular data to be shared before it is shared.

By clarifying when the §1033 framework applies as opposed to the FCRA, the Bureau can make sure that consumers are afforded appropriate protections under law that ensure safe access to their own data. It also can set appropriate standards for the specific consumer risks that attach in a consumer-permissioned sharing regime. Thus, §1033 rules should clarify the obligations of data providers and third-party data recipients and aggregators toward consumers.

The Bureau should consider putting in place similar consumer protections under §1033 to those under FCRA to the extent that such protections make sense for consumer-permissioned data. For example, in addition to requiring data to be produced when and as permissioned by the consumer, such protections might include data accuracy and dispute resolution requirements, which aim to protect consumers from unfair outcomes resulting from the denial of access to their data or inclusion of inaccurate information. In order to avoid consumer confusion and unnecessary compliance costs, it would be valuable for the Bureau to be explicit about whether it is extending FCRA requirements for data accuracy and dispute resolution to consumer permissioned access under §1033, or if it is imposing different obligations in light of the very different consumer risks that exist in connection with consumer permissioned access and sharing under §1033.

GLBA: The Gramm-Leach-Bliley Act ("GLBA") partially overlaps with the proposal's consent and authorization requirements, as well as its security recommendations. To the extent the

[9] *Id*.
[10] 12 C.F.R. § 1022.41(c)(3).

Bureau promulgates an annual privacy notice requirement as part of its §1033 rule, it should specify whether compliance with GLBA's annual privacy notice meets the requirements promulgated under §1033. As it clarifies the role of the certification statement, the Bureau should also consider annual privacy notices as an appropriate location for that information. As discussed in our responses to Q69 and Q111, we believe the GLBA Safeguards Rule to be an appropriate security standard for authorized third parties. Harmonizing any overlapping requirements that arise out of the §1033 rulemaking with GLBA would reduce the risk of consumer confusion, allow entities subject to both GLBA and §1033 to maintain one annual disclosure notice, and focus their compliance resources on developing the enhanced authorization experience and certification statement outlined in the Bureau's proposal.

Notably, the GLBA focuses its privacy provisions on notice, consent, and permissible sharing of consumer information by financial institutions, and not on use limitations, which the Bureau is considering in the Proposal. GLBA permits financial institutions to share nonpublic personal information about a consumer: (1) with affiliated third parties for any use (without a requirement for additional notice and consent); (2) with non-affiliated third parties for specifically enumerated uses (with notice, but no requirement for additional consent); and (3) with non-affiliated third parties for any use so long as there is notice and an opt out opportunity or consent. Further, if a GLBA-regulated financial institution receives nonpublic personal information from a non-affiliated financial institution, its use of that data is not restricted, although resharing of that data is limited by the GLBA.

While we recognize that implementation of §1033 in a manner that provides consumers with meaningful control over their own data may include additional disclosures and consent opportunities beyond the potentially overlapping ones prescribed by the GLBA, as the Bureau considers potential data use limitations pursuant to its §1033 rule, it should avoid treating data accessed by the consumer pursuant to §1033 differently than data shared among GLBA-covered financial institutions. Different standards could mean that a consumer's exercise of their own rights under §1033 are more restricted than a financial institution's exercise of its rights under GLBA over the consumers' own data. It also could foster confusion among consumers, who would be best served by consistent standards regarding notice, consent, and use across the financial services industry so they get to know what to expect from their service providers. Finally, different standards could create competitive disadvantages between GLBA-covered financial institutions and institutions relying on consumer-permissioned data collected under §1033. (See our response to Q147, for example.)

Accordingly, if the Bureau determines it is necessary to impose data use limitations, then the Bureau should either (1) amend the rules promulgated pursuant to the GLBA for consistency and defer implementation of the §1033 limitations until it is updated, or (2) make clear that the data use limitations promulgated pursuant to §1033 apply to consumer-permissioned data that is received by GLBA-covered financial institutions, just as it is for those entities that are not subject to GLBA. This clarity is important to avoid the negative impact that different standards would place on consumers and the anticompetitive consequences described above.

Challenges and costs to compliance
As described above, the Bureau can mitigate challenges and costs to compliance by clarifying when compliance with any requirements of the FCRA or the GLBA satisfy certain §1033 requirements. This will allow entities to provide consumers a consistent user experience, while reducing unnecessary compliance costs. Instead, entities can focus costs and resources towards compliance with the newer provisions outlined in the Bureau's proposal that are unique to §1033.

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?

Although student loans do not appear to be covered by the Bureau's proposal, if the Bureau were to expand the scope of the rule an additional relevant statute would be FERPA, 20 U.S.C. § 1232g, a federal law that protects the privacy of student educational records and the personally identifiable information they contain. Some student loan servicers interpret FERPA as allowing them to dictate the form of consent that they will accept, including whether to accept consumer permissioned access at all. The Bureau should therefore clarify that student loan data falls under the §1033 umbrella, and that consent authorization under §1033 satisfies FERPA requirements.

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?

Small entities tend to have smaller technology budgets, but also fewer requests for third-party access. Small entities' reliance on a core provider or other service provider could diminish the costs or burdens associated with the proposed requirements for establishing and maintaining third-party access portals. Similarly, to the extent small entities face any responsibilities for authorization or other manual or programmatic requirements besides authenticating the authorized third parties requesting access, those requirements could pose cost and compliance burdens. We believe the Proposal adequately assigns responsibility to third parties and data providers in such a way that would reduce costs for smaller 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.[11]

The purpose of the §1033 rule is to permit consumers to exercise control over their own financial data and, in doing so, to benefit from more competition and choice in the market for financial services. Some of the providers that consumers choose will be banks and credit unions that are not covered by the Bureau's supervisory authority – although they have other primary regulators – and some will be non-banks subject to CFPB rules and enforcement but that may rarely, if ever, be examined by CFPB. The CFPB may find it necessary to consider a larger participant rulemaking to ensure it has the ability to easily oversee large authorized third parties, both data aggregators and data recipients choosing to build direct connections to data providers' third-party access portals.

Nevertheless, because individual consumer harm related to violation of §1033's mandate may be comparatively small for an individual consumer (such that an individual would not be incentivized to pursue private, individual relief), but significant in the aggregate, and because harms to competition are nuanced and complex, supervision and enforcement are essential to uphold the purposes of §1033. See Appendix A for examples of consumer harms stemming from lack of reliable data access. Accordingly, the Bureau should focus its supervisory and enforcement resources on the highest impact and highest risk issues under §1033, i.e. those that inhibit informed consumers from exercising their data access rights and a fair, transparent and competitive marketplace.

Authorized third parties, including data recipients and data aggregators are also harmed when consumers are unable to access and share their data, which can severely disrupt their business operations and ability to deliver the services consumers are requesting. See also our response to Q144 for further details on impacts to authorized third parties' business models.

As practical, the Bureau should employ its full complement of tools beyond supervision to accomplish §1033 oversight, including:

- Requiring covered data provider reporting on availability and completeness of data, as well as performance criteria under the rule;
- Allowing authorized third parties that access data on behalf of consumers to share performance metrics for data provider portals with regulators to identify access issues in real time and validate reporting by data providers;
- Facilitating real-time notification of the Bureau's Consumer Response team by consumers or their agents when a data provider is not allowing access, and periodically publishing statistics on complaints and resolutions;
- Conducting risk-based exams of data providers and authorized third parties based on published performance data and complaints from consumers and their agents;

[11] Please note that several questions in the SBREFA Proposal request information or feedback that Plaid is not in a position to provide, usually because it is information specific to data providers. For clarity, we have omitted those questions from this response.

- Coordinating with prudential regulators to incorporate §1033 compliance reviews into their supervisory exams;
- Incentivizing data providers and authorized third parties to work together to quickly resolve problems with consumer data access; and
- Continued public messaging from the Bureau that it intends to use its supervisory and enforcement power to correct non-compliance, as well as reporting in Supervisory Highlights or Bureau Circulars about the consequences of non-compliance.

The advent of financial data technology also creates an opportunity for the Bureau to leverage that technology and use it for modern, scalable oversight. For example, if data providers are ultimately required to implement third-party access portals to comply with §1033, the Bureau could develop its own automated systems to systematically check those portals to assess compliance with availability requirements as discussed in §D.2.ii.a of the Proposal. Such testing systems can be developed at a relatively low upfront cost – particularly if data providers adopt a standardized third-party access portal like the FDX specification – and maintained at minimal cost and with limited human resources. Such test requests could alert the Bureau in real time to any access problems at every data provider, allowing Bureau staff to dedicate their resources to known access issues. This method of automated compliance checks running in the background without human intervention is already an industry standard for companies that work with and rely on third-party access portals, and could significantly reduce the supervision and enforcement burden on the Bureau and industry participants, while also allowing for near real-time identification and resolution of consumer harms.

Finally, in light of the finite resources available for supervision and enforcement, authorized third parties facing disruptions should be explicitly permitted to take expressly-defined actions in order to prevent, mitigate, and/or remedy consumer harm (e.g., the ability to fallback to screen scraping during times of third-party access portal downtime, degradation, or interruption, further described in Q55).

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?

Although the Bureau has signaled that this rulemaking is intended as the first in a series to ensure consumer access to their own financial data, the decision to limit its scope to only Regulation E and Regulation Z covered accounts puts at risk certain data sharing on which consumers are presently relying. If the Bureau decides not to expand the scope of this rule to include categories described below, then, at a minimum, the Bureau should make clear in the rule that the scope of the rule is not exhaustive or otherwise intended to limit the applicability of

§1033, and that a regulation issued pursuant to §1033 is not necessary for enforcement of the statutory requirement.

Two categories of consumer finance products are most at risk due to non-inclusion in the proposal: (1) non-credit card Regulation Z products, including mortgage, auto, student, and personal loans; and (2) asset accounts not covered by Regulation E, including brokerage and retirement accounts. Today, millions of consumers share these data elements with third-party data recipients via Plaid. For details on the types of information these consumers already have access to and choose to share, see Appendix B.

The Bureau should clarify that §1033 includes within its scope Regulation Z covered products, including mortgage, auto, student, and personal loan products, for which regulated institutions already provide direct and authorized third-party access to consumer data. Our experience indicates that millions of consumers currently permission access to their information in order to compare rates and to save on fees, interest rates, and financing. The Bureau would not need to expand its supervisory authority or navigate interagency oversight in order to oversee adherence to §1033 regulations for these kinds of accounts.

For asset accounts not covered by Regulation E, including brokerage and retirement accounts, the Bureau should clarify that these are included within the scope of §1033. The Bureau should coordinate with the agencies that primarily regulate those types of accounts on methods of oversight to ensure that consumer direct and permissioned third-party access to this data is preserved, including through action on consumer and third-party recipient complaints at other agencies about access restrictions. Many covered data providers already provide brokerage and retirement account data within the same consumer experience where they provide Regulation E-covered accounts, so the inclusion of these accounts in the rulemaking should not impose significant additional burdens on data providers.

Additionally, consumers would benefit from the inclusion of government benefit accounts used to distribute needs-based benefits programs. Today, more than 41 million people in the US receive benefits through Electronic Benefit Transfer (“EBT”) accounts that are primarily provided by two processors.[12] These lower-income individuals may be unbanked or underbanked and thus stand to benefit from financial products and services that can save them time and money and help them make financial decisions.[13] EBT accounts are designed as debit accounts with access devices including cards and online portals, but there are no requirements for EBT processors to provide electronic access to consumers’ data. If the Bureau does not include government benefit accounts within the proposed rule, those consumers may lose the ability to use existing services, like Propel, to manage their benefits, track their balances, and maximize the usefulness of their EBT funds.

Until the Bureau is able to issue detailed regulations about the applicability of §1033 to the above categories of consumer financial data, it should, at a minimum, make clear that the first

[12]“A Year in the Life of SNAP Households.” Propel, 2020. https://www.joinpropel.com/year-in-review-2020.
[13]“A Year in the Life of SNAP Households.” Propel, 2020. https://www.joinpropel.com/year-in-review-2020.

§1033 rule is not exhaustive in terms of §1033's protections and does not reduce the potential scope of statutory coverage under §1033. The CFPB should also make clear that regulations are not necessary to enforce §1033's statutory mandates.

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?

No, the Bureau should not exempt any covered data providers from particular proposals under consideration. The Proposal is clear in terms of its roles and responsibilities, and not overly burdensome for data providers, including smaller data providers. By placing obligations for both consumer disclosure and authorization management on authorized third-parties – i.e., the data recipient or data aggregator – the Proposal narrows the scope of obligations imposed on data providers. Exemptions would risk creating an unlevel playing field for consumers served by different sized data providers, where customers of some data providers have data access that others do not. All consumers should have their reasonable expectations for universal access to and portability of their information protected and preserved.

In particular, removing smaller data providers from the coverage of §1033 would harm both those institutions' consumers – who would be denied access to critical, competitive, and innovative financial services options – and overall competition by reducing the incentive for those data providers to offer services competitive with those of larger data providers or other innovative financial services providers. Over time this might even lead to greater consolidation in the banking sector if those exempted banks can no longer attract consumers because of their inability to support the data sharing with third parties that consumers want.

We agree that the impact of new regulations on smaller providers is of paramount concern. Based on our experience working with both small data providers and small data recipients, we have provided suggestions on how to minimize such impact (see our responses to Qs 15, 53, 76, 81, 91, 94, and 117, among others).

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?

Yes. Exempting certain covered data providers would negatively impact our organization, our thousands of data recipient customers, and the millions of consumers relying on us for permissioned access. Today's ecosystem already is rife with disparities among consumers' access to their own data, and exemptions would create incentives for further interference with consumers' access rights.

A strong CFPB mandate would incentivize core service providers to provide appropriate data

access solutions to their data provider customers.[14] Reliance on a core service provider should not change data providers' obligations, because the consumer's relationship is with their data provider and not their data provider's core service provider; consumers should expect their financial data access rights to be provided by their primary banking entity.

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?

Yes. Consumers and small businesses should expect a level playing field for access to their own financial information. Consumer-permissioned access to financial information has been shown to expand creditworthiness to underserved communities and provide access to small business credit.[15] The 50 million credit-invisible consumers would be particularly impacted by exemptions, as would minority-owned small businesses that benefit most from non-bank financing enabled by their authorized sharing of information.[16]

Today, banks with total assets greater than $10 billion hold 86% of banking assets, yet the more than 4,500 community banks in the United States that collectively hold over $3 trillion in assets represent 97% of the active bank charters.[17] More than 2,200 of those community banks are in rural communities of fewer than 50,000 people.[18] These community banks are essential to the communities they serve and rural communities would be disproportionately affected by an exemption for smaller banks.

Small banks also face competitive risks if third-party services are only available to consumers who bank with large financial institutions. Research shows over six in ten consumers would consider leaving their bank if they could not connect their accounts to third parties – so restricting access based on institution size could alter the competitive dynamics across sizes of financial institutions.[19]

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

---

[14] Research firm Gartner defines core banking systems as "a back-end system that processes daily banking transactions and posts updates to accounts and other financial records." Typically consumer-permissioned data access is provided by a digital banking platform, a subset of core providers.

[15] "[N]ew credit model outperforms the credit score in predicting delinquencies and charge-offs, that is, it identifies significant differences among all borrowers, even those with low credit scores". Di Maggio, Marco, Dimuthu Ratnadiwakara, and Don Carmichael. "Invisible Primes: Fintech Lending with Alternative Data." FDIC, February 10, 2022. https://www.fdic.gov/analysis/cfr/consumer/2022/papers/ratnadiwakara-paper.pdf.

[16] Research from New York University found that fintech lenders "played an important role in extending PPP loans to Black- and Hispanic-owned businesses."
Howell, Sabrina, Theresa Kuchler, and Johannes Stroebel. "Which Lenders Had the Highest Minority Share among Their Payment ... - NYU." New York University, December 10, 2020.
https://pages.stern.nyu.edu/~jstroebe/PDF/HKS_PPP_Minority.pdf.

[17] Sourced from FDIC Bank Data and Statistics https://www.fdic.gov/bank/statistical/

[18] Ibid.

[19] Plaid. "The Fintech Effect: Fintech's Mass Adoption Moment," October 12, 2021.
https://assets.ctfassets.net/ss5kfr270og3/5ibIlvGqujqTLronm8XgBX/19a1d7482945ddc2789a1d195dd91332/Fintech-Effect-2021.pdf?q=70.

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?

We do not believe there should be an exemption structure for covered data providers for the reasons outlined in our responses to Qs 6-8.

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.

Plaid does not believe there should be an exemption structure for covered data providers. If the Bureau were to provide a period of time before a data provider would be required to come into compliance with the rule, it nevertheless should make clear that it is permissible for authorized third parties to rely on screen scraping and similar technologies to serve consumer access needs during that transition period (as described in our responses to Q52 and Q54).

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?

We agree with the Bureau's Proposal that all individuals on an account should have access to information on and in the joint account, because this approach aligns with consumer expectations and behaviors. If multiple people have decided that they should have equal access to an account, then they will reasonably expect the same access either individually or jointly under §1033. As discussed in our response to Q117, authorized third parties would need to collect contact information on all account holders in order to satisfy other obligations regarding authorization management, disclosures, and troubleshooting.

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?

The authorization procedures outlined in the proposal are appropriate and well-defined. The primary benefit of the outlined procedures is that they position the consumer's authorization with the third party facilitating and managing the consumer's access, as opposed to the data provider responsible for making that consumer's data accessible. Positioning the third party to facilitate and manage authorization best serves consumers and the ecosystem, for the following reasons:

1. Consumers will receive the most accurate and appropriate disclosures with a singular authorization experience.[20] Because authorization captures a single set of consumer choices – i.e., "I want to share this data with *this* third-party recipient for *this* specific purpose" – the authorization experience needs to be singular and not split across multiple providers. Having the experience rest singularly with third parties as authorization managers leads to effective consumer control and protection, in that a consumer can direct that single party with a set of choices, expect their instructions to be followed, and expect resolution if that party does not act accordingly. In contrast, in today's environment, there are instances in which data providers serve separate, redundant, authorization experiences even after the consumer already permissioned the third party.[21] (See Appendix C for visual examples of data providers' permissioning experiences.) This duplicative authorization experience presents undue complexity to the consumer, introduces over- or under-collection risk, and may result in the consumer receiving inconsistent, incomplete, inaccurate and confusing authorization disclosures, particularly given the issues identified in parts 2-4 below.

2. The third party knows what information the consumer needs to access and share in order to power their selected use case; the data provider does not. Because the third party is the entity serving the consumer's desired use case, it has specific knowledge of the data elements, duration, and frequency required to serve the consumer's chosen use case. This is true whether the third party is the data recipient or the data aggregator.

Where the data aggregator is the third party, as part of their direct commercial relationship with the data recipient, the data recipient shares detailed information with the aggregator about the recipient's specific use case for consumers so that the aggregator can provide consumer-permissioned access to that particular data. The aggregator would capture consumer consent to that data scope authorization in order to access and share the consumer's information with the data recipient.

The data provider, on the other hand, generally does not have a direct relationship with the data recipient, and therefore does not have knowledge of the scope of data the consumer needs to share with the third party in order to power the use case. This lack of knowledge introduces risk of over- or under-collection by the third party, since the data provider might present the consumer with too many, too few, or incorrect authorization disclosures across multiple panes and click-boxes. For example, today, at least one data provider uses a one-size-fits-all authorization disclosure that informs consumers that they will be sharing their tax information with a peer-to-peer payments application,

[20] By "singular," we do not imply that there should be only one provider of authorization in the market, nor that every authorization experience be identical. Any third party should be eligible to provide and manage authorization, and there should be healthy competition among authorization managers like data aggregators who serve third-party data recipients.
[21] By "authorization experience," we mean the set of steps a consumer goes through in order to view disclosures and provide their consent.

despite that application not requesting that access, and such information not actually being accessed or shared by the data aggregator or data recipient application.

Conceivably, a data provider could request use case and scope information from the data recipient or the aggregator, but there is a very real risk that data providers will seek to challenge, approve, or disapprove third parties' use cases and specified data requirements, which would inhibit innovation and consumer access to the underlying financial services they select. It also would introduce an additional step, where, instead of the third party simply being able to act on consumer authorization, they would also need to keep the data provider informed of data access needs and use cases before effectuating authorization, which could interfere with a smooth consumer authorization experience.

3. **Having the third party act as authorization manager enables more effective regulatory oversight.** To effectively provide consumers meaningful data access rights, the Bureau should follow its proposal by regulating data providers with respect to access, and third parties with respect to authorization and data collection, use, and retention. Pairing authorization with data collection will significantly simplify Bureau oversight. If authorization were managed by the data provider, and only collection, use, and retention at the third party, for example, every instance of oversight relating to authorization would require the Bureau to look across both companies to match data provider authorization records with third party data retrieval and handling records.

4. Having the third party act as the authorization manager enables more effective consumer control and protection. Because authorization is where key terms of the consumers' requested access are disclosed and where consumers provide their informed consent, it is imperative that the experience be independent from anticompetitive behavior. Some data providers act on competitive incentives to withhold consumer data, while others introduce intentional friction into the authorization experience to discourage consumer information sharing.[22] Authorization disclosures and experiences managed by data providers are not only inconsistent across those data providers, but they are sometimes inaccurate, overly broad in their descriptions of the data to be shared, or crafted to intentionally dissuade consumers from sharing their data with financial service providers offering services competitive to those of the consumers' data providers.[23] (See Appendix C for data provider permissioning experiences.)

---

[22] "Many new market entrants rely on a consumer's ability to access and transfer their financial data to provide services, but big banks add unnecessary friction to this process to inhibit competition."
"Letter to CFPB from Consumer Advocate Coalition," May 27, 2021.
https://www.economicliberties.us/wp-content/uploads/2021/05/CFPB-Letter_5.27.pdf.

[23] "We have found that as the process by which consumers consent to permit access to their data is migrating from data aggregators to financial institutions' sites, completion rates once consumers are redirected to these sites vary considerably. This suggests that some have structured processes that, by design or otherwise, are sufficiently complex or contain warnings sufficiently dire to cause consumers to abandon the process midstream."
Silberman, David, and Corey Stone. "CFPB Should Write a Data Sharing Rule That Can Evolve with the Market." American Banker. American Banker, August 3, 2022.
https://www.americanbanker.com/opinion/cfpb-should-write-a-data-sharing-rule-that-can-evolve-with-the-market.

The way to shield consumers from anticompetitive practices during authorization is to place authorization in the hands of the entity better aligned with consumers' intentions to access and share their data, while establishing clear guidelines to ensure those entities act appropriately. In consumer-permissioned data sharing, the authorized third-party data recipient or aggregator is that entity. At the time consumers seek to authorize access and sharing, they will have already taken steps to sign up for a new use case provided by the third-party data recipient, indicating their intent to avail themselves of that data recipient's financial services. Consumers can, in the context of that use case, and with the transparent disclosures outlined in the proposal, make informed choices regarding their comfort level with sharing their information.

5. Consumers' financial lives are complicated, and managing authorizations should be easy: Most consumers use financial technology applications that rely on consumer-permissioned data because it saves them time and makes managing their finances easier.[24] The process of authorizing access to one's financial data and managing those authorizations should not introduce unnecessary complexity to consumers' already-complicated financial lives. By allowing authorized third parties like data aggregators to specialize in managing authorizations, consumers can benefit from authorized third-party access to their data, without facing new complexities in their financial lives.

Costs of this proposal are minimal

Under this proposal, data providers would not incur any costs to develop or implement authorization, since it would be facilitated and managed by third parties. For some providers which have chosen to build authorization disclosures already, the proposal would reduce their costs because they would no longer need to maintain those disclosures and software systems.

For third-party data recipients, the costs would depend on whether they choose to facilitate and manage authorization themselves, or to rely on data aggregators to do this for them. If they choose to do it themselves, then they would incur the costs of building a new consumer experience and complying with the obligations placed on the entity that manages authorization. If they rely on a data aggregator, then there would be no direct additional costs, since data aggregators would be required to facilitate and manage authorization as part of their services to the data recipient.

Data access rights can level the playing field for consumers by offering equivalent products regardless of their data provider. Data recipients see it as critical to be able to reach consumers from all data providers, but building and maintaining individual connections with thousands of data providers' third-party access portals could be costly for data recipients. This is why most

[24]Plaid. "The Fintech Effect: Stability, Impact, and Building for the Future," October 18, 2022. https://assets.ctfassets.net/ss5kfr270og3/5ibIlvGqujqTLronm8XgBX/19a1d7482945ddc2789a1d195dd91332/Fintech-Effect-2021.pdf?q=70.

data recipients rely on data aggregators to both build and manage those connections, and to manage the consumer permissioning experience. The Bureau should ensure that data recipients can continue to rely on data aggregators to manage authorization, as described in our response to Q14.

Third-party data aggregators seeking to manage authorization would face costs of building these experiences and complying with the obligations placed on the entity that manages authorization.

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.

As a consumer experience that enables critical, informed data sharing, authorization will become a competitive terrain in financial services, with companies competing to build the best, compliant consumer experiences.[25] The Bureau should establish core authorization requirements as outlined in the proposal – (1) provide authorization disclosures consistent with use case scope (and the ability for a consumer to select the specific accounts from which they want to share data), (2) obtain informed consent, and (3) certify that the third party will abide by obligations related to that consent – but should not overly prescribe the methods through which those requirements are accomplished. Authorization methods should be allowed to evolve alongside technology and consumer preferences, while still meeting the Bureau's requirements.

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?

Where a data recipient relies on a data aggregator to access consumer data from a covered data provider, the required data access authorization procedures and obligations should apply to the data aggregator.

As discussed in our response to Q12, authorization should be singularly managed in order to ensure accuracy, avoid consumer confusion, and mitigate against over- or under-collection. Just as authorization should not be split across the third party (recipient or aggregator) and data provider, nor should it be split across the data recipient and aggregator. In instances where a recipient relies on an aggregator, by having the aggregator facilitate and manage authorization,

[25] As an example, companies like Plaid already invest in building user-friendly experiences like Plaid Link, where we obtain the consumer's permission prior to accessing and sharing their data, and Plaid Portal, where consumers can view the data connections they have made through Plaid between their data provider and data recipients. Consumers can also use Plaid Portal to turn off any of those connections and instruct Plaid to delete their data. Regulation is likely to increase companies' investment in, and competition among, these tools. (See Appendix D for an example of Plaid's account linking experience, and Appendix G for Plaid's Portal.)

consumers will have more consistent experiences and a clearer understanding of which participant is responsible for managing their data sharing requests, as well as the security and fraud prevention benefits that come with reliance on an aggregator.

The data recipient and data provider should receive copies, in an agreed upon format, of the consumer's authorization from the aggregator, so that all parties involved have a common understanding of the consumer's authorization and consent. (See our responses to Q27 and Q75 for detail.)

In order to provide consumers with consistent data use and retention obligations across the entire system, data recipients should be required to have their own disclosures around their data collection, use, retention, and deletion. Those disclosures should live either in their end user privacy policy or as part of the data recipient's consumer onboarding process. But these disclosures should be distinct from the authorization disclosure, which should only apply to the party carrying out the authorized access on the consumer's behalf, because the act of receiving data does not necessarily require disclosure of information about account selection and management of connections with the data provider.

There may be some instances of an aggregator relying on another aggregator to provide access. The industry term for this is "wrapping," and it generally involves a commercial relationship between the two aggregators. Typically under such arrangements, one aggregator works directly with the data recipient to accept a consumer's access request, then that aggregator sends the consumer's access request to the other aggregator (the "wrapped" aggregator) to effectuate it by requesting the data from the data provider. In these cases, the aggregator that maintains a relationship with the data recipient should facilitate and manage authorization since, as described in our response to Q12, that aggregator, as a result of its relationship with the data recipient, will have the information necessary to provide a compliant authorization disclosure and obtain informed consent. The wrapped aggregator should not be required to facilitate or manage authorization, but could be required to operate under narrower collection, use, and retention policies since the wrapped aggregator does not obtain its own authorization from the consumer, instead functioning only as a service provider to the other data aggregator.

Q15. How could the CFPB reduce costs and facilitate compliance for small entities? Should the CFPB consider alternative authorization procedures for certain categories of third parties? If so, why would such procedures be appropriate?

The Bureau could reduce costs and facilitate compliance for small data recipients by clarifying that those entities can rely on third parties to manage authorization. This is in many cases the status quo today, where data aggregators reduce costs and compliance for both small data providers and small data recipients by managing the process of obtaining consumer permission to access their permissioned financial information. Additionally, the Bureau could reduce costs on small data providers by narrowing the scope of their requirements to verify third-party authorization, as discussed in our responses to Q73.

This is not meant to suggest that every data recipient needs to rely on a data aggregator for authorized access. The Bureau may be able to reduce costs and facilitate compliance for small entities that do not rely on data aggregators by providing alternative authorization procedures that apply narrowly to those use cases. For example, a small accounting firm that serves only small businesses in a single municipality may need only to gather information from local data providers. In this case, the authorization disclosure may be a once-a-year form as opposed to a just-in-time disclosure.

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?

As a principle, authorized access should mirror direct access, because many digital financial services will work more effectively – and often only – with consumer-permissioned access for a third party. For an account held by multiple consumers, this means any individual who has direct access to the account should be able to authorize equivalent third-party access, without additional friction. If consumers have already decided to share access to an account, then having equivalent access rights to authorize third-parties aligns with their expectations. Requiring authorization from each account holder would result in a cumbersome process, particularly for business accounts which may have dozens of account holders.

On the other hand, permitting a single account holder to choose to authorize access on behalf of all others may not be sufficiently transparent. To strike a balance between access and transparency, the Bureau should require that the authorized third party notify all account holders upon receiving authorization from any account holder or agent. This would give all account holders insight into the data sharing activities taking place at their accounts, without disrupting their shared account holders' access. The Bureau should recognize that in order for authorized third parties to send these notifications, they require contact information for all of the relevant parties (see our response to Q117 for more details on authorized third parties needing to collect contact information in order to manage authorization and consent).

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.

As noted earlier in these comments, portions of the financial services industry already are subject to disclosure rules regarding sharing of nonpublic personal information. As the Bureau considers authorization disclosures, it initially should determine whether any GLBA disclosure requirements are sufficient to accomplish the Bureau's goals and, in any final rule, be clear on its decision about compliance equivalency. See response to Q1, in which we propose that

compliance with the GLBA's annual notice requirements could satisfy any annual notice requirements promulgated under §1033.

The information categories proposed for inclusion in authorization disclosures – key scope and use terms, reference to the third party's certification, and a request for consent – should be required. However, authorization of specific account types introduces a resolvable (with clarity in the §1033 rule) timing challenge: if the consumer is using a third party for the first time, unless the Bureau requires that certain information be made available to the third party as the third party facilitates authorization, that third party will not know what accounts the consumer has at the data provider and so will be unable to enable the consumer to select the specific accounts from which the consumer wishes to share data. The Bureau should set rules for authorization so that the third party recipient or aggregator can accurately determine the available accounts in order to include that information in the scope part of the authorization disclosure.

In addition to disclosing the general categories of information to be accessed as part of the key scope terms in the disclosure, if the Bureau prescribes any limitations on use of the data accessed under §1033, then the Bureau could consider requiring the disclosure to display "reasonably necessary" and "secondary uses" for collection. Note, elsewhere in our comments, we recommend modification of the Bureau's proposed definition of "reasonably necessary" uses of the consumer-permissioned data to also include what we term "reasonable and expected" uses of consumer data that are common and non-controversial across industry and are typically employed to run a safe and well managed business (see our response to Q88).

Insofar as reasonable and expected uses are included as "reasonably necessary" in this rulemaking, however, disclosures pertaining to reasonable and expected uses should not be required to be included in the authorization disclosure because they are presumed. Reasonable and expected purposes are generally applicable business practices that do not pertain specifically to the use case for which the consumer is consenting, so they should not clutter that disclosure. Instead, the authorization disclosure should include a mechanism to allow a consumer to view the reasonable and expected uses at their convenience, such as in the accessible long form privacy policy. This would still allow a consumer to evaluate their willingness to share their information based on those uses, without disrupting their reasonably necessary use authorization.

Plaid also supports including in the key "use terms" the identities of intended data recipients and data aggregators to which the information may be disclosed, and the purpose for accessing the information. This requirement supports the consumer's ability to make informed choices about whether to share their information. Although it is our practice to have the third-party data recipient and any aggregator identified during the process by which we currently obtain consumer permission to access their permissioned data, this also is an example of a place where GLBA-informed standards may be useful both to avoid unnecessary expense and burden for businesses and to protect the consumer from getting so much information that the most pertinent details are lost; instead of providing the consumer with extensive detail on this issue

as part of the authorization, these details could be part of the long form privacy policy and/or annual privacy disclosure.

For an example of information Plaid currently provides in some of our account linking flows, see Appendix D.

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

Generally, no. The Bureau can sufficiently ensure consumer protection by describing the contents of the disclosure and prohibiting deceptive, misleading, or abusive statements. Model clauses or forms would introduce risk of falling behind innovation because we cannot predict consumers' future communications preferences, nor how technology itself might shape those experiences. The pace of innovation and development of new use cases would also put model disclosures at risk of becoming obsolete. For precedent we need look no further than the transition from paper to fax to computers to mobile.

Because consumer-permissioned financial data sharing involves a multitude of use cases, disclosures should include key scope and use terms that reflect specific use cases – a concept which is difficult to reflect in specific model clauses and forms.

If the Bureau does determine that model clauses or disclosures are necessary, it should take a principles-based approach focused on transparency and comprehensibility, as opposed to prescriptive language that would be difficult to evolve and adapt.

The Bureau may wish to consider a model disclosure for very small firms that engage in *de minimis* data access. See our response to Q15 for our perspective on this issue. For these firms, the cost savings of having a standard disclosure may outweigh the disadvantages of model disclosures described above. The Bureau could limit the applicability of these small entity model forms based on the number of data requests the company makes per year, the geographic area the company serves, or other criteria that would limit use of the model form only to the small entities who would most benefit from it.

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.

The Bureau should include requirements on both the timing and format of the authorization disclosure.

For timing, in most use cases, consumers should be expected to provide consent just prior to the time the authorized third party accesses their data as part of an authorization experience. There may be use cases in which a consumer signs up for a service but access to the

consumer's data is not required until a later time (e.g., a small business signing up for a tax preparation service in January, the service only requires access to the account in March to collect necessary tax documents prior to April 15). In order to capture both of these instances, the Bureau should require that authorization disclosures happen just-in-time, inclusive of either at the time of sign up for a new service, or immediately before the authorized third party will request access to their data from the data provider.

We recommend that overall disclosures be broken down into three categories to ensure consumers receive the right information when they need it:

> (i) **Authorization disclosure:** information to be included "just-in-time" prior to the request for consumer consent to access the consumer's information (e.g., key scope and use terms as set out in the proposal);
> (ii) **Post-authorization details:** Information presented after the authorization (e.g., how to revoke access or request deletion of data, periodic disclosures, reauthorizations,); and
> (iii) **Privacy policy:** Information to be included in longer form made accessible to the consumer from the authorization experience prior to consent by the consumer (e.g., privacy policy that includes information on retention policies, legal requirements, and the certification statement).

For format, the Bureau should direct that the authorization disclosure be clear and conspicuous and should prohibit deceptive, misleading, or abusive statements. The Bureau should refrain from an overly prescriptive segregation requirement that could interfere with the authorization experience.

If the CFPB were to impose data use limitations under this rule (see our response to Q88), and permit authorizations only for what is "reasonably necessary" to deliver the service, then this level of detailed disclosure may not be necessary and pre-populating consent requests might not present risk to consumers. That said, we recommend requiring that the consumer take an affirmative step (including clicking a button) to consent to access the data for sharing, and also prohibiting deceptive, misleading, or abusive practices related to authorization.

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?

We agree with the Bureau's Proposal to require an authorized third party to provide consumers a copy of their signed authorization, such as a consent receipt message. This would support consumer transparency and control, while providing uniform expectations across third parties that the Bureau can easily oversee. The Bureau should be flexible in its requirements for what constitutes an electronic signature, since technologies develop over time and consumers will expect their digital experiences to keep pace.

As discussed above, the signed consent could include information on how to revoke access or request deletion of data and be saved for future reference. If the authorized third party is expected to deliver a copy of the consumer's signed consent to the consumer, it will need contact information for that consumer. Therefore, regardless of the use case the consumer is permissioning, authorized third parties should always be permitted to collect relevant identity and contact information in order to comply with disclosure, notice, and delivery requirements. (For more details on this proposal see our response to Q117.)

The Bureau should not prescribe the mechanism by which such a copy would be delivered, since messaging systems and consumer preference will change over time, and consumers should be able to select their own contact preferences (text, email, mail, phone call, permissions portal). For the reasons outlined in our response to Q12, the Bureau should also clarify that the copies of the signed authorization should come from the authorized third party, so consumers know which party is responsible for that authorization.

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

Without a clear understanding of the length or form of the certification statement, our perspective is that the full certification statement should not be included in the authorization disclosure, since it may clutter the experience and distract from active consumer choices during authorization. The authorization disclosure should focus entirely on the key scope and use terms, so that the consumer can make informed decisions in-real-time.

A reference to the certification statement could be included in the authorization disclosure (for example, a stamp of certification), along with a link to the full certification statement (which could be located on the authorized third party's public domain or included in the long form privacy policy made available during the authorization experience). This stamp of certification would provide assurance that the authorized third party will act according to its obligations regarding collection, use, and retention of the consumer's information, and should be easily accessible both inside and outside the authorization experience.

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

<u>Input on the Bureau's proposed approach to defining data scope</u>

The Bureau's proposed approach of enumerating data categories is appropriate, and will ensure uniformity and consistency for consumers across their covered data providers.[26] Alternative

[26] In keeping with the Bureau's usage, we use the term "data categories," to describe the broad groups of information (e.g., identity information, account information), and "data elements" to describe granular pieces of information that sit within those categories (e.g., zip code, account number).

approaches, such as a broader definition like “all online banking data,” risk creating a perverse incentive for data providers to remove data from their online financial account management portals, giving consumers decreased access to their data. Consumer access under such an approach would also differ depending on the entity with which the consumer banks, meaning that consumers would have access to a different mix of information, and thus third-party services, based on their bank choice, with the cause of those differences likely opaque to most consumers.

On the other hand, specifically enumerating every single permissible data element would also carry risks, most prominently the possibility that the enumerated data elements become obsolete or incomplete or that new, unenumerated data elements could be useful for yet-to-be-developed use cases, leaving consumer access rights for those new data elements unprotected. In the event of either of these possibilities, the Bureau would need to update the regulation to ensure consumers’ right to access to their data remained preserved.

Open Banking in Europe has shown the downsides of both specifically enumerating data elements and too narrowly scoping data categories. As originally implemented, the data access and sharing contemplated by Open Banking regulations in Europe was limited to certain specified account types, while other data categories were not included within the regulations’ purview. This significantly impeded consumers’ ability to use innovative and competitive financial services (outside of the narrow subset of services premised upon the limited account type information consumers could share). Further, though there is now a desire to move from Open Banking to a broader “Open Finance” regime (where consumers can share a broader range of data to obtain a wider variety of competitive and innovative financial services), this transition has been discussed for nearly four years, and new data elements still have yet to be introduced.[27] Meanwhile, consumers in Europe continue to face challenges to availing themselves of that wider range of services.

Accordingly, the Bureau’s category-level approach (with data elements thereunder being illustrative, as opposed to exhaustive) appropriately balances the need for clarity with regard to consumer access rights and coverage, with the need for flexibility to incorporate future data elements as innovation develops. The Bureau can provide guidance in the future on how new data elements fit into existing data categories, and review industry-built technical standards to ensure that any new data elements are accurately reflected in third-party access portals.

Put simply, we believe the Bureau has three ways to shed light on data categories and types:

1. Regulation articulating consumer rights and prescribing obligations of covered entities, products, and general data categories;
2. Guidance to add or refine specific data elements which need to sit beneath those categories without being exhaustive;

[27] “Next steps for Smart Data” UK Gov https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915973/smart-data-consultation-response.pdf

3. Allowing industry bodies who can deliver technical standards to ensure any enumerated, illustrative data elements are reflected in technical capabilities in a third-party access portal. Industry bodies, like FDX, should also be permitted to define and expand upon specific permissible data elements and scopes within the parameters of applicable regulation.[28]

This multi-faceted approach to enumerating illustrative (not exhaustive) data elements provides strong foundational rights that would be consistently applied, while enabling industry bodies and Bureau-guidance and standards to move more quickly to adapt to the speed of innovation.

Feedback on categories and types

Plaid believes that all data categories on the Bureau's list of specific data categories should be included, with one exception: consumer reports. These reports are commercial products that a data provider typically paid a fee to obtain from another party. All other data categories in the proposal are byproducts of a consumer's direct engagement with a data provider. Excluding consumer reports from the list would maintain the principle that the consumer's data is that generated as a result of their interaction with the data provider. Moreover, including consumer reports is not necessary. Consumers have adequate means of obtaining their consumer reports, and data recipients who have a permissible purpose for requesting the report may do so pursuant to other means.

The Bureau should require that the categories of information covered be made available in their original, unaltered form to consumers. Data providers have implemented technologies that mask or tokenize underlying information such as account and routing numbers, which results in severe disruption of consumer use cases and makes it more difficult for third parties to identify fraud across the ecosystem. For example, a consumer might authorize a third party to access their account and routing number in order to generate printed checks to pay vendors – but if the data provider masks the account number, then the consumer's use case fails because the printed check does not capture the masked number. Or, because checks and wires are incompatible with tokenized account and routing numbers, attempts to collect money by an initiating party fail. Another example is that third party fraud verification does not work with tokenized numbers, and they interfere with fraud detection generally, because fraud programs cannot use automated systems that build on knowledge of risky accounts and patterns over time.[29]

To protect consumers who actively share data not covered in the Proposal, the Bureau should expand the categories in the Proposal to also include lending and assets data as outlined in our

[28] For example, industry-led data scoping in the United States has shown its ability to evolve quickly to meet market and consumer demand, with FDX already including data elements for investments, loans, and tax information in its model specifications – a data scope broader than this Proposal.

[29] Tokenized account numbers also introduce a fraud vector: fraudsters will apply for multiple loans using the same bank account. Because only a tokenized number is provided, the lender is unable to determine that it is in fact making multiple loans to the same consumer. The fraudster will then revoke access after the loan is disbursed. By revoking access to tokenized bank account numbers, fraudsters can then disable third parties' ability to determine which account the funds went to, making it difficult if not impossible to identify the account originating the fraud, recover the funds, and take other appropriate actions.

response to Q5 and detailed in our Appendix B. Millions of consumers today share lending and asset account information through Plaid with third-party data recipients. Excluding those data categories could result in consumer harm, either in the form of lost access to that information and third-party products and services, or in consumers being charged for access to this information they had previously received at no cost. If the Bureau decides not to expand the scope of this rule, then, at a minimum, the Bureau should include language in the rule that makes clear it is not intended to be exhaustive or to limit the full scope of potential applicability of §1033, and that a regulation issued pursuant to §1033 is not necessary for enforcement of the statutory requirement.

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?

As described in our response to Q22, the Bureau's category-level approach (with data elements thereunder being illustrative, as opposed to exhaustive) appropriately balances the need for clarity with regard to consumer access rights and coverage, with the need for flexibility to incorporate future data elements as innovation develops. The Bureau should use a combination of regulations, guidance, and standards to both provide strong foundations for consumer access rights and enable continued innovation in this space. In the context of the rulemaking, the Bureau can recognize as illustrative but not exhaustive the specific data elements within a particular listed category that consumers and third parties describe as currently sought or available as a way to preserve the current status quo without limiting future evolution of consumer use cases. In addition, the Bureau should, in the absence of issued guidance, permit industry bodies like FDX to define specific permissible data elements and scopes, as well as to innovate and develop access solutions, including programs to certify providers' implementations.

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.

Data providers typically make at least two years of transaction histories available for direct download. Consumers expect this same level of detail when sharing historical transaction data with third parties. Consumers unable to access two years of transaction history often contact Plaid asking us to retrieve the two years of data they require. Third parties often take the position that transaction histories shorter than two years are insufficient to provide insight to evaluate various items in use cases such as tax filing or evaluating creditworthiness. Cash flow-based use cases would particularly suffer if less than two years transaction history were available.

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?

The Bureau should require data providers to make bill pay details available to consumers and their authorized third parties. With this information, consumers can: (i) better track their recurring account payables; (ii) prevent unexpected consumer overdrafts and overdraft fees; and (iii) identify and eliminate unwanted recurring payments. Institutions that offer built-in bill pay functionality should serve this function to consumers in online financial account management portals. Including these data elements in the scope of §1033 would result in competition and innovation.

Being able to share information about planned inflows and outflows of money from a consumer's account are vital for that consumer to be able to use personal financial management products and services. With access to this information, consumers can benefit from greater insight and control over their bill pay experiences, including selecting from which accounts to pay their bills at a third party experience. This information would also allow consumers to more easily switch banks (helping to maintain a competitive marketplace) by enabling a consumer to easily port their regular payments to a new provider in a single action, instead of needing to manually enter each individual payment instruction one-by-one to a new provider.

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.

The Bureau notes a question about the degree of consumer benefit of authorized third-party access to certain identity and characteristic information and also suggests that the authorized third party could obtain such information directly from the consumer. With respect to the benefits of such authorized access, authorized third-party access to consumer's personal information can: (i) prevent fraud by helping a third party verify that a consumer is the same as the owner of the accessed account; (ii) simplify consumers' ability to switch and open new financial accounts; (iii) allow for more personalized experiences; and (iv) engage with consumers in their preferred methods of communication. See our response to Q27 for more details on how authorized access to personal information prevents fraud. While in certain circumstances it may be beneficial to obtain identity and characteristic information directly from a consumer (particularly for third-party data recipients), there are downsides to that approach, including the potential for consumers to accidentally mis-enter information and introduce accuracy issues. Similarly, to the extent authorization is a nexus for consumer engagement and also a potential fraud vector, authorization providers need to be able to develop anti-fraud mechanisms, which in large part depend on the ability to identify and match personal information.

We understand the Bureau's concerns that sharing certain consumer identity information with authorized third parties may present fraud, privacy, and other consumer protection risks. However, we believe that the Bureau can mitigate such risks and advance the security and privacy of information related to the identity and characteristics of the consumer in the following ways, which do not infringe on the consumer's right to access and share their information:

- Requiring all authorized third parties to maintain security programs, as discussed in our response to Q111;
- Allowing authorized third parties to develop security, fraud prevention, authentication, and identity verification tools as "reasonably necessary" uses of shared data, to better protect consumers and benefit the integrity of the overall ecosystem;
- Tiering the risks associated with disclosure of the above-described information according to severity, and requiring additional safeguards when consumers share highly sensitive personal identity information like social security number (see our response to Q89);
- Adopting widely-recognized industry security and privacy standards, including the Open Finance Data Security Standard,[30] SSAE18 Trust Service Criteria for Confidentiality, Integrity, and Availability,[31] ISO 27001,[32] and NIST CSF;[33]
- Setting requirements on third parties for authorization (e.g. data minimization, revocation, and deletion obligations) in the final rule that would further minimize any risks of making information related to the identity and characteristics of the consumer available to authorized third parties.

In addition, the security protocols for data providers' third-party access portals are robust and industry-proven.[34] Any security risks would also be mitigated by the outlined proposal's requirements that data providers only enable access to authenticated third parties which present proper evidence of consumer authorization (see our response to Q80).

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?

The confirm/deny model presents several challenges, and we do not recommend its adoption in regulation. Specifically, this model: (a) introduces significant, costly technical requirements for all parties; (b) reduces the effectiveness of anti-fraud tools; (c) reduces the effectiveness of Know Your Customer/Anti-Money Laundering ("AML/KYC") programs; (d) raises competitive concerns;

[30] "Open Finance Data Security Standard (OFDSS)." OFDSS. Accessed January 24, 2023. https://ofdss.org/.
[31] "2017 Trust Services Criteria (with Revised Points of Focus – 2022)." AICPA. Accessed January 24, 2023. https://www.aicpa.org/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022.
[32] "ISO/IEC 27001 and Related Standards - Information Security Management." ISO, October 25, 2022. https://www.iso.org/isoiec-27001-information-security.html.
[33] "Cybersecurity Framework." NIST, January 19, 2023. https://www.nist.gov/cyberframework.
[34] "FDX Security Specification Boosted with FAPI." Financial Data Exchange, November 11, 2021. https://www.financialdataexchange.org/FDX/FDX/News/Announcements/FDX_Security_Specification_Boosted_with_FAPI.aspx.

(e) prevents consumers from accessing and sharing their raw data for a number of reasons beyond identity verification; and (f) places the Bureau in a position of specifying architecture that the industry could otherwise resolve on its own. The Bureau instead should apply the same authorization and collection, use, and retention requirements as it is contemplating for all other consumer information.

(a) **A confirm/deny model introduces significant, costly technical requirements for all parties.** It would require a data provider to build and maintain new software code, which could be different across data providers and create inconsistencies for data recipients. For example, a data provider would need to create a new mechanism to receive data programmatically from third parties, evaluate that data, and make a confirm/deny decision. To the extent these mechanisms do not already exist, this would substantially increase costs for all parties, including data providers, data aggregators, and data recipients.

(b) **A confirm/deny model reduces the effectiveness of anti-fraud tools.** Specifically, eliminating data recipients' ability to collect identity information will lead to more fraud**.** Data recipients typically match consumer-provided information with the information that consumer holds at their data provider in order to help verify ownership of an account to reduce account takeover (ATO) and other transaction fraud. Fraudsters who have taken over accounts will often attempt to change email or phone number information to get access to one-time passcodes (OTPs) in order to bypass multi-factor authentication (MFA). Ensuring data recipients can access "raw" identity information will help reduce the success of these tactics. Perversely, a pass/fail matching mechanism hosted by a data provider may in fact create more fraud, since the third-party relying on that matching for fraud prevention would not be in a position to adjust its systems to monitor for new types of fraud.

(c) **A confirm/deny model reduces the effectiveness of Know Your Customer/Anti-Money Laundering ("AML/KYC") programs:** Some data providers have objected to sharing name and other consumer information that the data provider uses in its AML/KYC process because they don't want a third party to rely on or benefit from the data provider's AML/KYC when they should be conducting their own. To be clear, third parties already are required to conduct their own independent AML/KYC under existing applicable law, and already are prohibited from relying on a data provider's AML/KYC. A confirm/deny approach would ironically look very much like the third party relying on the data provider for AML/KYC. Additionally, eliminating a data recipients' ability to collect identity information will create undue friction for consumers and third parties as they meet their AML/KYC requirements. Consumers often authorize access to their name and other personally identifying information so that the third party can populate that information into the forms the third party uses for AML/KYC. This saves the consumer the work of filling out the forms themselves, and is a convenient way to share information that the data provider only has because the consumer gave it to them in the first place.

(d) **A confirm/deny model raises competitive concerns**. Specifically, a confirm/deny approach creates a new vector for competitive tensions. Consumers entering their information with the authorized third party will inevitably introduce errors, such as typos or outdated names (e.g. maiden names). Data providers will have every incentive to interpret such errors strictly, as a pretext to deny consumers the ability to onboard to services that may compete with the data provider.

(e) **A confirm/deny model prevents consumers from accessing and sharing their raw data for a number of reasons beyond identity verification**. A confirm/deny approach does not account for the additional products and services consumers want that rely upon them accessing and sharing their identity data. Two examples include: (i) automated form filling, in which data recipients can use identity data to automatically fill-in forms, such as bill pay information when they engage a new provider; and (ii) change of address monitoring, in which data recipients are notified when Plaid detects an address change so that they have the latest data on file.

(f) **A confirm/deny model places the Bureau in a position of specifying architecture that the industry could otherwise resolve on its own.** Were such a solution to arise, it should result from industry demand as opposed to regulatory obligation. We have not seen such demand.

The costs and downsides far outweigh the limited upside of a confirm/deny approach, particularly in light of the benefits described in Q26 and the privacy and security measures in place (also described in Q26) to mitigate any privacy and security concerns. The Bureau should not proceed with this option.

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?

As referenced in our response to Q5 and Q22, the Proposal's exclusion of asset and lending account data leaves millions of consumers potentially unprotected. While the Bureau evaluates the costs and benefits of expanding the scope of covered data providers, it should require that the data providers covered by the proposal include those data elements in their third-party access portals. The Bureau should also, at a minimum, make clear that the first §1033 rule is not exhaustive in terms of §1033's protections and does not reduce the potential scope of statutory coverage under §1033. Finally, the Bureau should make clear that regulations are not necessary to enforce §1033's statutory mandates. For details on data elements consumers currently have access to that fall outside the scope of the Proposal, see Appendix B.

Beyond those categories, the Bureau should also include Electronic Benefit Transfer accounts, and also Primary Account Numbers (PAN) associated with Regulation Z covered accounts.

Primary Account Number includes the full PAN, expiration date, name, and Card Verification Value (CVV). PAN access enables better fraud mitigation, by instantly verifying debit cards, and more payment options, by letting a consumer link multiple payment types at once.

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?

As referenced in our response to Q22, consumer reports fall beyond the scope of consumer-provided information, and might introduce contractual difficulties for data providers that purchase those reports from credit reporting agencies. Otherwise, the information outlined in §III.C.1.vi is not substantially distinct from other information any size data provider might be expected to provide to their consumers.

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).

We agree with the Bureau's narrow and strict construction of the §1033(b) exceptions to §1033(a). Any data categories and types required under §1033(a) (including those listed in §III.C.1.(i)-(vi), though this list should not be seen as exhaustive) should be expressly excluded from the exceptions under §1033(b). In particular, the Bureau should specifically prohibit two practices some data providers deploy today:

1. **Claiming, because an algorithm is proprietary, so are its inputs and outputs:** Data providers may claim that any consumer information fed into or generated by an algorithm must be treated as confidential or proprietary information subject to the exception in §1033(b) for "any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors." While an algorithm may itself be confidential information, neither the information fed into that algorithm nor the output of that algorithm are inherently confidential information, although they may be. In fact, they are often shared directly with consumers in the everyday course of business. For example, an interest rate charged to a consumer may be derived from a proprietary algorithm, but the interest rate itself is not proprietary and must already, by law, be shared with the consumer. The consumer should have the same right to that data under a §1033 rule.[35]

2. **Deliberately moving data outside the course of everyday business:** Section 1033(b) contains an exception for "any information that the data provider cannot retrieve in the

[35] We would support regulatory language prohibiting reverse engineering algorithms using data obtained through §1033 access, which would more directly address data providers' concerns without restricting consumer access rights.

ordinary course of its business with respect to that information." To try to bring data under this exception, a data provider may move ordinarily-retrievable data to locations that do not permit retrieval within the ordinary course of business in order to make it less accessible to a consumer. A §1033 rule should not create an incentive for this behavior, and the Bureau should pay attention to the rationale for any changes in data availability at institutions under its jurisdiction.

These examples illustrate the variety of ways in which a rule broadly defining a §1033(b) exception could be used to restrict consumer access and swallow the §1033 rule, harming consumers and competition. To protect consumers' access, the Bureau should provide clear guidance on narrow and strict exceptions in §1033(b), and clarify that such exceptions should not be used as a pretext to shield data from §1033(a)'s purview. Please also see our responses to Q32-37.

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

As long as the Bureau narrowly and strictly construes the §1033(b) exceptions, small covered data providers will not face disproportionate impact. Because the exceptions relate to information small covered data providers already do not display directly to consumers, they do not create any new requirements for those entities, both in the case of a dedicated third-party access portal and screen scraping.

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?

We agree with the Bureau's interpretation of "confidential commercial information" in the context of §1033. Any definition of "confidential commercial information" should expressly exclude: (i) the data categories required to be provided under §III.C.1.(i)-(vi); (ii) any other data or information that a consumer could use to obtain a product or service from an entity other than the covered data provider; or (iii) any other data or information that would allow a consumer to better evaluate the consumer's use of a consumer financial product or service from the covered data provider. Please also see Plaid's comments in response to Q30.

"Confidential commercial information" should include a covered data provider's proprietary, nonpublic technical and business information that is not a consumer's data. This includes trade secrets and other proprietary reports or products, business strategy, financial holdings, employee data, and regulatory filings – particularly to the extent that the disclosure of such information could cause substantial competitive harm.

In the event of a dispute – for example, if a consumer attempts to access information directly or through an authorized third party that the data provider believes is confidential commercial

information – the burden should be on the data provider to demonstrate that the data claimed is in fact "confidential commercial information."

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?

Currently, authorized third parties wishing to minimize screen scraping must often negotiate with data providers for access to their third-party access portals (to the extent such data providers have them). As part of those negotiations, authorized third parties have to negotiate with each individual data provider for specific data elements to be made available in the third-party access portals. "Confidential commercial information" is frequently cited as the basis for excluding certain data elements from the third-party access portals, even though those elements are otherwise available directly to consumers through the data providers' online financial account management portals.

The result is that: (i) consumers who bank with certain data providers may not have access to the information intended under §1033(a), resulting in potential harm to those consumers; and (ii) consumers experience inconsistent outcomes depending on the data provider with which they bank. See our response to Q143 for details on the differences in consumer access policies across different data providers. As described in our response to Q30, until the Bureau issues guidance on data categories and data elements that must be made available under §1033(a), data providers may be able to withhold information by calling it "confidential."

As an example, in negotiations, certain data providers have characterized a consumer's identity information (including their telephone number and address) as "confidential information," not subject to access. Their argument is that, because this information is used for proprietary processes (e.g., fraud checks), those processes make the underlying data confidential. However, while the proprietary technology and algorithms (e.g., those used to conduct those fraud checks) may indeed be "confidential commercial information," the underlying data – and even sometimes the output – is not. As another example, one data provider excluded interest rates from its third-party access portal on the basis that interest rates are confidential commercial information produced using algorithms that a third party could hypothetically reverse engineer. However, there is a clear distinction between the algorithm itself (which may very well be confidential commercial information) and the data output from that algorithm. As noted in our response to Q30, we would support regulatory language prohibiting reverse engineering algorithms using data obtained through §1033 access.

To guard against consumer harm and inconsistent outcomes, the Bureau should make clear that "confidential commercial information" expressly excludes the following data: (i) the data fields required to be provided under §III.C.1.(i)-(vi); (ii) any other data or information that a consumer could use to obtain a product or service from an entity other than the covered data provider; or

(iii) any other data or information that would allow a consumer to better evaluate the consumer's use of a consumer financial product or service from the covered data provider.

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?

We agree with the Bureau's proposed interpretation of "for the purpose of" to 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."[36]

For further clarity, Plaid recommends that §1033(b) be expressly stated to exclude: (i) the data fields required to be provided under §III.C.1.(i)-(vi); (ii) any other data or information that a consumer could use to obtain a product or service from an entity other than the covered data provider; or (iii) any other data or information that would allow a consumer to better evaluate the consumer's use of a consumer financial product or service from the covered data provider. Plaid believes that the Bureau's proposed definition of "for the purpose of," as well as the clarifying exclusions proposed by Plaid, will prevent the adverse consumer outcomes described in our Appendix A.

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?

We agree with the Bureau's proposed interpretation of "information required to be kept confidential by any other provision of law" to 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." In its Proposal, the Bureau indicates that "information that the covered data provider must keep confidential from persons other than the consumer, but not keep confidential from the consumer themself, would not be subject to the exception." The Bureau should clarify that the definition of "consumer" should include authorized third parties, so that the consumer's use of an authorized third party to access their data does not become a ground for withholding under §1033(b).

The following are examples of the sorts of legal requirements that should inform the Bureau's considerations regarding which information data providers should be required to keep confidential from consumers. This list not intended to be comprehensive:

1. Confidential supervisory information, under 12 CFR § 261.2.b.1

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

2. Confidential regulatory information, under 12 CFR § 1271.15
3. Legal subpoenas for confidential regulatory information under 12 CFR § 1271.21.b

Q36. What specific "other law(s)" should the CFPB be aware of when interpreting "kept confidential"?

We do not believe there are other laws the Bureau should be aware of when interpreting "kept confidential" beyond those included in our response to Q35.

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?

As a principle, the Bureau should require parity and equal access between "direct access" and "third-party access," as the terms are defined in the Proposal, because many digital financial services will work more effectively – and often only – with consumer-permissioned access for a third party. As discussed in our response to Q30, the Bureau should be cognizant of data providers' capabilities to alter their systems in order to constrain access to consumer data. The Bureau should strongly protect consumers against such harmful actions by enumerating the broad categories of information available to the consumer or authorized third party, including as outlined in §III.C.1.(i)-(vi). The Bureau should consider a range of interventions to prevent such harmful activities, such as those outlined in our response to Q4.

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."

The Bureau's definition of "current" provides adequate requirements for data providers to disclose up-to-date information.[37] However, in the interest of ensuring consumers have full access to pending information, the Bureau should clarify that "current" includes not only period statement data and pending transactions, but also posted transactions that are not yet included on a statement. Consumers expect real-time information and are used to seeing both posted and pending transactions in their mobile and online financial account management portals. There should be no temporal distinction between directly- and authorized third-party-accessed information from either a historical or a current perspective.

To ensure consumers have consistent access to their information, availability requirements should apply to current data. This means data providers should not be able to limit the times at which consumers can access or have authorized third parties access their information. Certain data providers today restrict Plaid's ability to gather consumers' information during the daytime, which leads to consumers obtaining outdated information. Such restrictions result in consumer

[37] "[T]he most current information that the covered data provider has in its control or possession at the time of a request for current information."

harm and an uneven playing field where authorized third parties are consistently unable to provide the same consumer information as data providers.

From an availability perspective, the Bureau may need to account for short technical lags between a consumer taking an action and that information being available. While near-immediate availability should be the requirement, similar to other availability requirements, if access to a consumer's information is delayed more than six hours (the typical time between data requests to update third parties), an authorized third party should be able to fallback to screen scraping in order to ensure timeliness of data.[38]

The Bureau's definition of "historical" is generally appropriate, since data providers should not be expected to gather information beyond what their consumer has generated over the course of their relationship with the data provider (see our response to Q24 for details on historical transaction information currently shared). However, the Bureau should not define scope of historical data according to what is included in an online financial account management portal, since that may introduce perverse incentives for data providers to remove historical information from their online financial account management portals (see our response to Q30 for details on data providers' ability and incentives to alter systems to avoid data sharing).

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?

Plaid does not have complete visibility into whether data providers currently charge consumers specific fees to access information directly. From a cursory scan of major financial institutions, consumers are able to obtain digital copies of their information both via online financial account management portals and in downloadable machine-readable formats without a fee.[39] Some data providers may introduce fees for shipping physical documents, but presumably those charges are for costs of printing and delivery, not for the information itself.

The Bureau should restrict covered data providers from charging specific fees for direct and authorized third-party access. Such a restriction would achieve the Bureau's desired result of lowering costs of access for consumers, lowering barriers to consumer switching and comparison, and increasing market competition to serve consumers on a level playing field. As discussed in our response to Q22, today, millions of consumers already access and share information without a fee. The Bureau should expect that, absent a prohibition, data providers might seek in the future to charge consumers for access to their information, thereby raising costs and harming competition and innovation.

[38] As discussed throughout, screen scraping can be tokenized, eliminating the need for consumers to share their credentials.
[39] See, e.g., Account Statement FAQs. Bank of America. Accessed January 5, 2023. https://www.bankofamerica.com/deposits/account-statements-faqs/

The Bureau should also restrict data providers from charging authorized third parties for access to information, under the principle that consumers should have equivalent direct and third-party access, as discussed in our Executive Summary. Third parties who are authorized by the consumer to access the consumer's information are doing so on behalf of the consumer. If the data provider were to charge the authorized third party and not the consumer themself, those costs would inevitably fall to the consumer and result in reduced competition by increasing the price of competing products. Choosing a service that can only work with digital access to data should not burden the consumer with additional cost.

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.

Plaid is not privy to the policies and procedures that covered data providers have in place to ensure the accuracy of information made available through their online financial account management portals. The Bureau should require policies and procedures to ensure information 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. Those policies and procedures should be applied equally to both the portals through which consumers directly access their data and the third-party access portals made available to authorized third parties.

Q45. Through what channels other than an online financial account management portal do covered data providers make information available electronically to consumers?

Covered data providers make information available electronically to consumers via dedicated mobile applications, web pages, and links to statement downloads, which typically produce .pdf or .doc documents for printing or mailing, or .xls files for further analysis in spreadsheets. Most data providers allow consumers to "go paperless," and receive information electronically via email. Some data providers also make information available via dedicated consumer interfaces designed to show historical trends.

Q46. How do covered data providers authenticate a consumer's identity when making information available other than through an online financial account management portal?

Covered data providers have myriad ways of authenticating a consumer's identity. These may include:

- Credentials (such as username/password);
- Multifactor (such as biometrics, one time passcodes, security questions, e.g. mother's maiden name);
- Personal identification numbers (PINs) (such as CVV for credit transactions or ATM PINs

for cash withdrawals); and/or
- Secure token confirmation (through cookies or other exchanges)

Each data provider may institute a different method (or combination of methods) to authenticate users. Plaid is not immediately aware if any of these methods are in use to offer information outside of an online financial account management portal, but instead offers them as illustrative examples of digital authentication.

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?

The Bureau's proposal would effectively provide consumers the protections and benefits of authorized access and mitigate risks to data providers. Availability requirements ensure consistent experiences for consumers and prevent anticompetitive behavior by data providers (see our response to Q59). Establishing a general framework under which industry-set technical standards can further develop would appropriately balance the need for regulation with the pace of innovation and consumer expectations in this system (see our response to Q57).

To protect consumers' rights to reliable and consistent access, the Bureau should address three outstanding issues pertaining to third-party access portals:

1. Prevent data access agreements from being used to disrupt access

In the proposal, the Bureau describes non-screen scraping access as "a portal based on a data-sharing agreement." We believe such contracting should not be a necessary precondition for an authorized third party to access a data provider's third-party access portal, for two reasons:

1. Data access agreements (or data-sharing agreements) were developed in the absence of regulation defining roles and responsibilities, and because of ambiguity about, for example, overlapping regulatory obligations or regulatory guidance that was not designed for or lacked clear applicability to a system where the consumer has control over their own data. Many of the issues discussed in the Proposal – including the impact of overlapping regulations, coverage of data providers, scope of available data, availability requirements, obligations on third parties, disclosure, authorization and consent – would address topics that have otherwise been the subject of negotiation in data-sharing agreements. In the past, Plaid has had difficulty negotiating consistent consumer access rights across data providers (see our response to Q143) and thus strongly endorses the Bureau clarifying the legal mandate for data providers to provide consumer access, including through authorized third parties. With a §1033 rule, consistent oversight and enforcement, and the Bureau's use of other tools, such as its Consumer Response program, guidance,

and consumer education efforts, substantial portions of the topics negotiated in data access agreements will be covered under regulation, eliminating the need for their inclusion in bilateral contracts.

2. Third parties already have active data access with certain data providers that does not involve a data-sharing agreement. Certain data providers have built third-party access portals that are open and accessible to third parties who register with their portal. (See our response to Q148.)

The Bureau should aim to regulate the system in such a way that data providers and authorized third parties can interact without the need for bilateral contracts. Of course, businesses may also see additional benefits in bilateral contracts, so some may remain – particularly to the extent data providers and third parties seek to align on elements of the consumer experience beyond the regulatory requirements, to address coordination in light of their connected technologies, and coordinate handling of disputes and technology changes/availability. But the core items in today's data access agreements should be addressed in and superseded by the §1033 rule.

2. Maintain the outlined Proposal assigning responsibilities to specific parties

The outlined Proposal appropriately assigns roles and responsibilities based on consumers' best interests and entities' core business competencies. Data providers hold a consumer's information, but have no insight into or control over a consumer's choice of third-party data recipients, because that consumer chooses to engage with a third party outside of the context of their relationship with a data provider. Therefore data provider responsibilities should only extend as far as data availability, data accuracy, and portal security. Third parties seeking consumer authorization to access and use their data, should be responsible for managing authorization and abiding by certain obligations regarding collection, use, and retention. This balancing of responsibilities will ensure clarity for participants of all sizes.

3. Coordinate with prudential regulators to clarify that data providers' third party risk management responsibility covers only the authorized third party, and is specific to permissioned data access

The framework underlying §1033 — a *consumer* has the right to decide which company can *access* their own account data at their data provider — is a profound shift from the traditional third-party or vendor risk management worldview, where the *bank* decides who *it* will do business with and *send* consumer information to. Since the OCC's 2020 Interagency Third Party Risk Management Guidance,[40] which for the first time addressed the role of data aggregators, data providers and aggregators have navigated uncertainty around where bank providers' third party risk management obligations begin and end. While the 2020 Guidance helpfully clarified that screen scraping does not create a "business arrangement" between a bank and an

[40] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29." OCC, March 5, 2020. https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html.

aggregator, it left ambiguity about data sharing under a data access agreement. The 2020 Guidance indicated that a data access agreement creates an unusual "business arrangement" because "the bank typically is not receiving a direct service or financial benefit." In the absence of specificity about data providers' risk management obligations in connection with data sharing under §1033, there has been friction between the parties that interferes with consumer access. More specifically, data providers that wished to make consumers' data available to them through access agreements parties have been unsure how to balance access with third party monitoring obligations, and authorized third-party data aggregators have been required to provide repeated, overlapping, and inconsistent information to satisfy data providers' shifting beliefs about their own regulatory obligations. Some data providers have demanded information on Plaid's customers, including confidential business information that could be used in an anti-competitive manner.

If left unaddressed, the §1033 rule could exacerbate this problem. While the proposal correctly would require a data provider to allow a third party with proper authorization to access data, the unresolved questions resulting from the 2020 Guidance could suggest that data providers will be expected to extend their third party risk programs over thousands of different third-party data recipients, most of which have no relationship with the bank. The data providers' concern about this possible interpretation of the 2020 Guidance has led to significant effort by some data providers to control aspects of consumer data access and sharing, up to and including restricting third party use cases. Other data providers take the position that they have no responsibility once the data leaves their hands on its journey to the data recipient. The concomitant impact on consumer access and innovation is obvious – if data providers are worried about being held responsible for data sharing that they do not even want to take place, then they are likely to resist data sharing arrangements or even access altogether.

To resolve this tension, the Bureau should consult with the prudential regulators to update their third party risk management guidance to clarify four things:

1. In the context of §1033 data sharing, a data provider only has risk management obligations related to companies that directly manage authorization and directly collect data from third-party access portals.
2. These risk management obligations are distinct from other third party risk management obligations and are limited to the authorization and data collection processes. Data providers should not seek to control which entities the consumer chooses to share their data with, or how that data is used after it leaves the data provider. Those issues should be governed by the §1033 rule, and should be explicitly carved out from a data provider's responsibilities. This approach will reduce regulatory uncertainty for data providers and prevent the risk of anticompetitive limits on consumer data access.
3. When a data recipient relies on a third-party data aggregator to facilitate and manage consumer authorization and data access, the data provider does not have "fourth party" obligations with respect to the data recipient.
4. Finally, whatever standards the Bureau places on authorized third-party data recipients or data aggregators should be consistent across those entities. Oversight and

supervision of the data authorization management process, whether managed by third-party data recipients or data aggregators, would be appropriate given its centrality in the data access system. CFPB supervision of data recipients or data aggregators that manage authorization will ensure the protection of consumers and their data, more properly accomplish risk management specific to consumers sharing their financial information, and reduce unnecessary burden on data providers that do not have an interest in the consumer's use of other financial services providers.

Q51. Please provide input on how covered data providers' customers can share their account information with third parties today.

Data providers' customers have four mechanisms by which they share account information with third parties today:

1. **Manual**: Consumers can directly download account statements from publicly facing online financial account management portals and physically or electronically deliver those statements to a third party. Consumers can also manually enter account information like account and routing number into third parties' consumer interfaces, and verify account ownership by confirming micro-deposit amounts. These methods are useful in high-touch, low-frequency contexts like financial advising, but highly inefficient when a third party requires continuous access to consumer information, or when a consumer has time-sensitive needs. Micro-deposits take days to verify, so they are not a feasible option for consumers who need real-time access to their finances.

2. **Credentials-based screen scraping**: Consumers can provide their login credentials to a third party, and allow that third party to act on their behalf to access their information directly from a data provider's publicly facing online financial account management portals. Prior to data aggregators, consumers would share their passwords directly with third-party data recipients. Some data aggregators now obtain consent and collect user credentials on the consumer's behalf to reduce the number of parties required to obtain credentials in the ecosystem.

3. **Tokenized screen scraping**: Data providers can implement technology that allows consumers to exchange their credentials for an access token, which the third party then uses to log in to the online financial account management portal on the consumer's behalf and scrape data from the online financial account management portals. This model eliminates the need for third parties to collect consumer credentials, but requires data providers to deploy both an up-front and ongoing technology investment, and certain security configurations. This technological investment for tokenization is nontrivial, but less than developing a full API.

4. **Application programming interface ("API")**: APIs are dedicated technical infrastructure, referred to in the Proposal as "third-party access portals," that allow software systems to communicate with one another programmatically. More than 60% of

Plaid's traffic is on APIs due to our integrations with many of the largest financial institutions and digital banking infrastructure providers. APIs consist of two parts: (a) token exchange and (b) data sharing endpoints.

- **Token exchange** is software that enables consumers to enter their credentials on a data provider's website, and generates an access token for the relevant authorized third party.[41] Authorized third parties redirect consumers from their own domain to the data provider's domain, passing information to the data provider identifying themselves as an authorized entity. The data provider validates that request and displays a login experience to the consumer, who enters their credentials just as they would under direct access. Once their credentials are validated, the data provider generates a token for the authorized third party and redirects the consumer back to the third party's experience to complete the data sharing process. Authorized third parties then return with that token in order to access consumer-authorized information on the frequency and duration to which the consumer has authorized them.
- **Data sharing endpoints** are dedicated software that provide consumer data to an authorized third party upon receiving third party permission to access and share. Endpoints can be scoped to certain data elements, or can surface a broader set of information. Within the FDX standard, for example, endpoints are scoped to reflect data categories similar to those outlined in the Proposal (transactions, identity, account information).[42] Some risk exists in scoping data sharing endpoints, since as discussed in our response to Q12 data providers do not have full detail on the use cases or data elements required by every authorized third party and might therefore mis-scope their endpoints resulting in over- or under-sharing of data. To require data providers to constantly update their data sharing endpoints to reflect consumer demands would be to significantly increase the investments required in data sharing.

Data providers' third-party access infrastructure should be responsive to the consumer rights enumerated in the final §1033 rule, and not determinative of those rights. Industry data standards, like the FDX API specification, are a powerful way for data providers to quickly and consistently provide consumers with access to their data – but only if that standard, which was developed before the §1033 rule was promulgated, is updated to match the rule's requirements once it is finalized. The same is true for data providers' existing proprietary APIs and other methods of providing access.

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

[41] OAuth is the industry standard model for token exchange: Hardt, D. "The OAuth 2.0 Authorization Framework." IETF, October 2012. https://www.ietf.org/rfc/rfc6749.txt.
[42] FDX API v5.2 Specification

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?

Yes, the Bureau should require that data providers make information available to authorized third parties before they establish a third-party access portal. We recognize the Bureau is concerned that screen scraping presents some limitations and risks to consumers, data providers, and third parties, including risks related to possession of a consumer's credentials. These security risks can be managed, and any other outcome would result in consumer harm, as data providers could effectively cut off consumers from their existing use of third party financial products and services on which they rely. Tens of millions of consumers would be vulnerable to financial disruption, particularly customers of smaller data providers, which are more likely not to have existing third-party access portals.

Such a requirement would necessitate that covered data providers continue to allow authorized third parties to engage in screen scraping, which is already the status quo in these instances. If this approach is adopted, authorized third parties should be held to the rule's privacy and security standards before the data provider's third-party access portal is complete, to ensure that screen scraping-based access does not result in unintended security risk or consumer harm.

There are no 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. As described in our response to Q51, tokenized screen scraping is a method of screen scraping that eliminates the need for consumers to share their login credentials with any third party. But, any other technology for making the data itself available, such as sharing spreadsheets or .pdfs of information, would introduce substantial latency and disruption to authorized third party business models and consumer experiences.

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?

Based on Plaid's experience engaging with data providers of various sizes, we recommend the following classification:

- Class 1: CFPB-supervised data providers
- Class 2: Non-CFPB supervised data providers that rely on core providers/digital banking

infrastructure providers[43]
- Class 3: Non-CFPB supervised data providers that do not rely on core providers/digital banking infrastructure providers

This classification reflects our understanding of how well equipped entities would be to meet certain timelines. Large data providers are best-equipped, followed by those relying on core providers, followed by those that build their own infrastructure. See our response to Q121 for details on how long our implementations with data providers typically take.

A tiered implementation for third-party access portals should not delay applicability of the data sharing mandate, as data providers may comply with the rule by permitting screen scraping before they establish a third-party access portal. That expectation should carry across all data providers.

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?

Please see our response to Q121 for details on our experience with implementation timelines for dedicated third-party access portals, which involves not only technical building, but also a migration of existing connections from screen scraping to token-based access. Plaid believes the Bureau should set reasonable timelines that account for differences in data providers' capabilities (see our response to Q53 for details on classes of data providers, based on our experience). As discussed in our response to Q52, the Bureau should protect consumers' data rights during any transition timeline by allowing authorized third parties to continue to utilize screen scraping to provide consumers' access to their data.

These responses would not 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 prior to establishing 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?

[43] Core banking providers provide platformed services primarily to small financial institutions to enable them to leverage technology and automation available at scale.

We strongly support an effort to proliferate third-party access portals universally, such that screen scraping in general is no longer a requirement in this ecosystem. In those cases where data providers' third-party access portals experience downtime, degradation, or interruption, we believe, data providers should be required to permit screen scraping in order to persist consumer's data access rights. In industry parlance these instances are called "fallback," meaning they are only employed when all other services are down.

Service interruptions harm consumers by cutting off access to their data. Fallback screen scraping requirements should apply whether the consumer is initiating an authorization or an authorized third party is continuing to carry out its authorized access. Such fallback access should be explicitly temporary, so that the third party only collects credentials during the time when a data provider's third-party access portal is down, and is required to coordinate with the data provider to exchange those credentials for an access token (without further consumer action) and purge the credentials promptly after the third-party access portal is restored.[44]

Should third-party access portal be unavailable for any period of time, tokenized screen scraping is another acceptable fallback mechanism that eliminates reliance on credential sharing. Tokenized screen scraping requires that the data provider accept OAuth access tokens on their online banking sites. See our response to Q51 for details on tokenized screen scraping.

As described in our response to Q64, data providers should be required to maintain consistent, publicly available reporting on the availability of their third-party data access portals, which would provide records of a service interruption. This reporting should occur both on their own publicly available website where their customers can research service disruptions, and to third party recipients or aggregators that are accessing their third-party access portal and should see a confirmation or denial message when sending data requests. Service interruptions can be either planned or unanticipated (see Q59). For planned outages, data providers should be required to notify third parties in advance and minimize the amount of downtime to a reasonable amount in line with industry expectations. For unplanned outages, data providers should be required to provide near-immediate notifications to third parties.

There are not reasonable alternatives to screen scraping as a fallback option in instances in which a third-party access portal experiences 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

[44] Swapping an existing credential-based connection for a tokenized connection is a standard industry practice when a data provider initially deploys an API, and the process of swapping in tokens followed by a purge of third-party-held credentials is generally referred to as "migration." Plaid has purged tens of millions of credential pairs over the past three years as the largest banks have developed reliable APIs.

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.

As described in our response to Q51, tokenized screen scraping is possible and secure, so long as the data provider provides a standard authentication and token exchange flow, and modifies their financial account management portal to accept authorized third-party access tokens as an authentication method. Leveraging tokens for authentication in lieu of credentials eliminates risks associated with credentials-sharing. Additionally, if an aggregator serves as the authorization and data minimization manager, the risk of over-sharing is also mitigated as the aggregator uses filtering or data purging technologies to only collect and share the data that has been permissioned by the consumer, whether the data is accessed via screen scraping or via API. (See our responses to Q90 and Q109 for details on filtering data collected via screen scraping.)

The Bureau should establish a general principle that authorized third parties not retain consumer credentials for any period of time longer than is necessary to fulfill the consumers' primary use case, including reasonably necessary uses. (See our response to Q88 for details on "reasonably necessary"). In application, this principle would sufficiently provide privacy and security while maintaining consumer access. The Bureau should use guidance, rather than the rule itself, to enumerate use cases in which these policies may be implicated.

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?

The Bureau should regulate availability requirements, but leave technical standards to the market. Availability requirements, as described in §D.2.ii.a, prescribe requirements for the outputs of a third-party access portal: uptime; latency; response time; and error resolution. Technical standards, on the other hand, prescribe technical specifications for the mechanisms a data provider can use to produce those outputs. For example, an availability requirement might say "a third-party access portal should be operational 99.9% of the time," whereas a technical standard would say "use this technical specification to move this information from within your internal servers to these dedicated endpoints as part of your third-party access portal."

By regulating availability requirements and leaving technical standards to the market, the Bureau can establish uniform requirements that ensure consistent consumer rights, while maintaining flexibility for industry to meet those requirements and develop alongside innovation.

The maturity and suitability of existing technical standards make CFPB-defined technical

standards unnecessary. By leaving the development of technical standards to the market, the Bureau can ensure that consumer access, security, and privacy keep pace with innovation, as industry standards can move more swiftly to incorporate new technologies and use cases than prescriptive regulation. Instead of producing regulatory technical standards, the Bureau should regularly review standards bodies, their deliverables (issued standards), and the implementation of those standards to ensure they support consumer access to their own data, compliance with §1033 requirements, and a fair, transparent, and competitive marketplace.

Today the U.S. open banking industry convenes around a standard developed by FDX, an organization of data providers, recipients, and aggregators, collaboratively building technical standards (disclosure: Plaid is an FDX board member). Similar to our description of API-based access in our response to Q51, FDX's technical standards include both a token exchange and an endpoint specification, in addition to security and privacy requirements.

The FDX technical standards are currently being applied to many third-party access portals, supporting over forty-two million consumers in accessing and sharing information from their data provider accounts with other financial products and services they want to use.[45] FDX standards help ensure that data elements and other technical components are consistent for a data provider's third-party access portal, no matter which third-party data recipient or data aggregator is connecting to that portal. This helps reduce costs for smaller providers because they only need to build a single third-party access portal that can be used by all third-party data recipients and data aggregators.

What's included in the FDX technical standard

FDX's API specification includes all of the data elements outlined in the Proposal as well as additional categories and elements not presently included. The structure of the organization – in which data providers, data recipients, and data aggregators are all equally welcome to propose and contribute to updates and modifications – is such that when new use cases emerge participants can act quickly to add new data elements requirements. The Bureau should therefore view FDX as an appropriate body for the continued development of technical specifications pertaining to third-party access portals. (See our response to Q22.)

FDX also prescribes security architecture that satisfies the requirements in this Proposal, including secure message transport, third party registration, and tokenization of consumer credentials. Much of this architecture is adapted from other jurisdictions and reflects years of testing (e.g., the API specification incorporates Financial Grade API (FAPI), which is a security standard also used in UK and Australian data sharing contexts.[46])

[45] "Financial Data Exchange (FDX) Reports 42 Million Consumer Accounts on FDX API to Continue Driving Open Banking." Business Wire, October 31, 2022. https://www.businesswire.com/news/home/20221031005060/en/Financial-Data-Exchange-FDX-Reports-42-Million-Consumer-Accounts-on-FDX-API-to-Continue-Driving-Open-Banking.
[46] "FDX Security Specification Boosted with FAPI." Financial Data Exchange, November 11, 2021. https://www.financialdataexchange.org/FDX/FDX/News/Announcements/FDX_Security_Specification_Boosted_with_FAPI.aspx.

How to ensure industry data standards support consumer rights and competition

We recommend that the Bureau oversee industry standards along two vectors: compliance and anticompetitiveness. The Bureau can use its existing authorities, primarily 12 U.S.C. §5512(C)(1)-(4), to monitor the governance of technical standards bodies, review the standards and other products they produce, and publish reports on their standards' compliance with §1033 rules. The Bureau may also wish to use guidance to update data access expectations with which the output of standards bodies would need to conform.

- **Compliance**: Standards will need to reflect the §1033 rules regarding technical functions such as authorization, authentication, availability requirements, data elements, and portal security. The Bureau should review the FDX specification – as well as any other industry-created standards – for its conformance with the §1033 rule, to ensure data providers relying on the FDX standard remain in technical compliance.

- **Anticompetitiveness**: To mitigate the risk that standards could be used to favor certain market participants over others in a manner that harms competition and consumer choice, the Bureau should develop general language around governance of industry standards, which FDX and other groups could use to inform their actions and limit anticompetitive behavior. Finally, the Bureau should provide an anonymous mechanism by which participants can report anticompetitive behavior.

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?

The Bureau should very tightly scope the possible subjects for industry-led dispute resolution. In a highly competitive ecosystem of companies with substantially different resources, industry-led mechanisms for dispute resolution could be captured or abused by entities with greater means. For example, with the ability to broadly dispute every part of data access, a data provider could *de facto* restrict access to a competing authorized third party by disputing every aspect of every access attempt. This would result in substantial consumer and competitive harm.

Any issue relating to third-party access portal availability and completeness should be directly overseen by the Bureau. Similarly, any issues related to the authorization process, an authorized third party's certification statement or adherence to obligations concerning collection, use, and retention of the consumer's information should be subject to Bureau oversight (see our response to Q12 for details on authorization). If any party raises concerns related to those issues, they should be able to petition the Bureau for intervention or to use the information to inform its supervision and enforcement prioritization. (Consumers, of course, should be encouraged to use the Bureau's Consumer Response resource to raise issues as well.)

Data accuracy may be one area where industry-led dispute resolution can simplify oversight, by

setting out simple processes for auditing data trails.

In general, the Bureau should clarify the difference between standards development and dispute resolution, the former being well-suited to industry mechanisms, the latter dependent on clear §1033 regulation.

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?

Regulatory requirements for third party portal availability factors will set the bar for a high quality consumer experience and enforce data provider accountability to maintain performance parity between first party access and third-party access.

To incentivize performance, third-party access portal availability requirements – and data providers' success metrics in meeting those requirements – should be visible on data providers' public facing websites to consumers, third parties, and regulators. This would substantially increase transparency, as many data access agreements prohibit public disclosure of third-party access portal performance. Such reporting could be performed by the data provider themselves, authorized third parties, or, ideally, both.

Below we identify the importance of each availability requirement, and provide recommendations based on industry expectations. References here to FDX are distinct from technical standards and simply point to industry-accepted availability requirements. The Bureau should view these availability requirements as potentially useful in regulation since they establish the existing quality of consumers' access, but should not mandate the technical standards that might underpin these requirements.

Availability Requirement	Why it matters	Recommended requirement
Uptime	Uptime matters for both initial and recurring requests for information by an authorized third party to a third-party access portal. Downtime during both initial and recurring requests can lead to consumer harms described in our Appendix A and severe disruption to third parties' business models. If an authorized third party's initial request fails, then the consumer will not be able to access their	Data providers should be required to meet the same reliability standards for their third-party access portals as their online financial account management portals, since consumers should reasonably expect that their authorized third-party access is as reliable as their direct access. The Bureau may wish to consider a safe harbor that deems a data provider compliant if they maintain 99.9% uptime. As a point of reference, the FDX standard already includes an availability standard of

	data and may abandon their effort to use their selected financial services provider. If recurring requests fail, an authorized third party will be unable to access the consumer-authorized information, which will interfere with the consumer successfully receiving the financial service they already requested.	99.9%.[47]
Latency	Low latency is critical for user-present data requests because if the response to a request for the consumer's data is slow, the consumer may be discouraged and abandon their effort to use a financial services provider (other than their data provider).	Reasonable commercial expectations today are for latency to be between 0.2-0.5 seconds, which is also FDX's recommendation.[48] FDX's standards also provide a more detailed set of latency expectations, including latency requirements for both the token exchange as part of the initial request, and for recurring data requests. The Bureau may wish to consider incorporating these types of expectations into the rule.
System maintenance	System maintenance matters because authorized third parties need to account for service interruptions, and data providers need to have processes to ensure consumers do not lose access as a result of routine technical upkeep.	The Bureau should require that data providers notify authorized third parties in advance of scheduled downtime. With this advanced notice, third parties can prepare accordingly by informing their customers of expected downtime. Third parties should also be able to capture consumer authorization during planned downtime and later access the requested data from the provider once services are restored.
Error response	Error response refers to the data providers' procedures and timelines for responding to authorized third parties' notifications that something has gone wrong (either missing data, unexpected downtime, or a rejection of legitimate consumer access).	Data providers should follow industry standard error response expectations, so that authorized third parties can understand and work to resolve issues. FDX includes useful examples, such as "HTTP error codes 400 (Bad Request) and 401 (Invalid Request)."[49]
Access caps	Access caps are an arbitrary limit set by data providers on the number of times their third-party access portals will fulfill	Data providers should not be permitted to implement access caps, since those caps necessarily constrain consumer access and

[47] "Foundational Requirements for Data Providers." Financial Data Exchange, August 17, 2020. https://fdx.atlassian.net/wiki/spaces/FDX/pages/29655070/Foundational+Requirements+for+Data+Providers.
[48] Ibid.
[49] Ibid.

	authorized third parties' requests, usually within a 24 hour period, even though the data requested is otherwise available. These caps can harm consumers in two ways. First, a consumer trying to access their data at the end of the day may be blocked from doing so because "too many" other consumers have already requested access that day. Second, many consumers rely on ongoing access for use cases (like those involving budgeting or financial management), which third parties usually satisfy by batch-requesting data every 6 hours. With an arbitrary cap in place, authorized third parties must either stop allowing new consumers to authorize access or throttle batch data requests to every 12, 24, or even 48 hours in order to stay under the cap. Throttling substantially impairs data freshness and often breaks use cases dependent on up-to-date data, for example a budgeting app that warns a consumer before they overdraft.	override a consumer's authorization. The Bureau should permit data providers to implement solutions like universally scoped tokens, which can decrease the volume of requests they receive from authorized data aggregators. Such a solution, however, requires that data aggregators be allowed to send authorized data requests for all information to which a consumer has authorized from that data provider, including data that will ultimately be shared with multiple data recipients. These requests still require consumers to authorize to every use case basis, but when the data aggregator returns to the data provider with future authorized requests, they return with an authorized request that reflects that consumer's authorization to the data aggregator. [50] See Appendix E for visual details on this model.
Unplanned events	Unplanned events are when an unforeseen technical challenge prevents data access. These are similar to planned maintenance, in that the consumer loses access to their data, but by their very nature do not allow data providers to give advance notice to third parties so that they can plan for the disruption.	Data providers should be required to have a dedicated communication channel with third parties that can be used for notification and troubleshooting of unplanned events, and to promptly notify third parties of the event and expected timeline for resolution. This will enable third parties to accurately communicate with consumers on the nature and likely duration of an outage. As discussed in our response to Q55, in case of unplanned or extensive downtime, data providers should be required to allow fallback screen scraping.
Data Freshness[51]	Data freshness refers to how up-to-date is the information data providers make	The Bureau should apply the principle of parity across direct and authorized third-party access, as

[50] "Investing in Infrastructure: Supporting the True Size of Digital Finance." Plaid, March 14, 2021. https://assets.ctfassets.net/ss5kfr270og3/6roEKHgg2i3Tm1X7L6ibu6/3985709f12e549e4cb95c812afb99627/Plaid-Data_Access-Whitepaper.pdf.

[51] Data freshness is distinct from latency: latency pertains to the data provider's third-party access portal's response to an authorized third party's request; data freshness pertains to the information itself.

	available to authorized third parties. Consumers depend on data freshness to have the most accurate, up-to-date information about their finances, and third parties depend on data freshness to ensure the quality of their services. Data staleness is the opposite of data freshness, and describes the period of time that could pass between data's being up-to-date and its being collected by an authorized third party.	discussed in our executive summary – meaning, there should be zero latency between when information is available directly to consumers and when it is available via an third-party access portal. Certain mechanisms exist to support real-time data freshness, including "push requests," in which a data provider's third-party access portal pushes information to an authorized third party, as opposed to the authorized third party "pulling" information from that portal via a request. Push requests have the added benefit of reducing costs for data providers, as their third-party access portals will only be used when new data is available.

Q60. Should the CFPB articulate similar availability factors with respect to the online management account portal proposal described above in part III.D.1?

Yes. There should be no distinction in availability factors between authorized third-party and direct access, and we are supportive of the Bureau imposing minimum availability requirements for such access (see Q59). The underlying mechanism to retrieve information from the data provider's internal systems should be the same for both, so there is no technical difference that would justify the application of different factors. If the Bureau were to permit different availability requirements for, e.g., online financial account management portals and third-party access portals, then consumers might experience different levels of access depending not only on their data provider, but also on whether they were accessing data directly or through an authorized third party. Permitting a distinction in availability factors between authorized third-party- and direct- access would permit data providers to discriminate against authorized third-party access (and the market-competitive financial products and services reliant on such authorized access), thus enabling anticompetitive behavior and harming consumers, as well as small data recipients which depend on third-party authorized access to provide critical financial products and services to those consumers.

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?

We agree with the Bureau's three outlined mechanisms to ensure that third-party data access portals are reliably available and believe that a combination of those mechanisms will best serve consumers and their ability to access their data.

As discussed in our response to Q59, we believe that establishing performance standards related to the availability requirements will help to ensure reliable availability. With that said, 100% availability is not feasible for any technology, and a requirement for near-100% availability is a more workable approach to ensuring consumer access. (See our response to Q59.) As discussed in our response to Q65, data providers are familiar with technology performance standards and could establish policies and procedures to ensure reliable performance of their third-party access portals in line with the Bureau's consideration of whether to "requir[e] the establishment and maintenance of reasonable policies and procedures to ensure availability."

As the Bureau proposes, data providers should also be prohibited from engaging in conduct that would adversely affect the third-party portal availability factors. (See our response to Q66.)

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?

Regulation of third-party access portal availability needs to balance consumer protection and transparency with reasonable requirements for covered data providers. Because third-party access portal availability is a continuous need, the Bureau should rely on its complete set of tools to incentivize data providers to meet availability requirements.

At the highest level, the Bureau has the opportunity, through its rulemaking process, to issue broad regulatory availability requirements that (a) set minimum standards for covered data providers, and (b) require data providers to publish prescribed availability data at a regularly-defined cadence and in a reasonably-accessible location (as described in Q4). The §1033 rule should reflect the minimum standards with which data providers will need to comply, while leaving expansion of those minimum standards and more detailed guidance thereon to industry-led bodies, like FDX, and to the Bureau's own issuance of guidance and specifications. (See our responses to Q22, Q57, and Q59.)

The following tools can allow the Bureau to further define and enforce availability requirements, and to quickly adapt those standards as technology changes:

> (i) the publication by the Bureau of Supervisory Guidance, Circulars, Bulletins, and Supervisory Highlights detailing specific technology expectations, and remedies for non-compliance;
> (ii) Supervision and Examinations of covered data providers which are not meeting minimum standards;
> (iii) Education of consumers about their data access rights and actions they can take when they are not able to take advantage of their rights; and
> (iv) the publication of annual Consumer Response data about availability complaints.

This combination of approaches will ensure strong enforcement of consumers' data access rights, and will provide industry with sufficient guidance to ensure a nimble response to changing technology, regulatory, and consumer expectations.

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?

As discussed in our response to Q41, charging fees for access – either to a consumer directly or to an authorized third party – undermines a core principle of §1033 access rights. In the Bureau's 2020 Advanced Notice of Proposed Rulemaking, the Bureau made clear that the authorized third party is the consumer's "agent," taking on the role of the consumer in accessing their information. Thus, there should be no distinction between charging a consumer or an authorized third party for access to data directly or via a third-party access portal. Moreover, as a practical matter, many consumers will depend on authorized third parties to help them access their data so they can use the full range of innovative and newly available digital financial services and products available to them in the market.

Permitting data providers to charge fees for access to information through their third-party access portals could harm competition and consumers. Data providers could, for example, set access fees at a price that would make third-party business models unprofitable. Data providers could also charge variable rates depending on how threatening the prospective use case is to their own business model; for example, a lender charging a higher rate for interest rate information to prevent a consumer from sharing that information with a different credit provider.

If data providers are permitted to charge for access, authorized third parties will face new costs to build and deliver their products and services. These costs could create a new barrier to entry and raise the costs of their products for consumers, since third parties would incorporate the costs of data access into their pricing.

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.

Performance standards only hold value if they are measurable, accessible, and enforceable. Because they control the data sharing infrastructure, data providers already have access to performance standards data. The data should be available regularly to the Bureau, consumers, and authorized third parties, including on data providers' publicly facing websites, as outlined in our response to Q59. Costs for tracking and making the data available should *de minimis*,

costing in the low thousands of dollars.[52] Plaid does not have insight into the compliance costs data providers would face in reporting this information to regulators.

As discussed in our response to Q4, the Bureau should allow authorized third parties to report performance information about the data providers from which they access information, both as a means of identifying real time access issues, validating the data providers' reported performance standards, and of helping to inform the Bureau's §1033 compliance oversight.[53] If data providers and authorized third parties reported materially different performance data, that information could assist the Bureau's supervisory prioritization decisions.

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?

We do not believe there to be any disproportionate effects of availability requirements on small data providers, and authorized third-party data aggregators are well positioned to provide support to data providers, including small ones, in terms of their compliance with such requirements.

Small covered data providers have benefited significantly from technology advancements made in consumer-permissioned data sharing in the past five years.[54] These advancements have brought down the costs of building and maintaining infrastructure (like third-party access portals), and provide roadmaps for testing and continuous improvement of that infrastructure. Processes related to troubleshooting, availability monitoring, and resolving technical issues have also developed, as third parties have coordinated with small data providers to improve their access. Data aggregators in particular have processes to engage with data providers to manage issues and maintain communications related to third-party access portals.[55]

FDX provides a comprehensive API roadmap and a development portal data that providers can use for testing purposes. Aggregators in general are deeply experienced in supporting data providers with their third-party access portal construction and management. For data providers building to our Core Exchange specification, Plaid offers robust validation and continuous testing tools.[56] This means data providers can rely on data aggregators to report back to them availability and uptime, as part of their interactions.

---

[52] One API reporting company offers their services for $500/month (https://apimetrics.io/features/api-monitoring/)
[53] Today, some data providers contractually prohibit third parties from disclosing performance data on their APIs to regulators. The Bureau should consider prohibiting such restrictions.
[54] "Jack Henry Integrates with Finicity, Akoya and Plaid." Finextra, October 12, 2021. https://www.finextra.com/pressarticle/89707/jack-henry-integrates-with-finicity-akoya-and-plaid.
[55] For data providers that may not be positioned from a cost- or resourcing-perspective to build their own third-party access portals, Plaid has also developed an FDX-aligned toolkit called Core Exchange, which gives those data providers all the tools they need to build and manage their own third-party access portal. We have seen 48 data providers commit to build third-party access portals to this specification, including 9 digital banking platforms who are building Core Exchange on behalf of their 500+ institutions. Typically these small data providers have introduced live data traffic on their third-party access portal within three months. (See: https://plaid.com/data-connectivity-core-exchange/)
[56] Plaid's Core Exchange Documentation (https://plaid.github.io/core-exchange/)

Availability requirements like those outlined in this response are generally accepted best practice for any technology. Data providers of all sizes will have experience with availability requirements for their own user experiences and back-end infrastructure, and will make technology decisions that best suit their capabilities (for example, build in-house vs. outsource to a vendor).

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?

The Bureau should employ two of its three proposed approaches – policies and procedures, and prohibition on conduct that would adversely impact the accuracy of transmitted information – in order to ensure that covered data providers transmit consumer information accurately. It should not attempt to prescribe standards for data accuracy under §1033, because such an approach doesn't exist in other data accuracy regimes like FCRA, and could introduce unnecessarily conflicting accuracy regimes.

Consumers' financial data rights and competition in financial services both depend on consumers having access to accurate information. The consequences of a consumer, authorized third-party, or data recipient accessing and ingesting inaccurate information are potentially significant; the consumer may make important financial decisions based on inaccurate information, and the financial products and services they are seeking to use may not work or may provide incorrect advice, services, or information based on the original inaccuracies. In addition, authorized third parties and data recipients can only fairly compete with data providers and each other when they have accurate information (since their products and services are dependent on this).

Data providers should be required to employ reasonable policies and procedures for maintaining data accuracy both for direct and authorized third-party data access. Included in these procedures should be requirements that data providers inform authorized third parties of key updates to consumer's personal information, such as a change of address or phone number. This information falling out of sync can lead to consumer confusion and an inability to provide proper authorization disclosures, revocation, and deletion.

Finally, the Bureau's proposed prohibition "against data provider conduct that would adversely affect the transmission of accurate information" would help protect consumers, as well as competition promoted by consumers exercising their data access rights. Consumers expect their information to be accurate everywhere, and accuracy should not depend upon differences in competitive incentives as between a data provider maintaining its online financial account management portal (direct access) or its third-party access portal (third-party authorized access).

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?

The Bureau should consider requiring that covered entities have policies and procedures to always provide accurate information and methods for rapidly resolving inaccuracies if they occur. Data providers that are already FCRA compliant should be able to adapt pre-existing accuracy policies and procedures for §1033 compliance.

Accuracy standards could be difficult to assess, since only the data provider would have the source information against which to compare potential inaccuracies. Therefore the Bureau should require that data providers include in their policies and procedures a means by which to routinely assess the accuracy of their third-party access portals against their consumer-facing direct access portals. This would properly ensure parity across those channels.

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?

The Bureau is correct to consider not proposing new or additional data security standards with respect to covered data providers' third-party access portals. The GLBA Safeguards Rule is a sufficient requirement for third-party access portal security, and so those security standards should be directly adopted. See our response to Q1 for more detail on our perspective on GLBA potential overlap with §1033.

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?

There are two types of authentication in consumer-permissioned data sharing: (a) consumer authentication and (b) authorized third-party authentication.

Consumer authentication is where a company verifies that the consumer seeking to authorize access to their information is the same person who controls the associated account.[57] In consumer-permissioned data sharing, when a consumer initially authorizes a third party, the data provider authenticates the consumer's credentials and generates an access token for the authorized third party. This access token becomes the tool the authorized third party uses,

[57] In general, both data providers and third parties conduct consumer authentication – data providers when consumers initially seek to authorize access to their accounts, and third parties when consumers first sign up for their services (e.g., signing up for an application that uses consumer-permissioned data) and later when those consumers return to use those services.

alongside its own identifier (a string of code given by the data provider to the authorized third party during registration that is used for future identification - see our response to Q80 and Q81 for more details), to authenticate itself to the data provider and access the data on the consumer's behalf.

> **Methods for consumer authentication:** For initial consumer authentication, where the data provider's third-party access portal needs to issue an authorized third party an access token, the industry has aligned around OAuth as the primary method for authentication. OAuth is a global standard in which a third party redirects a consumer to the data provider's domain, where the data provider authenticates the consumer. This authentication can happen using credentials, biometrics, device identification, or otherwise. Once authenticated, the data provider issues an access and a refresh token to the authorized third party, which the third party uses on subsequent data requests. Third parties can authenticate their consumers by similar methods outlined in response to Q46.

Third-party authentication is a computer-to-computer communication where authorized third parties identify themselves in their access requests to the data provider. This involves an authorized third party using some designated identifier to identify itself to the data provider so that the data provider can authenticate that the authorized third party should receive access to the consumer's information. Third-party authentication happens both on initial and recurring access requests.

> **Methods for third-party authentication:** Three primary methods exist for authenticating authorized third party requests.
>
> 1. **Allowlisting Internet Protocol (IP) addresses**: With screen scraping, an authorized third party can provide IP addresses to the data provider, which allows the data provider to set up its servers to identify and permit access requests coming from that authorized third party. Identified IP addresses are authenticated; non-identified IP addresses are not.
> 2. **Access token with a unique identifier**: When a third party registers with a data provider's third-party access portal (see our response to Q81 for details on pre-registration), that data provider issues a unique identifier to the third party. The third party includes that unique identifier in every successive authorized access request, including both initial and recurring requests, allowing the data provider to authenticate the legitimacy of that request as from a known entity. This is possible under both tokenized screen scraping and API-based access.
> 3. **API Keys**: When a third party registers with a data provider's third party portal, the data provider can issue API keys to that third party. API keys function similarly to user credentials that the authorized third party would use upon both initial and recurring requests. This is only possible with an API.

The Bureau is right to focus authentication on the authorized third party because the consumer

should not be required to re-authenticate every time the same authorized third party, acting at the consumer's direction, requests access to their data. This would result in superfluous authentication requests severely disrupting consumers' financial experiences. For example, if a consumer authorizes a third party to collect their transactions information every day in order to track expenses, then that consumer should not need to re-authenticate themselves for every recurring authorized third-party access request.

The Bureau should implement availability requirements related to both consumer authentication and third-party authentication. Consumer authentication, as discussed in our response to Q61, is a critical experience that should not be disrupted. Third-party authentication is a critical feature of availability – if a data provider cannot effectively authenticate legitimate third party requests, then its access portal is rendered essentially useless. Both should have uptime requirements. These availability requirements should be available to consumers and included in regulatory reporting.

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?

When accounting for GLBA coverage (see our response to Q1), the Proposal effectively addresses all relevant security requirements for data providers' third-party access portals. Fraud monitoring requirements should be borne by both data providers and authorized third parties, which should have common reporting standards to each other in case either one notices suspicious activity on their surfaces. The Bureau should lay out, in guidance, that data providers and authorized third parties should report suspicious activity to each other, but leave to the industry specifics for how those reports are generated and handled.

The Bureau should be conscious of attempts by data providers to interfere with consumers' ability to access their data via authorized third parties by claiming security concerns. The Bureau should clearly articulate instances in which a data provider can impose heightened access restrictions with respect to their third-party access portal and place the burden of proof on the data provider to demonstrate why such restrictions are necessary for security purposes. The data provider should be required to inform an authorized third party if it notices suspicious activity potentially stemming from that third party, and the third party should have the opportunity to explain or rectify the issue (to the extent within the third party's control) before the data provider can restrict access.

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?

The Bureau should make clear that data providers' third-party access portals can refuse requests from third parties that do not satisfy the conditions of presenting (i) authority to access information, (ii) information sufficient to identify the scope of information, and (iii) information sufficient to identify their identity. This would effectively – and programmatically, to the extent these access portals are programmed to reject such requests – prevent third parties that do not satisfy those conditions from obtaining information. However, such a clarification should in no instances outweigh the data provider's obligation to provide access to legitimately authorized third parties. Meaning, data providers should have very narrow justifications for refusing access requests (specifically, the absence of any of the required information from an authorized third party), and should be required to inform the authorized third party and the consumer of the reason for the refusal (see our response to Q85).

The Bureau's list of conditions is comprehensive, and provides sufficient information for a data provider to provide an authorized third party access to their third party portal. There are no 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. There are no circumstances in which third parties should be permitted to access information even if they do not satisfy the conditions the CFPB is considering proposing.

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?

We agree with the Bureau's recommendation that the authorized third party provide evidence of its obtaining consumer permission to access their data prior to receiving consumer information from a data provider, but note that the authorized third party may need to collect basic account information to provide a complete authorization experience that also addresses the scope of permissioned access. Authorized third parties should be able to programmatically provide evidence of their authorization disclosure and consent capture in the immediate context of making the request to the third-party access portal. Technical standards, including FDX, exist to normalize the mechanisms and descriptions authorized third parties can include in their requests to third-party access portals, which will minimize costs of compliance and verification for data providers. As discussed in our response to Q80, authorized third parties should also provide evidence of their registration with the data provider's third-party access portal, in order to authenticate themselves as legitimate requestors.

The Bureau might explore alternatives in very narrowly scoped cases, but primarily should establish that authorized third parties be obligated to provide this evidence. As outlined in our

response to Q12, there would be significant risk to consumer data access and competition if the Bureau allows data providers to seek duplicative evidence of authorization for every data request. Adding an extra layer of review would not reduce costs for providers as the proposed outline claims in §D.2.iii.a. In fact, it would have the opposite effect of increasing costs on data providers, which would need to write and maintain new processes to carry out this review.

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.

Consumers may seek to revoke their access through their data provider, data recipient, or third party aggregator, and the Bureau should not limit those options. Currently, some data providers limit authorized third parties from providing revocation functionality, a practice the Bureau should prohibit in the interest of consumer control of their data. There are two additional principles that the Bureau should incorporate into the rule in order to support consumers' choices:

1. The entity receiving the consumer's authorization revocation must be required to inform other relevant ecosystem participants promptly of that revocation.
    a. Data Aggregator: Some data aggregators offer revocation experiences – Plaid Portal is our version. When a consumer uses a data aggregator's revocation experience to revoke access to a given data recipient's access, that aggregator should share that revocation request with both the data provider and data recipient so both have records of that termination.
    b. Data Recipient: If a consumer were to instruct the data recipient to stop accessing the consumer's financial information, and the data recipient relies on an authorized third party aggregator for authorization, then the data recipient will need to inform the aggregator of the revocation request. The aggregator would be responsible for relaying the revocation record to the data provider.
    c. Data Provider: Data providers may choose to offer their own revocation functionality. If a consumer instructs the data provider to revoke access to a given data recipient, then the data provider needs to inform the data recipient of that revocation, as well as any authorized third party providing authorization.
2. A data provider may not take evidence that a consumer revoked access from one third-party data recipient as evidence that the consumer has revoked access from other authorized third-parties.

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?

A covered data provider should be required to notify a consumer of a third party's initial access attempt. However, a data provider should not be permitted to confirm with the consumer the authorization of a particular third party prior to making information available. To ensure clarity between these two concepts, the Bureau should distinguish between *informing* a consumer and *confirming* with them. Informing, such as by sending an email, supports consumer transparency. Confirming, such as by introducing additional details or disclosures or required actions during the authorization experience, could introduce the downside risks discussed in our response to Q12 (including confusion, duplicative authorizations, and anticompetitive disclosures).

For reasons laid out in our response to Q12, the authorization experience should be singular to ensure consumers make a single set of informed decisions. If a data provider interjects itself into the third party's authorization experience, then a consumer may be confused by the data provider's additional disclosures or questions (as discussed in Q12), which may lead the consumer to make misinformed decisions or to abandon their efforts to use the data recipient's product or service altogether.

Data providers also should not be permitted to inform consumers of their data sharing choices in a manner designed to intentionally disrupt the consumer's authorization. Data providers should be allowed to share this information in general statements, paired with a statement on consumers' data access rights, as described in our response to Q87. For example, some data providers make it possible for their consumers to easily see recurring payments or connections to data recipient applications through their financial account management portal. Such features are useful for consumer comprehensibility. In the interest of promoting consumer transparency and control, data providers should be allowed to provide these permissions management experiences, but only insofar as they are consistent and synchronized with the authorized third party's revocation experiences.[58]

Since the Proposal places management of the authorization experience on third parties – and revocation is a part of that experience (i.e., the withdrawal of the previously-provided authorization) – the Bureau should explicitly provide that third parties may implement revocation and authorization management portals for consumers, and allow data providers to connect their authorization management portals to third party portals so that they remain synchronized.[59] Because consumers may seek to revoke authorization through their data provider, third-party data recipient, or third-party aggregator, a data provider should not be permitted to preclude an authorized third party from displaying its connections in the authorized third party's own revocation experience, as some do today.

[58] By "synchronized" we mean mirroring the exact status of the authorization at all locations. If both a data provider and an authorized third party provide an authorization management portal, then both of those portals should be required to provide real-time status of that authorization (e.g., "active, revoked"). This may require coordination: for example, if a consumer revokes their authorization at the data provider, then the authorized third party would need to be notified of that revocation immediately so that they can update their authorization management portal.

[59] Plaid has worked with data providers within FDX to build such solutions for synchronization, including the consent notifications framework RFC 0198, which provides a system by which data providers can immediately notify an authorized third party if a consumer has instructed the data provider to revoke their access, and vice versa.

Q76. Please provide input on the approach the CFPB is considering. Are there any alternative approaches the CFPB should consider?

We agree with the Bureau's Proposal that covered data providers generally 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. The Proposal properly assigns responsibilities for authorization to the authorized third party and for data access to the data provider. Under part III.E of the Proposal, the authorized third party itself – and not the data provider – is responsible for collection, use, storage, revocation, and deletion of the consumer's data. The data provider's responsibility should be to validate that the third party has legitimate consumer authorization for those activities, but should not be permitted to do more than verify that authorization was properly granted, and authenticate the authorized third party. For reasons outlined in our response to Q12, all other obligations for authorization disclosure should fall to the authorized third party.

As described in our response to Q12, with millions of consumers providing authorized access to thousands of third parties for hundreds of data elements, there is tremendous complexity in ensuring that third-party access properly reflects the consumer's authorization. This complexity will create significant risk if data providers attempt to determine the scope of every third-party authorization. There are also technology risks in requiring data providers to be responsible for dictating the scopes of information to be returned to an authorized third-party request. Specifically, if a data provider were required to scope their third-party access portal endpoints (the pieces of software that determine which types of data to return upon request) to each individual third-party use case, they may end up with thousands of endpoints customized to each of the thousands of use cases. This problem has been identified in FDX and has not been resolved despite years of technical efforts.

The best way to ensure that third parties abide by their consumer authorizations, and that data providers do not mis-scope data is to place all authorization obligations with the authorized third party and to exercise direct oversight, including through supervision, over the data providers and third party entities that handle consumer authorization and effectuate data access under this rule.

Duration and frequency of access should be determined by specific authorizations, as the Bureau proposes. As outlined in our response to Q12, the authorized third party, and not the data provider, knows what data elements, duration, and frequency of access is needed to power the consumer's desired use case (including information needed for reasonably necessary purposes or authorized secondary uses, as described in our response to Q88 and Q98). A data provider should not be permitted to interfere with the duration and frequency required by that authorization. Instead, duration should be governed by rules around revocation timelines, and frequency by availability requirements (see our response to Q59).

Small data providers stand to benefit when their obligations are limited to (a) verifying that

authorization was collected by the third party, and (b) authenticating the authorized third party. Any additional obligations introduce operational complexity and costs, as well as the other consumer risks discussed in Q12. Data providers' third-party access portals can both (a) verify that authorization was collected and (b) authenticate the authorized third party by programmatically reading access requests, which typically include these details according to industry standards. (See FDX RFC0156: Consent API for a detailed access request that includes all of the above information).

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?

Covered data providers should not be allowed to limit the frequency or duration of authorized third parties' access under screen scraping since this would adversely impact consumers. Duration and frequency should be set by authorized third parties who know these details as part of their delivering a use case to consumers, and should be authorized by the consumer alone.

Q79. Please provide input on the proposal the CFPB is considering. What alternative approaches should the CFPB consider?

We agree with the Bureau's Proposal that a covered data provider 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. However, the Bureau should clarify the meaning of "provided the information is covered by the rule." As discussed in our response to Q22, the Bureau should ensure the data categories covered under §1033 include those discussed in our response; this is necessary to ensure millions of consumers currently accessing data not expressly included in the Proposal will continue to have their financial data access rights protected and will continue to be able to use the financial products and services they rely on. At minimum, the Bureau should be explicit that the data categories enumerated in the rule are not intended to be exhaustive or to otherwise limit the full scope of potential applicability of §1033, and that a regulation issued pursuant to §1033 is not necessary for enforcement of the statutory mandate.

In addition, the Bureau asks whether a covered data provider should be permitted to seek to clarify with the consumer the scope of an authorized third party's access request where a covered data provider does not have enough information to know how to respond to the request. Plaid recommends that the Bureau narrowly define instances in which a data provider can seek to clarify the scope of an authorized party's request. Where an authorization includes all details outlined in the Proposal, such an authorization request should be deemed inherently sufficient, and the data provider should not be permitted to clarify the authorization.

Rather, data providers should only be able to clarify the scope of an authorized party's request when an authorization does not contain one or more of the three details described in the Proposal: general categories of information to be accessed, terms related to frequency and duration of access, and a method to revoke access. The Bureau should take into account two technical considerations if it adopts this approach. First, granular details around duration, frequency, and scope of data can be conveyed programmatically in an authorized third party's request to a data provider's third-party access portal. But proof that an authorized third party has presented a revocation method is only a binary yes or no (e.g., "has it been displayed or not"). To avoid a circumstance in which data providers see an obligation to manually review every third-party authorization disclosure to ensure a revocation method has been displayed, the Bureau should clarify that the data provider can accept a yes/no response programmatically included in the authorized third party's request. Second, per our recommendation for timing requirements around authorization disclosure in Q19, we believe that method to revoke should be presented after a consumer authorization and not before, since revocation only applies to existing authorizations. Therefore, the Bureau should also clarify that the yes/no response can refer to the authorized third party's subsequent disclosure.

Outside of these instances, permitting data providers to clarify otherwise valid authorization requests would not only add costs and inefficiencies for consumers, data providers, data recipients, and authorized third parties (including the possibility that consumers abandon their efforts to use a particular financial service or product), but would also introduce opportunities for data providers to impede data access in a way that harms competition. For example, a lender could seek clarification on every data access request for interest rates where a consumer is exploring credit products with a data recipient other than the lender. For the reasons outlined in our response to Q12, third parties are best positioned to manage authorization.

Finally, the Bureau mentions a possible circumstance 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." For reasons described above and in our response to Q12, the Bureau should also narrowly define this circumstance to include only those instances where the data provider itself has direct knowledge of the data elements required to serve the use case. This could occur in circumstances where, for example, the data provider and authorized third party have contracted to share this information.

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?

The Bureau is correct in identifying the need for data providers to authenticate the identity of the authorized third party. The mechanism by which that authentication takes place should involve a combination of pre-registration of the third parties set to receive consumer authorization, followed by backend authentication of that third party that would take place at the time of the

authorized request between the authorized third party and the data provider (see our response to Q70 for details on third-party authentication). The technologies required to pre-register and then authenticate authorized access requests to a third-party access portal are well-established and currently in use across thousands of providers (see our response to Q81 for details on pre-registration).

Pre-registration should only apply to the specific third parties making authorized requests directly to a data provider's third-party access portal, since those are the only parties interacting with the data provider. In instances where a data recipient relies on a data aggregator for authorization, the data provider's pre-registration obligations should extend only as far as the data aggregator serving that authorization disclosure and not to the data recipient in such situations. A requirement to pre-register data recipients that rely on data aggregators would burden smaller data providers by introducing complexity and cost. For example, with larger financial institutions it took Plaid nearly four months to register our 7,000 data recipient customers, and we typically engage with at least two full-time staff at those data providers whose responsibility it is to manage the pre-registration process.

Data aggregators should themselves be required to conduct their own pre-registration with their data recipient customers, meaning they should secure their own APIs with the same pre-registration and authentication model as outlined here. Plaid takes this approach, and we understand it to be a best practice already employed today across the industry. This dual layer of security ensures that data recipients are authenticated when they make requests to the data aggregator, just as data aggregators are authenticated when they make requests to the data provider.

The Proposal outlined is comprehensive. There is no 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?

As referenced in our response to Q80, the best way for data providers to authenticate authorized third parties is by having those authorized third parties pre-register with the data provider's third-party access portal. While the Bureau should not prescribe specific procedures, they could prescribe specific types of information required for pre-registration, such as business name and point of contact. This information should be consistent, limited to identifying or security information, and should explicitly exclude sensitive business information such as use case, business purpose, or any commercial information not necessary for identification.

To facilitate compliance and reduce costs for data providers, the Bureau should clarify that data providers need only pre-register authorized third parties which (i) obtain authorization from one of the data provider's consumers, and (ii) are the same party that will send a request to their third-party access portal. Put another way, the data provider should not be responsible for registering any party that does not directly come into contact with their third-party access portal, since that would only introduce costs and not result in any additional security (there is no need to authenticate a third party that never sends a request).

Requiring that data providers only pre-register the authorized third parties directly contacting their third-party access portals would achieve two goals: (i) ensure that the data provider has sufficient information to authenticate every authorized request; and (ii) eliminate any unnecessary costs of pre-registering thousands of data recipients which do not themselves contact the third-party access portal.

For example, if the authorized third party is a data recipient, then that data recipient should pre-register with the data provider's third-party access portal before sending authorized requests. Similarly, if the authorized third party is a data aggregator, then that data aggregator should pre-register. However, in the case of the data aggregator, the data provider needs only to pre-register that aggregator to authenticate its requests, and has no need to pre-register any of the data recipients using that data aggregator since those data recipients will neither obtain consumer authorization nor send authorized requests to the data provider portal.

Several technology standards allow for rapid third-party registration with a data provider's third-party access portal, including FDX's dynamic client registration (RFC 0153) and delegated application registration (RFC 0206). The Bureau should also set reasonable timelines for pre-registration, so that data providers cannot intentionally delay pre-registration as a means of refusing to provide access. As referenced in our response to Q80, data providers today approach pre-registration with varying methods – some near-instantaneous, others taking weeks or months to manually approve a new registrant. Without clear guidelines or requirements for pre-registration, data providers' pre-registration processes could be wielded as an anti-competitive tool. Such an outcome would harm both consumers' ability to benefit from their chosen financial services, and also third-party business models.

Q82. Should covered data providers be required to make information available to third parties when they know the information requested is inaccurate?

Plaid does not have a position on whether or not data providers should be required to make information available to third parties when they know the information requested is inaccurate, but we believe the Bureau should be aware of certain risks as it weighs this consideration. First, as a matter of principle data within the data access ecosystem should be accurate, and if it is known to be inaccurate it must be flagged as such. Otherwise, as the Bureau's Proposal identifies, both third parties and consumers could face risks if they are dealing with information they do not know is inaccurate. Second, to the extent the Bureau defines "accuracy," it should also define the terms by which such accuracy can be determined.

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)?

While there may be instances when a consumer wishes to authorize sharing of information known to be inaccurate, e.g. to help the consumer handle a dispute about the data's inaccuracy, Plaid has not seen any evidence of this use case in practice.

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?

Yes, covered data providers should, in general, be required to provide disclosures to both third parties and consumers about why access is prevented. These disclosures would serve two purposes: (i) provide transparency to consumers and third parties so that they understand whether action can be taken to remedy access; and (ii) mitigate against over-reliance by data providers on §1033(b) exceptions (or other reasons why access is prevented) as a pretext to avoid making certain information available to consumers or authorized third parties. Please see Plaid's response to Q30-Q37 for details on the §1033(b) exceptions. At minimum, such disclosures should include the data being withheld and the specific reason such data is being withheld. The Bureau should require that such disclosures be in plain language and not be deceptive, misleading, or abusive.

Whether a disclosure should be provided to a consumer or a third party or both should be determined based on the reason access has been prevented. For example, if a data provider rejects an authorized access request because it believes it has not obtained sufficient information (see Q79), then it should relay that information both to the consumer and the third party. However, if a data provider rejects an authorized access request because of a technical issue specific to the authorized third party, then it should relay that information only to the third party, as it would have limited value to the consumer.

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.

We do not believe that policies and procedures alone will sufficiently protect against the use of §1033(b) exceptions or other reasons why access is prevented as a pretext to avoid making certain information available to consumers or authorized third parties. Requiring notification to the consumer and authorized third party at the time the access is denied, in line with our response to Q85, ensures that the authorized third party and consumer can assess whether and how access can be remedied.

Q87. Please provide input on whether and how covered data providers should inform consumers of rights afforded to them pursuant to the rule.

Data providers should be required to inform consumers of the data access rights afforded to them under the rule by posting publicly accessible information on their consumer interfaces (including websites and mobile applications) detailing the specific rights afforded them by §1033, including how to reach the Bureau's Consumer Response team in case of access restrictions and failures (see our response to Q4 for our suggestions for consumer redress). Information included in these disclosures should cover both direct and authorized third-party access, which should be presented on equal terms.

General data provider communications about consumer access, including notices described in our response to Q85, should also be required to be paired with a statement of consumer rights.

In addition to requiring data providers to disclose consumers' data access rights, the Bureau should also prohibit data providers from making deceptive, misleading, or abusive statements, including publishing information intended to dissuade consumers from exercising their statutory rights under §1033. Today, in the absence of such requirements and prohibitions, certain covered data providers publish consumer-facing information seemingly designed to discourage consumers from authorizing third-party access. By requiring covered data providers to provide complete and accurate information to consumers about their rights, including their right to authorize third parties to share their data, consumers will be better positioned to access the benefits afforded to them under §1033.

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

The Bureau's proposed "limitation standard" – which would limit authorized third parties' collection, use, and retention of consumer information to that which is "reasonably necessary" to provide the product or service the consumer has requested – recognizes that §1033 is focused on consumer choice, but omits many reasonable and expected uses of consumer data that are common and non-controversial across industry and are typically employed to run a safe and well-managed business. In addition, by excluding any potentially authorized secondary uses of data, the narrow definition may have the unintended effect of preventing consumers from controlling how they wish to share and use their data and reducing ecosystem security and fraud prevention, without addressing some of the concerns that may be behind the proposed "limitation standard."

Section 1033 was enacted to allow consumers to benefit from access to their own financial data by providing autonomy over its use – and portability for use – by different financial services

providers. The statute envisions a profound shift from bank- and business-centric decision making to consumer-centric decision making. Accordingly, decisions to limit consumer control, such as those contemplated in the limitation standard, should be narrowly focused on preventing specific and identifiable harms, and, given §1033's goal of increasing consumer choice, such decisions should also be as competitively neutral as possible.

Although not stated in the Proposal, we consider the possibility that the Bureau is concerned about authorized third parties using §1033 to amass data collections that – in and of themselves or because of non-consumer-friendly uses that do not directly provide the product or service requested by the consumer – pose consumer risk. We understand and share the Bureau's consumer protection concerns, as well as §1033's goal of shifting control to the consumer, and for that reason our business model is based on consumer permissioned data sharing. But, we also believe the "limitation standard" is too narrow and that secondary uses can be regulated in a manner that protects consumers.

The Proposal indicates that the proposed "limitation standard" is "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." Elsewhere in the Proposal, the Bureau addresses content and clarity of authorization disclosures and procedures, requirements for consent as to use cases and scope of authorized access, and data security expectations. Given that the Bureau can directly address over-collection/data minimization, retention of sensitive information, and risks of breach with the more targeted requirements already included in the Proposal that do not burden consumer choice, we request the Bureau explain with more particularity what harm it seeks to address by its narrow "reasonably necessary" standard. As explained below, Plaid recommends expanding that definition to include reasonable and expected uses that provide indirect consumer value and are compatible with the consumer's primary purpose, and using the authorization requirements, including opt-in and opt-out requirements, to regulate secondary uses of data.

The Proposal also references consistency with "various State and international privacy regimes." Many regimes, such as the European General Data Protection Regulation, ground their purpose limitation on compatibility with "specified" and "explicit" uses disclosed to the consumer, and allow further processing only with the consumer's consent.[60] Similarly, the Virginia Consumer Privacy Act requires consent for collecting and processing data and provides consumers with the right to opt out of many secondary uses that might not be compatible with the uses for which they shared their information.[61] The wisdom of these approaches is that they situate control with the consumers and use consent requirements and obligations on data recipients to limit expansive collection and use. If the Bureau's concern is that existing consent mechanisms are not adequate to protect consumers, then it would be useful to open a dialogue about how to fully empower consumers to maintain control over the use of their own data.

[60] "Principles of Data Protection." Data Protection Commission. Accessed January 24, 2023. https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection
[61] Code of Virginia. Title 59.1. Trade and Commerce. Chapter 53. "Consumer Data Protection Act"

Importantly, because the proposed “limitation standard” would be applicable only to consumers accessing their own data via authorized third parties, while data providers’ use of consumers’ data would be left unrestricted, a limit on permissible uses may interfere with innovation while bolstering anticompetitive advantages held by incumbent data providers. If the “limitation standard” were put in place as described, data providers would paradoxically be treated with more agency over consumers’ data than the consumers themselves. The disparity would be magnified when data providers also are data recipients and, because they are GLBA regulated, treat the consumer-permissioned data that they receive as if it were regulated only by the GLBA.

In sum, while we agree with the Bureau's aims of providing control and protection to consumers in terms of how their data is used, the proposed “limitation standard” (1) unnecessarily limits the consumer’s right, in light of the many other protections included in the Proposal, to make informed choices about how to permission access to and share their own data, and (2) creates a competitive advantage for data providers by giving them more rights over uses of consumer data than consumers are permitted to grant to their chosen financial providers. The Bureau should ensure that any use standards it determines to impose apply to all participants in the §1033 ecosystem, including to data providers.

Any use limitation standard should apply to all participants in the §1033 ecosystem, not just third parties

As the Bureau considers limiting the collection, use, and retention of consumer-authorized information by third parties to what is “reasonably necessary” to provide the requested product or service, it should avoid treating data accessed by the consumer, via an authorized third party, pursuant to §1033 differently than data collected and used by data providers under the GLBA. The GLBA focuses its privacy provisions on notice, consent, and permissible sharing of consumer information by financial institutions, and not on use limitations.

The Bureau should take care to ensure that the §1033 rule does not lead to unintended effects because the proposed limitation applies only to authorized third parties and not data providers. For example, it would harm consumers were the Bureau to permit an outcome whereby a data provider (unrestricted by the above Proposal and subject only to GLBA) could, by disclosing its actions, use consumer information for marketing, share that same information with its affiliates for marketing without any consumer consent, and sell that information to a non-affiliated company for marketing, but a consumer (restricted by the Proposal) could not make their own decision to share their data with an authorized third party for marketing or even for consumer-value-adding purposes such as network security, fraud prevention, authentication, or identity verification. Indeed, this situation already exists today, as some financial institutions that receive consumer-authorized data under §1033 treat it as governed only by GLBA (meaning there are no use limitations imposed), while trying to limit how other third parties can use the data accessed from a data provider by an authorized third party on behalf of a consumer under §1033.

In short, different standards under the GLBA and §1033 could mean that a consumer's exercise of their own data access rights under §1033 are more burdened than a financial institution's exercise of its rights under GLBA over the consumers' same data. It also could foster confusion among consumers, who would be best served by consistent standards across the financial services industry so they know what to expect. Finally, different standards could create competitive disadvantages between GLBA-covered financial institutions and institutions relying on consumer-permissioned data collected under §1033.

If the Bureau decides to impose data use limitations that differ from the limitations under the GLBA, then the Bureau should either (1) defer implementation of the §1033 limitations requirements until the rules promulgated pursuant to the GLBA are updated, or (2) make clear that the data use limitations promulgated pursuant to §1033 apply to all ecosystem participants, including data providers, data aggregators, and data recipients regardless of whether they are subject to the GLBA. With respect to the latter point, a consumer-centric approach requires that all participants in the §1033 ecosystem be subject to equivalent use limitations; consistent application of such standards recognizes that §1033 data belongs to the consumer and that the consumer should be empowered to make informed decisions with respect to their data – regardless of whether that data is held with a data provider or an authorized third party. The consistent application also prevents confusion in an increasingly common circumstance where a data provider is acting as both a data provider and an authorized third-party data recipient.

While we recognize that data providers have advocated to limit the uses to which third-party data recipients and aggregators can put consumer-permissioned data, and we strongly support certain transparency, consent requirements, and use limitations, some of their arguments to limit use do not come from the consumer-centric perspective of §1033, but rather from an attempt to safeguard perceived competitive advantages. As discussed below and in response to Q98, 100, 101, and 118, we believe that a consumer-centric view of transparency, consent requirements, and use limitations recognizes that there are reasonable and expected uses of consumer-permissioned data that should be considered reasonably necessary uses that the consumer authorizes because they are uses of consumer data that are common and non-controversial across industry and are typically employed to run a safe and well managed business. There are also secondary uses that provide consumer value and are compatible with the consumer's primary purpose but, in light of the consumer's strong interest in transparency, should only be used with notice and an opportunity for the consumer to opt out. There are other secondary uses – such as use of personally identifiable information for marketing or advertising of products to consumers that do not have a direct relationship to the provider (see our response to Q98 for more details) – that should only be used with notice and an opportunity for a consumer to opt in.

While the above points are important considerations for fully realizing the promise of §1033 as a method of shifting power from businesses to consumers, and creating a transparent, fair, and competitive financial services marketplace, we nevertheless believe the Bureau's outlined approach broadly addresses the important consumer privacy issues – so long as (1) use

limitations are imposed uniformly and (2) certain adjustments to the Bureau's definitions of "reasonably necessary" and "secondary" uses are made, as outlined below and in Q98.

The definition of "reasonably necessary" should be expanded

As it considers whether and how to limit collection, use, and retention of consumer-permissioned information, we recommend certain adjustments to the proposed definition of information "reasonably necessary to provide a product or service." These recommended adjustments would ensure the definition captures the information needed for the requested product or service, as well as information needed by authorized third parties for reasonable and expected uses that should not be considered secondary uses because they are common and non-controversial across industry and are typically employed to run a safe and well managed business. To be clear, without such expansion the current definition could lead to consumer harm by impeding authorized third parties' ability to enhance their security or troubleshooting systems, which are core to consumer safety.

The proposed definition of "reasonably necessary" should expand beyond that necessary "to provide a product or service" to include:

> (i) the information needed to power the use case;
>
> (ii) information needed to support an entity acting on a consumer's authorization, revocation, or deletion request (see our response to Q117 for details on why authorized third parties need to collect personal information in order to manage authorization, deletion, and revocation requests); or
>
> (iii) information needed for additional reasonable and expected uses that are neither primary nor secondary uses of data, including the following:
>
> a. fulfilling legal obligations;
> b. preventing, detecting, or investigating fraud or security threats against any related party (data recipient, provider, or aggregator);
> c. protecting third party rights and property;
> d. protecting others in the ecosystem from harm;
> e. supporting risk management;
> f. troubleshooting; or
> g. improving the same product or the consumer experience for which the consumer's information was originally collected.

This definition – and any use limitations more generally – should apply to all 1033 ecosystem participants, not just third parties. Consumer authorization for both reasonably necessary and secondary uses of their permissioned data should be governed by appropriate consent and data minimization requirements. (See also Q19 regarding disclosures). For additional perspectives on data retention, see our responses to questions 104, 105, 106, 119, and 147.

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.

Please see our response to Q88 regarding collections limitations. While we agree that certain types of data are of heightened sensitivity, we believe the collections limitations outlined sufficiently protect consumers across the board.

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?

Please see our response to Q88 regarding the proposed collection limitations. Subject to that response, we note that third parties can limit collection and retention of data in a screen scraping environment by filtering at the point of access or purging after access.

- **Filtering at the point of access:** When screen scraping, third parties write scripts to access specific fields from a data provider's online account management portal. Those scripts can be written specifically to the online account management portal's syntax, so that the third party will not collect any more information than what has been permissioned by a consumer.
- **Purging after collection:** Where filtering at the point of access is not possible, third parties routinely collect, filter, and purge unnecessary or non-permissioned data after it's been collected.

Third parties should be afforded flexibility to employ either option as a mechanism for achieving the goal of data minimization.

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?

The Bureau's Proposal for limiting duration and frequency of data access is reasonable and should fall into the same framework as overall collection – meaning, frequency and duration should serve only the reasonably necessary purposes (as defined in our response to Q88) and any authorized and permissible secondary uses for which the consumer has permissioned access. Given the complexity and range of authorized uses existing today (and likely to be developed in the future), restrictions on duration and frequency of data access require a principle-based framework rather than prescriptive requirements that attempt to identify rules for every authorized use. The Bureau should therefore establish a principle around duration and

frequency, instead of attempting to define limits for every use.

> **Duration.** Duration of access should be governed by the specific authorized use and should be described in the authorized third party's certification statement. For example, a tax use case might only need to collect data for one or two months as they gather information for tax filing purposes each spring, or a rates comparison use case might only access data once, but a personal financial management use case has its duration measured only by the continued value the consumer finds from its usage – which could stretch on for years. Disclosure during authorization makes it possible for the consumer to understand what they are permissioning and sets a clear standard upon which to oversee compliance.
>
> **Frequency.** Frequency of access also should be governed by the consumer's authorization. Critically, frequency should always be of service to consumers' authorized uses; there should be no regulatory or technical override of consumers' authorizations (for examples of technical justifications being given for limiting authorized third-party access frequency, see our response to Q143). Frequency should instead be of service to availability requirements, including data freshness as discussed in our response to Q59.

The best way for a data provider to minimize costs while enabling consumers' data access rights is to avoid duplicative access requests. As described in our response to Q59 in the context of access caps, a data aggregator, for example, may be authorized by the same consumer to access the same data from the same data provider for multiple third-party data recipients. Data providers stand to benefit from reduced traffic where data aggregators can rely on one access request to serve multiple use cases, instead of multiple redundant access requests, while consumers retain the same protections under separate authorizations provided to that aggregator. (See Appendix E for visual depiction of a data aggregator serving multiple data recipients with a single request to a data provider's third-party access portal).

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.

As it considers reauthorization mechanisms, the Bureau should note that today reauthorization is frequently employed as a tactic to disrupt consumers' sharing their financial data, as has been pointed out by Georgetown Law Professor Adam Levitin: "Large financial institutions have imposed onerous user reauthorization requirements and regularly interrupted third-party connections, leading to long periods of downtime or brownouts that undermine service reliability."[62] The Bureau's proposal for a maximum data access duration also raises concerns in light of the adverse impact felt in the United Kingdom when a reauthorization requirement was

[62] "Consumers — not banks — should control access to personal financial data" Adam J. Levitin, The Hill https://thehill.com/opinion/finance/561645-consumers-not-banks-should-control-access-to-personal-financial-data/

set for 90-days, which was too short for many authorized uses and not otherwise tied to those particular authorized uses (some of which, by their very nature, required durations of longer than 90 days).[63] Instead of prescribing either a fixed duration for each authorized use or a maximal duration period for all uses, the Bureau should prescribe a principles-based framework that applies across all uses. The framework should be tied to:

- **Consumer control:** Consumers should be permitted, at their convenience and desire (and as reasonable), to instruct third parties to extend authorization periods. For example, the Bureau should permit third parties to offer consumers the option of adjusting their authorization period to a time frame of their preference.

- **Consumer experience:** To avoid burdening consumers with reauthorization requests that would disrupt their financial lives, the Bureau should allow a consumer to reauthorize multiple uses at the same time. (See our response to Q144 for details on potential harms reauthorization could bring to third-party business models, which apply similarly to consumers.) This process works especially well where a consumer has authorized multiple uses with a single authorized third party, such as with a data aggregator or with a data recipient offering multiple services. In practice, a consumer could be prompted to reauthorize one use, and see an option to "reauthorize all" while visiting an authorization management portal. The Bureau should also consider what triggers the "clock" on reauthorization. The variety of uses in consumer-permissioned financial data sharing make categorizing reauthorization timelines in regulation a significant challenge.[64] Instead the Bureau should establish a principle of recency of use to provide that a consumer's recent use of an authorized product or service constitutes a reauthorization (see our response to Q93 for details).

- **Location:** Just as authorization under the Proposal would be managed by third parties, so too should reauthorization. The United Kingdom initially prescribed a reauthentication requirement (as opposed to reauthorization, but intended to have the same outcome of verifying that a consumer wanted to persist access) at the data provider, but after observing the harm it caused to consumers and third parties, they adjusted to a reauthorization requirement at the third-party data recipient.[65] We note here that, unless there are legitimate security concerns based on which the data provider believes reauthentication is necessary, the data providers should be prohibited from using reauthentication as a means to circumvent the reauthorization process and to break otherwise legitimate connections made between a consumer's financial accounts and

[63] The United Kingdom's 90-day reauthentication program resulted in significant consumer drop-off and is under re-examination. "FCA publishes changes to 90-day reauthentication rules"
[64] For example, for consumers who have authorized a data sharing connection to support a budgeting app, it may make sense to ask the consumer to refresh authorization for a data sharing connection on a yearly basis. On the other hand, in the case of data sharing that enables a recurring payment or transfer such as to pay down a 30-year mortgage, the consumer could be negatively impacted if they miss the prompt to refresh their reauthorization at 12 months and their recurring payment or transfer is interrupted as a result. In such a case, it may be more reasonable to prompt the consumer to refresh authorization for data sharing only after the defined term of the recurring payment.
[65] "FCA publishes change to 90-day reauthentication rules"
https://www.openbanking.org.uk/news/fca-publishes-changes-to-90-day-reauthentication-rules/

the data recipients' product or service.

As discussed in our response to Q93, an ideal outcome for consumers would be for them to be able to reauthorize all of their use cases at once. The Bureau should not prohibit authorized third parties from offering consumers the ability to reauthorize all of their authorizations at once.

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?**

Please see our response to Q92 for recommended reauthorization principles that would reduce negative impacts on consumers while protecting their financial data access rights. To reduce unnecessary costs on third parties and to facilitate efficient oversight, the Bureau should direct that authorization and reauthorization be handled by the same authorized third party.

The Bureau should allow consumers to refresh their authorization before the authorization period lapses. We recommend that third parties enable authorization management portals that also would allow consumers to refresh or revoke authorizations. Such portals could allow consumers to refresh multiple authorizations at once, providing a consistent, high-context experience in which to make reauthorization choices. This solution provides the consumer the ability to synchronize the authorization time periods across all their authorizations, if they so choose.

The Bureau should also 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. Specifically, the Bureau should establish a principle of recency of use, and rather than attempt to define recency characteristics for each use case, define it broadly to reflect the variety of use cases in the market.

Because in some instances the authorized third party will not be the data recipient, recency of use should reflect the consumer's use of the data recipient's product or service, instead of their interaction with the authorized third party. For example, if a budgeting application relies on a data aggregator for authorization, and a consumer uses their budgeting application weekly, then that weekly use should qualify as a regular reauthorization even though the consumer has not interacted directly with the authorized third party. The market can respond to the recency principle by developing signals to provide confirmation of use, especially where a data recipient

relies on a data aggregator for authorization.

As discussed in our response to Q146, imposing undue reauthorization requirements on authorized third parties will create an unlevel playing field where data providers can offer identical products and services without facing equivalent reauthorization requirements.

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.

We agree with the Bureau's proposal that authorized third parties provide consumers with a mechanism through which they may revoke the third-party's access to their information. The Bureau should require that authorized third parties provide such a mechanism, but should not prescribe the location or particular mechanism by which the revocation is served, other than to require that the revocation be at the same level of comprehensibility as, and consistent with, the authorization experience. The Bureau should also consider the need for such mechanisms to be accurate and synchronized with other authorization management portals, as discussed in our response to Q75.

Plaid has built a permissioning management tool called Plaid Portal, where consumers can view and revoke their connections across data providers and recipients (see Appendix G).[66] As discussed in Q139, it cost Plaid over $1 million and 13,000 hours to build Plaid Portal. However, such costs will be lower for data recipients and providers, which manage fewer connections than aggregators.

The Bureau could reduce costs and facilitate compliance for smaller data providers and data recipients by enabling them to rely on the authorized third party for revocation purposes, either by hosting a link to that authorized third party's experience, or by including instructions for doing so in an information center on their domain.

As discussed in our response to Qs 11, 16, 20, and 117, authorized third parties will need consumers' contact information in order to deliver authorizations, disclosures, and revocation mechanisms.

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?

[66] The Plaid Portal can be visited at https://my.plaid.com/

Data providers should be permitted, but not required, to provide consumers a mechanism by which they may revoke third-party authorization. The additional technology costs of such a requirement would burden smaller data providers.

The benefits of data providers providing revocation mechanisms could include consumers feeling more in control of their data choices by having more locations at which to revoke access. This same goal would be achieved by a data provider simply informing consumers about where to go to revoke authorizations. Therefore data providers should be required to provide directions to their customers about how to revoke authorizations at the authorized third party.

It is not feasible for data providers to programmatically provide revocation mechanisms where credentials-based screen scraping is used. Where screen scraping relies on consumer credentials, the only way in which a data provider could revoke third party access would be to discontinue a consumer's credentials, which would carry significant consumer cost. A data provider could coordinate with an authorized third party to manually relay a consumer's revocation instructions for the third party to implement, but this would entail some cost and friction. If tokenized screen scraping is in use, then a data provider could revoke a token without discontinuing credentials. For this reason, in addition to those outlined in Q94, authorized third parties should be required to offer a revocation process and mechanism, with data providers being permitted to offer a revocation mechanism if they choose. As noted in Q75 and Q94, the Bureau should also consider the need for such mechanisms to be accurate and synchronized with other authorization management portals.

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?

Yes, an authorized third party should be required to report consumer revocation requests to a covered data provider. Where the authorized third party is a data aggregator, it should also be required to report revocation requests to the data recipient reliant on the aggregator to manage authorization. These requirements will help to maintain synchronization across the ecosystem for the consumer, ensuring they have confidence that their desired revocation is carried out. Several mechanisms exist by which an authorized third party can report the revocation – e.g., via an API integration, webhooks, and audit logs – so the Bureau should not prescribe a particular mechanism by which this reporting occurs. It should, however, have a requirement for a period of time in which they should have this information updated, so that the information is consistent everywhere. See our response to Q75 for details on synchronization of revocation requests.

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?

There should be requirements for third parties to carry out consumers' revocation requests of any kind. In general, as explained in Q12 and Q74, the authorized third party is best suited to carry out revocation, because it has insight into both the authorized uses and the scope of authorization.

So long as the authorized third party is responsible for authorization and revocation, the costs of consumers' revoking access to one authorized use among many are *de minimis* for third parties. Authorized third parties would simply manage their own technology to update the access requests they send to the data provider based on the latest authorization. They would also send a record of that revocation to the data provider and, as applicable, the data recipient (if access is handled by a data aggregator), so that each party's systems would be synchronized (see our response to Q75 for details on synchronization).

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.

The Bureau's proposed definition of "secondary use" should be narrowed and should apply to all ecosystem participants.

The Bureau proposes to define 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." (Emphasis added.)

The Bureau's proposed definition of "secondary data" is so broad as to include uses of consumer data that are common and non-controversial across industry and are typically employed to run a safe and well managed business. In response to Q88, we proposed an adjusted definition of "reasonably necessary" that would ensure that the definition captures all authorized uses that are reasonable and expected (i.e., expand the definition of "reasonably necessary"). Because those uses are reasonable and expected, they are *not* secondary uses and should not be subject to any secondary data use restrictions. These reasonable and expected authorized uses are essential both to consumers benefiting from their financial data access rights and to the overall health and competitiveness of the ecosystem. For example, without authorized third parties' ability to use consumer-permissioned information for troubleshooting, consumers may have frustrating and broken experiences.[67]

[67] In order to troubleshoot issues with the consumer's connection, data, a third party needs to be able to locate and identify the consumer's connection and data. The third party can only do that if they are able to use certain identity information, such as the consumer's name, address, or telephone number, to search for the connection and data.

The Bureau's definition of "secondary data," as written, only applies to third parties. As set out in Q88, any use limitations standard should be applied consistently to all §1033 ecosystem participants, including third parties *and* data providers. This introduces competitive implications: if use restrictions are not applied consistently to participants – for example, if authorized third parties are not able to use consumer-permissioned data in the same way data providers do to protect consumers from fraud and security risks, protect ecosystem participants from similar risks, or improve user experiences or products – then consumers will not only be directly at risk, they will also face an ecosystem in which the data provider can provide a more secure and user-friendly experience than the authorized third party.

The Bureau should regulate "secondary uses" in line with certain principles outlined below, and consistent with international and state privacy law practices.

Taking into account the premise that secondary data use limitations do not include "reasonably necessary" uses and should be imposed on all ecosystem participants, not just third parties, the Bureau should adopt a multi-faceted approach to regulating secondary use of consumer data based on the principle of highest value delivered to the consumer. Because secondary uses can deliver substantial value to consumers – such as the development of new products and experiences, the improvement of existing products, and the ability to introduce new valuable use cases – the Bureau should not ban all secondary data use.

Instead, the Bureau should regulate the types of consent and disclosures required for secondary uses. As considered in the Bureau's proposal, both opt-out and opt-in requirements should apply, depending on the type of secondary use:

- **Secondary Opt-Out:** Uses beyond reasonably necessary which uses (including reasonable and expected uses), which are compatible with the consumer's primary purpose, but where consumer's privacy interests could outweigh the third parties' interests in using the data. Examples of this include:
    - Marketing or advertising products or services provided by the same company with which the consumer is already a customer, like a checking account provider also offering a savings account.

- **Secondary Opt-In:** Uses beyond reasonably necessary that are not compatible with the primary use case. Examples of this include:
    - Use of data by a third party for lead generation or marketing.

Finally, the Bureau should be clear that de-identified data is not considered a consumer's personal data and therefore should not be subject to secondary data use restrictions. (See our response to Q102.)

Without this information, the third party will be unable to troubleshoot or resolve the concern, leading to a poor (if not broken) consumer experience.

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?

Please see our response to Q88 and Q98 for details on our proposed definitions of reasonably necessary and secondary uses of data.

The timing and format for disclosures about secondary use should follow the same criteria as "reasonably necessary" use (based on the adjusted definition offered in Q88) authorization disclosures. The Bureau requested input in Q19 about authorization disclosures, and our response there addresses the identification of primary and secondary uses in those disclosures.

As set out in Q98, "opt-out" and "opt-in" mechanisms are appropriate depending on the type of secondary use. In the interest of aligning the authorization disclosure with consumers' most immediate data-sharing decisions, we recommend the following:

- For secondary opt-in uses, third-party data recipients should be permitted to request opt-in consent during the authorization experience.
- For secondary opt-out uses, the consumer should be given the opportunity to opt-out of those uses at the revocation experience.
- Secondary uses that may require opt-out or opt-in consent should *also* be addressed in the accessible long-form privacy policy and, per our recommendation in response to Q20, in the copy of the signed authorization.

We recognize there may be some high risk secondary uses of data, but we are not familiar with the details of those uses. Accordingly, we focus on disclosure and opt-in/out-out mechanisms to ensure that consumers are informed about their choices and the corresponding risks in a way that balances costs for third parties.

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.

The Bureau should implement a layered approach to restrictions on data use, with requirements for "reasonably necessary" uses, as modified to include reasonable and expected uses, secondary opt out uses, and secondary opt in uses for consumer-authorized data. (See also our response to Q88 and Q98.) As we describe in response to Q88 and 98, the Bureau should adjust its standard of what information is necessary to obtain the product or service requested by the consumer. Additionally, the Bureau should only prohibit third parties' use of consumer-authorized information where the Bureau has compelling evidence of an unacceptable risk of consumer harm. This approach benefits consumers for the following reasons:

- Reasonable and expected uses of information – which may be beyond those which are strictly necessary to obtain a product or service – can improve consumer outcomes, which is why we recommend that they be included in the definition of "reasonably necessary." (See our response to Q88 for details and Q98 for examples of these uses.)

- Applying such a prohibition only to third parties, and not to data providers, creates inconsistent standards, where data providers (under the GLBA) can use consumers' own data in ways that consumers themselves (under §1033) cannot. Any use limitations should be applied consistently to ecosystem participants and not to third parties alone.

Should the Bureau identify any high-risk secondary uses of data that it determines warrant prohibition, those prohibitions should apply broadly across the industry.

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.

Plaid uses data for reasonably necessary purposes outlined in our response to Q88, and for common other uses like to improve our products and services and build new products and services. For example, we build fraud prevention technologies that provide greater levels of certainty and security to consumers, in response to market demand for those products.[68] We also build data sharing portal technologies to better enable consumers to control their authorizations in one place, and use metadata about the consumer, like which data providers to which they have previously connected, to create simplified experiences for consumers.

We build these new products and services because consumer behavior is constantly changing in the digital era, and demand for digital products and services requires data-driven innovation. We are focused on the consumer and providing them value.

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

[68] Hampole, Rahul. "Announcing Plaid Signal: Unlock Instant Ach and Reduce Return Risk." Plaid, November 17, 2022. https://plaid.com/blog/plaid-signal-unlock-ach/.

to provide the requested product or service? If so, by what standard should consumer information be considered "de-identified"?

Global precedent establishes that de-identified data that cannot be reasonably reidentified can be used beyond what is "reasonably necessary" (as defined in Q88). De-identified data should follow well-accepted global standards, which hold that, if a data user can demonstrate that the individual cannot be reasonably re-identified given the circumstances of the individual use case and the state of technology, the data can be considered anonymous.

We recognize that the ability of organizations to manage anonymization of data may vary, and recommend that there be different standards for internal and external use of de-identified data. The expectation for making an de-identified data set available externally should be very rigorous. This is because external, particularly public, availability increases the risk that someone will attempt to re-identify individuals in that data set. When data sets are retained within an organization, the organization can implement both technical controls and policies that reduce the likelihood of re-identification.

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?

So long as the Bureau expands the definition of reasonably necessary to include uses described in our response to Q88, we support the requirement to delete data that no longer meets those definitions. The Bureau should clarify, however, that de-identified data is not subject to these restrictions because it no longer has privacy implications to the consumer. (See Q104 for further details.) Finally, the Bureau should apply these requirements equally across data providers and authorized third parties, for reasons discussed in our response to Q1.

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?

No, an authorized third party should not be required to automatically delete consumer information upon receipt of the consumer's revocation request. A principle of consumer control is that one consumer action should not be assumed to imply another. Revocation and deletion are fundamentally different actions, and conflating the two risks consumer harm, as demonstrated by the examples in our response to Q108 and Q144.

Instead, at the time of revocation, consumers should be informed that they also have the separate right to delete their personal data, should they wish. This gives control to consumers

over how their data is handled, rather than making choices on their behalf. While revocation should not require deletion in any circumstances, the Bureau should be aware that multiple laws (for example those setting forth AML/KYC obligations) require retention of data irrespective of a consumer's choice.

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?

Yes, if the law permits, authorized third parties should be required to disclose to consumers that their information is being retained. Because legal obligations should fall under reasonably necessary uses (as discussed in our response to Q88), this information should be included at a high level in the authorized third party's privacy policy, in keeping with our recommendation responding to Q19. This information could also be surfaced at the time a consumer makes a deletion request, if permitted by law, to clarify to consumers that legal obligations impose certain requirements on third parties.

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?

As set out in Q104, an authorized third party should not be required to automatically delete consumer information upon receipt of the consumer's revocation request. A principle of consumer control is that one consumer action should not be assumed to imply another. Revocation and deletion are fundamentally different actions, and conflating the two risks consumer harm. Thus, upon receipt of a revocation request, it should not be assumed that a third party is required to delete any information. See our response to Q144 for details on the consumer and third party harms that could result from such an assumption. As noted in our responses to Q104 and Q105, there may be circumstances when it is necessary to retain consumer data regardless of a consumer's deletion request. Moreover, there may be reasons a consumer would prefer not to delete their data. Our recommendation is that at the time of revocation, consumers should be informed that they also have the separate right to delete their personal data, should they wish.

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?

Yes. Some authorized third parties offer multiple products or services that use overlapping data elements. For example, a consumer might use – from the same data recipient – (i) a personal financial management service that accesses the consumer's transactions and balances from a data provider; and (ii) a loan application service that accesses two years of financial statements (which include transactions and balances) from the same data provider. If, after receiving the

loan, the consumer instructs the data recipient to delete the financial statements, regulation should not presume that this is also a request to delete all transactions and balance information collected as part of the personal financial management service, nor should it presume that the deletion requests constitutes a revocation of ongoing access to that information for the purposes of the personal financial management service.

Q108. Should deletion of consumer-authorized information be required when authorization lapses at the end of a durational period?

No. The Bureau should clarify the distinction between revocation and lapsed authorization. Revocation is an affirmative consumer action, and, at the time of the revocation, the consumer should be able to ask the third party to delete their data, if they so choose. With lapsed authorization, the consumer has not taken any action and may very well choose to reauthorize at some point in time.

To protect consumers from unintended harm, when there is a lapsed authorization, third parties should be given a reasonable amount of time to seek reauthorization before deletion. Consumers do not always take action the first time they are prompted, and they should be given multiple opportunities to make active choices with their information before their choice is assumed from inaction. We recommend twelve months should elapse before lapsed authorization implies deletion. This would allow a consumer time to notice their product or service usage has been interrupted and to reauthorize, while retaining the value of that product or service based on their previously-shared information.

As discussed in our responses to Q144 and detailed in Appendix A, consumers can face financial harm if lapsed authorization overrides their data sharing choices. The Bureau should note that there are a number of use cases – for example, mortgage payments – that by their nature extend for many years. Treating lapsed authorization as a deletion in these rare cases, even after a period of years, may break connections in a way that could be extremely deleterious to certain individuals. In these cases, lapsed authorization should be treated as deletion only where the use case is no longer viable – e.g., after a mortgage has been paid off.

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?

As described in our response to Q90, there are multiple methods authorized third parties could use to minimize data collection and retention under screen scraping. Under the first method described in our response to Q90, in which the authorized third party writes a software script to only gather the required information, the deletion requirements should be exactly the same as under a third party data access portal arrangement – meaning the third party should delete, if there is a deletion request, or if there is a lapsed authorization of 12 months. Under the second

method, in which companies may over-collect data but then purge the data, deletion requirements should be imposed at the point of collection, meaning the third party would be required to immediately purge unauthorized data, and include information about that procedure as part of their certification statement.

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?

Yes. De-identified (anonymized) information is no longer consumer personal information and so falls into a separate category outside of any use limitations. Parties use de-identified data to improve their products and develop new products, including building fraud mitigation and security tools that make the ecosystem safer. The Bureau should establish a set of principles to guide determining what constitutes de-identified information, and allow authorized third parties to retain this information.

Finally, we note that GLBA-compliant financial institutions routinely package and distribute de-identified information for marketing purposes, and the Bureau should not set an inconsistent standard as between §1033 and GLBA, as explained in greater detail in Q1 and Q88. For the reasons explained in those responses, any restrictions on the use of de-identified data should apply to all participants in the §1033 ecosystem.

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?

We agree with the Bureau's proposal that authorized third parties be required to comply with the GLBA Safeguards Rule or Safeguards Guidelines. As the Bureau notes, many if not all authorized third parties are already subject to these requirements. Moreover, these requirements already take into consideration the compliance impact for small businesses, as they are tailored to the "size and complexity" of the business, and the sensitivity of the information at issue.

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?

At Plaid, data is secured through a defined and managed information security program that meets and in some cases exceeds requirements established in industry frameworks such as SSAE18 Trust Service Criteria for Confidentiality, Integrity, and Availability, ISO 27001, and NIST CSF. We follow the GLBA Safeguards Rule. We would ***not*** reduce any form of security infrastructure if the requirements under a §1033 rule fell below our current practices. As outlined in our response to Q111, we believe the Safeguards Rule to be appropriate for all authorized third parties in the consumer-permissioned financial data sharing ecosystem.

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?

The Bureau's approach to require authorized third parties to maintain reasonable policies and procedures to ensure information accuracy is appropriate. However, the Bureau should be explicit about where responsibilities begin and end, because third parties have no control over data providers' infrastructure or general business processes, and so cannot rectify accuracy errors introduced by data providers (e.g., if a data provider provides an inaccurate account number in their third-party access portal).

Authorized third parties' data accuracy can be promoted through policies and procedures that center on internal controls designed to ensure (i) reliability of data, and (ii) system integrity. Requiring technical controls that ensure integrity of systems processing data (such as appropriately mature change management controls) is appropriate for data accuracy requirements. There are also common frameworks (e.g., SSAE18) that address systems integrity, which should be included in frameworks for ensuring data accuracy.

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?

Plaid resolves errors in consumer-permissioned data through our support channels. We have systems in place to evaluate the severity of an error, investigate to identify the root cause, and help rectify the situation.

The majority of accuracy-related questions that consumers identify to us are "perceived" inaccuracies. For example, a data provider may substitute the consumer's actual account number for a tokenized number the consumer is not familiar with. In these cases we educate the consumer on tokenization. A smaller set of accuracy questions relate to categorization, i.e. how a transaction is categorized. In those cases we work with the consumer to resolve questions around categorization. Notably, the substantial majority of overall consumer requests sent to our support channels relate to consumers' inability to access their information from a data provider.

To resolve accuracy issues in access via screen scraping, we take action to investigate the root cause and resolve issues where we can – for example, where a data provider changes its online financial account management portals or access portal we may have to adjust our screen scraping scripts or systems. (For details on how third parties manage data collection under screen scraping, see our response to Q90.)

Where data is obtained pursuant to a data access agreement, error resolution is typically governed by our relationship with the data provider. In such cases, we start by investigating whether our systems were the cause of an issue, and if they were we move swiftly to resolve them. If we find no internal issue, then we work directly with the data provider to address the issue. As discussed in our response to Q57 on availability requirements, the Bureau should encourage data providers and third parties to collaborate in such investigations, to ensure consumer protection and issue resolution.

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?

Our internal research indicates that the majority of actual accuracy errors (rather than perceived errors as described in Q114) result from inaccuracies in the data we collect from data providers, as opposed to inaccuracies that occur during our transmission of that data to recipients. Such data provider-introduced inaccuracies might include wrongly categorized information, or numerical errors such as displaying or transmitting incorrect transactional or balance information.

Whether or not third party policies and procedures can fix errors in data that was inaccurate when accessed from a covered data provider depends on the type of access.

- **Under screen scraping:** Errors can arise when a data provider makes a change to their financial account management portal, for example by redesigning the user experience of their account landing page, changing copy on that page, or migrating their systems to another digital banking platform or core provider. When these changes happen, the authorized third party's software scripts might inadvertently collect the wrong information. Such an issue could be resolved by the data provider notifying the third party of upcoming changes, so that the third party can update their scripts. This would also involve a data provider providing authorized third parties with test credentials, which are proxies for consumer credentials, and would allow the authorized third party to test its updated script.

- **Under dedicated third-party access portals:** Errors arising under these portals would result in inaccurate data being surfaced via the portal. A consumer could point out that

inaccuracy to the third party, which could correct that information and relay it back to the data provider. One recent example is a data provider that accidentally surfaced a previous name for a consumer, who, upon seeing their previous name in a third-party application, notified that application of a mistake. The application then notified Plaid, which in turn notified the data provider.

Common policies and procedures for addressing known issues that cause inaccuracy would be beneficial to consumers. Clear guidelines for engagement across participating entities could support industry resolution where collaboration is needed.

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?

Yes, policies and procedures to ensure accuracy should include addressing disputes submitted by consumers. As discussed in response to Q1 above, the Bureau should clarify overlap between FCRA and §1033 with regard to dispute resolution. In setting dispute resolution requirements, the Bureau should distinguish between two types of third parties at issue – (i) data aggregators; and (ii) data recipients – given the different relationship each has with the consumer. Dispute resolution policies and procedures should be complementary to the requirements imposed upon covered data providers with respect to accuracy.

The Bureau should require that covered data providers, data aggregators, and data recipients cooperate in addressing and investigating consumer disputes, and set response timelines for each party, depending on the severity of the dispute.[69]

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?

We agree with the Bureau's recommendation for authorized third parties to provide consumers with periodic disclosures. Periodic disclosures are a helpful mechanism and a familiar experience to consumers, who see such disclosures when companies (that have consumers' personal information to be able to contact them) send updates to their terms of service or privacy policies. The costs of these new disclosures would be *de minimis* for companies that already have annual privacy notice obligations. Such disclosures should be allowed to be delivered electronically, which further minimizes costs. The Bureau would reduce costs and facilitate compliance for small entities by allowing data recipients to rely on data aggregators to serve periodic disclosures and reauthorization, when they already rely on that same data aggregator to serve as the authorization and revocation manager.

[69] This requirement should assume consumers' cooperation, and provide flexibility for compliance by providers, aggregators, and recipients in instances where a consumer does not cooperate with the investigation.

Periodic disclosures and reauthorization are only possible if the authorized third party has contact information for the consumer who authorized the data to be collected and shared. Contact information is not always necessary for the data recipient's particular product or service (e.g., a budgeting application may only require transactions data, not identity data, to provide the consumer with its budgeting service). However, that contact (or identity) information is necessary for an authorized third party to, for example, properly manage authorization, revocation, and disclosure. That is why, in our adjusted definition of "reasonably necessary" in Q88, we proposed that the definition be expanded to include other expected information, like contact information. If identity information is obtained in this manner, then the aggregator serving as the authorized third party would only be able to use that contact information for the explicit purposes associated with the management of authorization – i.e., serving reauthorization, revocation, or disclosure – and any reasonable and expected purposes, such as fraud or abuse detection or prevention, troubleshooting, or improvement of the authorization service. It could not be used for, say, the development of new products.

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?**

As discussed in our response to Q19, we believe that disclosure should be broken down into three categories – (i) authorization disclosure, (ii) reauthorization/revocation/periodic disclosure, and (iii) disclosure of privacy policies and terms of service. Each category should abide by principles of consumer control and comprehension for informed decision making, and each should be the responsibility of the authorized third party and not the data provider.

> (i) The authorization disclosure should occur just-in-time, to give consumers context for making decisions about which parties to authorize to access their information. The authorization disclosure should happen either (a) at the time of initial sign-up for a third party product or service (for example, signing up with a tax accountant in July even though they will not access your information until March), or (b) at the moment at which a consumer is establishing authorized access for the purpose of benefiting from a third party product or service (for example, linking new accounts to that tax service while conducting tax preparation in March).
>
> The authorization disclosures described in §III.B.2.i appropriately reflect the information that should be displayed at just-in-time disclosure: data elements, purposes, mechanism for revocation. Content requirements should be flexible and principles-based, as

opposed to prescriptive, since model clauses can fall behind innovation and lead to consumer confusion (see our response to Q18).

(ii) The periodic reauthorization disclosure should happen on a regular basis, as outlined in our response to Q92. This disclosure should reflect the same information provided in the initial disclosure – data elements, purposes, mechanism for revocation – but should add two new categories: mechanism for reauthorization and mechanism for deletion. These new categories should clarify the implications of reauthorization and deletion, including the inability to recapture previously deleted data.

(iii) The privacy policies and/or terms of service should be accessible within other disclosures, but should not be required to be displayed in full therein so as not to overwhelm the consumer.

Data providers should not be required to serve these disclosures, since they are not responsible for obtaining authorization nor for defining the purposes for which such data is being requested. They should be required, as discussed in our response to Q75, to notify a consumer of a third party's initial access attempt (but not be permitted to confirm with the consumer the authorization of a particular third party prior to making information available, for the reasons discussed in Q12 and Q75).

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?

A properly focused record retention requirement is reasonable and would support industry compliance. Those requirements should be tailored to the specific obligations of data providers and authorized third parties. Both data providers and authorized third parties should be required to retain records regarding (i) consumer complaints, (ii) consumer requests to revoke access, and (iii) consumer data deletion requests.

Data provider records should primarily pertain to the performance metrics of their third-party access portals (see Q59), and response to consumer authorization and revocation requests. For example, these records would include reporting on the availability requirements outlined in §III.D.1.ii.a, and the list of authorized third parties currently accessing their portals. As described in our response to Q80, the list of pre-registered authorized third parties should only include the entities directly accessing the third-party access portal, and data providers should not be required to maintain records of all data recipients who may rely on a data aggregator for authorization.

Authorized third parties should be required to maintain records on consumer authorizations, revocation and deletion requests, issues related to data providers' third-party access portals.

The Bureau should also recognize that in order for record retention to be comprehensive, authorized third parties will require contact information for the consumers that authorize them. As described in our response to Q117, the Bureau should clarify that an authorized third party must be allowed to obtain consumer contact information in order to carry out the reasonably necessary uses of authorization management, record retention, and disclosure.

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?

No, the policies and procedures outlined in the Proposal are sufficient for data providers and authorized third parties to be able to comply with obligations under the rule. Any requirement to maintain policies and procedures not outlined here would result in additional costs for both small data providers and small authorized third parties and would not materially improve compliance with the rule.

Q121. Please provide input on an appropriate implementation period for complying with a final rule, other than the potential third-party access portal requirement. 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?

The Bureau should allow a transition timeline for data provider compliance with the rule, but prevent anti-consumer activities such as blocking authorized third-party access during that time. The Bureau should also recognize that existing consumer connections would need to be transitioned from screen scraping to third-party access portals, in order to not disrupt consumers' financial lives. Based on our experience transitioning screen scraping traffic to third-party access portals with data providers of various sizes – including small data providers that would fall into our Class 3 described in our response to Q53 – transition timelines include three phases (we list timelines here for informational purposes; these are not meant to be recommendations to the Bureau):

- Phase One: Data provider builds third-party access portal – 3-6 months
- Phase Two: Data provider tests the portal for quality, to ensure that it is robust, secure, and reliable before sending live requests – 3 months
- Phase Three: Data provider works with third parties to migrate existing users from screen scraping to third-party access portal – 6-12 months (This process involves the data provider and third party collaborating to exchange credentials for access tokens, so

that connections maintain and consumer financial lives are undisrupted. New customers can initiate access requests while this is taking place, but existing customers will need to continue relying on screen scraping until their access can be transitioned).

In total this requires between six months to two years of technical effort on the data provider as well as third parties to transition all consumers from a screen scraping integration to a dedicated third-party access portal. Because phase three involves collaboration with a data aggregator to move credentials to tokens, data aggregator resources are a factor outside of a data provider's control. Otherwise, this timeline is largely contingent on the resource model and technical capabilities of the data provider (how many issues that need to be resolved in testing etc.) as well as the complexity of the backend systems (more challenging for data providers with numerous sub-entities or tech stack providers).

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, including updating policies, procedures, processes, and employee training programs?

The Bureau should set reasonable timelines for small covered data providers to implement the proposals under consideration, including policies, procedures, processes, and employee training programs. Some of these policies and procedures already exist, via relationships small data providers have with aggregators in which they, for example, have a communication channel with an aggregator for resolving consumer questions. While technology infrastructure costs are relatively higher for smaller data providers, costs of implementing policies and procedures can be smaller due to more nimble organizational structures and narrower scope of coverage.

Q123. Please provide feedback on the CFPB's understanding of the industries that could be affected by the proposals under consideration.

The list outlined in the Proposal captures the industries currently implicated in consumer-permissioned financial data sharing. All of the categories defined therein capture the markets Plaid currently serves with our data aggregation services, which may be considered data recipients under the Proposal.

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?

Over the last two years Plaid has observed that the consumer-permissioned data sharing network is increasingly bi-directional, meaning data recipients are becoming data providers and vice versa. Plaid counts dozens of companies that initially were only data providers as data recipients relying on our aggregation services, including many of the largest financial

institutions. These organizations deploy a wide variety of use cases, from personal financial management to wealth management to debt consolidation and refinancing. (On a related note, the overlap between data providers and data recipients is one of the reasons the Bureau should ensure any use limitations are applied uniformly, to the extent it determines to impose use limitations beyond those applicable to ecosystem participants in the GLBA. See our response to Q88.)

Similarly, many of Plaid's largest data recipients are now also data providers, though not all of them may be covered by the proposed data scope (for example, we support consumers' ability to share their investments holdings from several investing applications).

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?

Plaid currently provides disclosures to consumers within our own platform. (See Appendix D for an example of Plaid's account linking experience.) The expected costs to modify the content of any disclosures would be 30 to 40 hours of employee time, including legal and compliance review. The costs to modify technical systems are much greater because, for data aggregators, there is significant complexity to surfacing data elements and requests across our thousands of data recipient partners. Our estimate is that building the capabilities to provide any additional disclosures called for by the rule may cost approximately $1 million. These costs would be substantially lower for data recipients, since they would have more consistent and uniform disclosures.

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?

Yes, we have policies and/or procedures in place regarding the treatment and protection of consumer-authorized data. The development of these policies and procedures took a range of time to develop, with simple procedures requiring tens of staff-hours of time, ranging to the most complex requiring several hundreds of hours of staff time. Implementation costs vary widely, and range from the tens of hours for those requiring minor process updates, to over a thousand hours to implement the most complex policies requiring major system updates.

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?

Yes. Plaid has consumer-facing tools for access revocation and deletion. Specifically we host a consumer permissions management tool called Plaid Portal.[70] Since we power connections for millions of consumers, our systems require intensive and costly investments. Plaid invested seven full time engineers for one year to build our revocation and deletion tools on both the front- and back-end, an approximate total of 13,000 hours at a cost of over $1 million.

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?

We expect to incur between $40k-75k in up front costs plus $5k-10k per year in satisfying the training costs associated with the third party obligations and record retention obligations of the proposals under consideration.

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?

Plaid primarily offers business-to-business services and does not primarily offer consumer financial products and services. We provide services to companies acting as both data providers and recipients, and share consumer-permissioned data from both traditional and new financial service data providers, many of which would not have been able to develop or able to provide services without also being recipients of consumer-authorized information.

Products that complement traditional financial services include peer-to-peer payments services for smaller financial institutions, budgeting applications that help consumers manage funds across multiple accounts, and savings tools that push money from a checking account to a savings account within a single institution. Products that compete with traditional financial services include wealth builder credit cards, early access to earned wages, robo-advising tools, and fully digital checking and savings accounts.

Analysis of the industry indicates that legacy financial institutions mimic innovations developed by upstart companies, including the below examples (list not exhaustive):

- A major financial institution offers early access to earned wages programs, which were pioneered by fintech companies a decade ago[71]
- Financial institutions of a range of sizes have begun to offer buy now, pay later services[72]

[70] The Plaid Portal can be visited at https://my.plaid.com/
[71] "JPMorgan Chase, taking a feature from fintech rivals, gives some customers early payday deposits" CNBC, October 19, 2022 https://www.cnbc.com/2022/10/19/jpmorgan-chase-gives-early-payday-deposits-to-secure-banking-customers.html
[72] "Banks Moving Off the Sidelines to Snag Piece of Growing Buy Now, Pay Later Market." PYMNTS, February 11, 2022.

- Major brokerages reduced their commissions to zero dollars following financial technology startups.[73]

These examples illustrate how consumer data access rights drive innovation and enhance existing services. Consumer-authorized information access means that the providers of products and services compete on the basis of providing the best service, rather than locked-in, historical access to a consumer account or financial information.

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?

While Plaid is not privy to data providers' written policies, our direct interactions with data providers indicate that there are significant differences in consumer-authorized information access policies between covered data providers. Certain data providers have made clear to us that these differences reflect their belief that the data belongs to them and not their consumers. Differences tend to fall into five categories:

1. **Data scope**: Some data providers prohibit consumers from authorized sharing of certain information, including APR/APY, pending transactions, transactions history, identity data elements (name/phone/email), and raw account number (some replace account and routing numbers with tokenized account numbers that break multiple consumer use cases). These data elements are available to consumers on the online financial account management portals or mobile app (including online financial account management portals), but not in the data providers' third-party access portals. There are at least four major financial institutions that currently limit data scope availability in their third-party access portals.
2. **Access caps**: Some data providers implement data access caps, which vary depending on institution size. These caps introduce friction in consumer experiences by limiting information freshness and disrupting real-time, consumer-present connections. In some cases, consumers are completely blocked from accessing their data and connecting their accounts. Every major financial institution with a third-party access portal currently imposes some kind of limit or access cap on consumers' ability to authorize access to their own data.
3. **Third party registration**: As discussed in our response to Q80, some data providers require Plaid to pre-register all 7,000+ of our data recipient customers. Others do not, and only pre-register Plaid as the authorized third party. Pre-registration has competitive implications, and any security and compliance concerns could be mitigated through the recommendations made in Qs 80 and 81.

---

https://www.ctmobi.com/articles/4818078/banks-moving-off-the-sidelines-to-snag-piece-of-growing-buy-now-pay-later-market.

[73] "Lookout, Robinhood. E*Trade, Schwab, Ameritrade go zero-fee" TechCrunch, October 2, 2019 https://techcrunch.com/2019/10/02/robinhood-e-trade-schwab-ameritrade/

4. **Usage limitations**: In some instances, data providers purport to retain authority to limit use cases for consumer-permissioned access and in many instances data providers have held up progress on data access agreements because they have wanted the power to determine acceptable and non-acceptable use cases. We have consistently taken the position that the consumer is the party who can decide how to use their own data and that we are not authorized to limit the consumer's choice of services or products. We do impose contractual restrictions on our data recipient customers, such as prohibitions against sale of consumer data. Please see our discussion in Q88 about ensuring that any use limitations the Bureau determines to impose are consistently applied to all ecosystem participants and not only consumers and authorized third parties.
5. **Mandatory intermediaries**: Some data providers have taken the position that third parties, both data recipients and aggregators, may not directly connect to their third-party access portal. Instead these data providers dictate that the third parties must instead connect to an intermediary access portal controlled by a separate company that happens to be owned by a consortium of financial institutions. That intermediary would then take the data request from the third party, request the same data from the data provider, and relay the data to the third party. The CFPB should prohibit data providers from mandating the use of any intermediary for data access, because such practices are equivalent to granting a monopoly on access to the chosen entity. Monopolies, such as mandatory intermediaries, depress competition. Where a monopoly exists, there is an increased risk of price fixing, poorer access to data, and lack of incentive for innovation. This outcome is inconsistent with section 1033's goal of shifting power away from businesses and toward consumers. Consumers are entitled, under the law, to access and share their own data. They should be able to choose data recipients without limits that are imposed by the data providers, including any data aggregators that support their access and sharing. If a data provider wants to use an intermediary, that intermediary should be required to compete in the market and demonstrate sufficient value for third parties to choose to connect to it, not because they are forced to connect to it.

There are products and services for which prohibitions on access could lead a consumer to choose to switch from one covered data provider to another. We have seen examples of:

- Consumers who rely on Personal Financial Management apps sometimes switch banks because certain data providers do not provide pending transactions or refreshed transaction data; and
- Consumers trying to move money between accounts or make a payment will switch banks when data providers block them from accessing their data.

Currently, consumers do not have any remedy for denial of their right to authorize access to their own data, but a cursory social media search reveals consumer frustration and willingness to switch banks if doing so allowed the consumer to more easily connect accounts and share data in order to receive the products and services they want. Essentially, these consumers want to use competitive products and services available in the market but are being stymied by their

existing bank's restrictions on authorized data access.[74]

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?

Requiring the deletion of consumer data upon authorization lapses or revocations would significantly impact third-party products and business models. Three disruptions stand out:

1. **Breaking products and services whose usage does not align with the authorization timeline**
    a. Lending: Take a lender who needs consumer-permissioned data access to collect automated repayments. The consumer signs up for a sixteen-month term loan and authorizes automated payments, but the authorization intentionally or inadvertently lapses after, e.g., twelve months and the lender is required to delete that account number. With four months of outstanding payments, the lender would either need to re-onboard that customer in order to gain renewed authorization to that account information, or accept a substantial loss resulting from their inability to collect payments. This imposes unnecessary costs on both the lender – potentially increasing the cost of the product or service to the consumer – and administrative burden on the consumer to intervene in a financial plan that is serving the exact purpose desired by the consumer, or else to suffer an adverse credit event.
    b. Recurring payments: This same lapse would impact any third party relying on account numbers to initiate recurring payments, from subscription streaming services to fitness centers. This new risk of lapsed third-party authorization, deletion of data, and new onboarding could severely harm third party business models.
2. **Discontinuity of consumer relationships**
    a. Taxes: Consumers very often share their information for tax purposes once annually. Many consumers rely on the same tax preparers for years, and the value of service they obtain from tax preparers is directly correlated with the prior insight those tax preparers have into their finances. If third party accountants, whether large software companies or small businesses, were required to delete consumer-authorized information due to a lapse in authorization, the value of their service would substantially decrease.
    b. Personal financial management: Consumers who want to track their finances rely on providers to have deep insights into their current and historical patterns,

[74] An executive at one of Plaid's customers noted: "We're onboarding our users who connect to XYZ Bank, migrating them from one aggregator to another to use the open banking implementation. Some users are concerned enough with losing pending transactions and available balances when connecting to aggregators (due to XYZ bank's open banking implementation) - so much so that they'd like to switch banks to receive pending transactions and/or available balances again. Could you please confirm which OAuth Institutions we can recommend to users to receive pending transactions and available balances via Plaid? We'd also be happy to recommend particularly good non-OAuth Institutions with these features too, if any come to mind."

including savings, spending, borrowing, and investment. Similar to the tax preparation example, the value of these services increases with duration. A requirement to delete prior data for a lapsed authorization would effectively break the value of these services, and severely harm their business model.

3. **Inability to mitigate fraud**
    a. Third parties often rely on consumers' information to mitigate fraud, and a deletion-upon-revocation requirement introduces a fraud vector for third parties to manage. For example, fraudsters might try to open consumer accounts using fabricated consumer information, which third parties guard against by examining whether their already-stored consumer information matches information coming in from a new consumer request under the same name. If consumer revocation also required deletion, they would lose that fraud mitigation technique.

As referenced in our response to Q104, the Bureau should not require third parties to delete data as a result of a lapsed authorization, since doing so would introduce the harms above.

Q145. Would the proposals restricting certain secondary uses of consumer data impede products or business models used by third parties?

Yes. Restrictions on secondary uses of consumer data could impede products or business models. Depending on what is considered a secondary use, restrictions also could reduce the ability of third parties to improve security, fraud prevention, authentication, and identity verification in the ecosystem.

The rule should ensure consumers have access to safe, innovative and increasingly effective services and products while balancing consumer privacy interests. (See our response to Q88 and Q98.) In Q88 we recommend that the definition of “reasonably necessary” be broadened to include related and expected uses that are not primary uses; such uses should be excluded from any secondary data use definition. These related and expected uses serve the consumer and the ecosystem by permitting safety and product improvements. In Q98 we propose a definition of secondary uses, which excludes primary and related and expected uses, i.e. the expanded version of “reasonably necessary.”

Using these definitions, authorized third parties rely on consumer-permissioned data for:

- Primary uses, such as to provide specifically requested products and services;
- Related and expected uses, such as to improve existing consumer-facing products and services or to prevent fraud; and
- Secondary uses, such as to develop completely new products and services, or cross-sell products via ordinary marketing channels.

We believe the Bureau would seriously impede products and harm business models if it prohibits reasonable and expected uses of consumer permissioned data because these are common and non-controversial, non-primary uses of data. We also believe the Bureau can

regulate secondary uses of data, as defined in Q98, through consent requirements, as is the norm in various state and international laws. If the Bureau takes a different position, and determines that reasonable and expected uses or secondary uses of consumer permissioned data should be prohibited, then it should impose that limitation on all participants in the ecosystem, including third parties and data providers.

Q146. Would any limitations created by the data availability standards impede products or business models used by third parties?

Data availability requirements would provide significant enhancements to the products and services that third parties' provide to consumers. Third parties' products that rely on consumer-authorized information are highly dependent on the timeliness, quality, and availability of that information. Clear and high standards for data availability would enable third parties to consistently and reliably serve their consumers without diverting resources to repair access or navigate consumer complaints about inconsistent data access.

Inconsistent access has an impact across all types of products and services. Inconsistent connections or downtime result in consumers leaving third party platforms. Personal financial management tools are most at risk of inconsistent access, because consumers rely on them having real-time information to provide insights and guidance.

Q147. Would periodic reauthorization requirements lead to reduced customer retention for products or business models used by third parties?

Yes, periodic reauthorization requirements would lead to reduced customer retention for products or business models used by third parties, and would introduce competitive imbalances with data providers' products, which would not face similar requirements. As noted in Q93, the Bureau should establish a principle of recency of use to provide that a consumer's recent use of an authorized product or service constitutes a reauthorization.

The Bureau should consider the competitive impacts of reauthorization requirements. The United Kingdom's 90-day reauthentication requirement resulted in 20-40% consumer drop-off, which prompted their revision of Strong Customer Authentication (SCA) rules.[75]

Data providers face no reauthorization requirements for their own products. So if a burdensome reauthorization requirement were established under §1033, a data provider could offer an identical service as a third-party data recipient – which, as pointed out in our response to Q142, they already do – and the data provider's product would have a competitive advantage over the data recipient's identical service due to its lack of reauthorization requirements.

[75] "PS21/19: Changes to the SCA-RTS and to Guidance in the Approach Document and the Perimeter Guidance Manual." Financial Conduct Authority, November 29, 2021. https://www.fca.org.uk/publications/policy-statements/ps21-19-changes-sca-rts-and-guidance-approach-document-and-perimeter-guidance-manual.

To be clear, we are supportive of reauthorization as a concept. But the Bureau should focus on the principle of recency of use – and should consider consistent requirements across the ecosystem – so as to not introduce competitive imbalances across data provider and data recipient products.

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?

We expect the proposals under consideration to reduce the costs of negotiating data access agreements. Data access agreements were developed in the absence of regulation and often require between twelve and twenty-four months of negotiation. Pending the outcome of this rulemaking, there could be instances in which a data access agreement is not a prerequisite for authorized third-party access to a data provider's third-party access portal. Nevertheless, there will be some circumstances when parties will still want data access agreements and they should be permitted so long as they are not in conflict with regulation.

Many of the issues discussed in the CFPB's Proposal would address topics that have otherwise been the subject of extensive negotiation in data access agreements or resulted in limitations on consumer access. We estimate that within our past DAA negotiations, approximately 60% of the time was spent on topics that the Bureau is considering addressing, including: consumer permissioning, disclosure, authorization, coverage of data providers, scope of data, availability requirements, and obligations on third parties. Approximately 20% of negotiating time was spent on issues not included in the Proposal, such as allocation of liability and oversight of third-party data recipients. The final 20% of negotiating time has typically been spent on issues that can be resolved in standard terms of access to be agreed to as part of third party registration with a data provider (for example, technical standards for integration).

If implemented, the Proposal would result in less time spent negotiating agreements, less costs related to customizing activities for each data provider,[76] and less service disruption associated with unreliable access. Moreover, while the Bureau is not considering addressing allocation of liability, the clarification of roles and responsibilities may ease liability discussions. Further, if prudential regulators were to clarify the applicability of third party risk management guidance (as discussed in our response to Q50), then that might further reduce time spent negotiating agreements.

More importantly, Plaid anticipates that the outcome for consumers of the rule will be increased power and control related to the use and sharing of their own data. In the past, Plaid has had difficulty negotiating consistent consumer access rights across data providers in data access agreements (see our response to Q143) and thus strongly endorses the Bureau clarifying the

[76] An example of "costs related to customizing activities for each provider," is pre-registering all 7,000 of Plaid's data recipients according to specific requirements that differ across providers. Discussed in more detail in our response to Q81.

legal mandate for data providers to provide consumer direct and authorized third-party access. With a §1033 rule, consistent oversight and enforcement, and the Bureau's use of other tools, such as its Consumer Response program, guidance, and consumer education efforts, substantial portions of the topics negotiated in data access agreements will be covered under regulation instead of bilateral contracts.

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?

FinRegLab's research on the use of alternative data in credit underwriting shows that consumer permissioned sharing of bank account information can supplement credit reporting in providing clearer pictures of small businesses' creditworthiness.[77] Research from New York University shows that fintech lending "played an important role in extending PPP loans to Black- and Hispanic-owned businesses."[78] Community banks also benefit from having consumer-permissioned access to data that large banks maintain. This access can level the playing field for credit delivery and underwriting, enabling smaller institutions to compete with larger peers.

[77] "The Use of Cash-Flow Data in Underwriting Credit - Empirical Findings." FinRegLab, 2019. https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.
[78] Howell, Sabrina, Theresa Kuchler, and Johannes Stroebel. "Which Lenders Had the Highest Minority Share among Their Payment ... - NYU." New York University, December 10, 2020. https://pages.stern.nyu.edu/~jstroebe/PDF/HKS_PPP_Minority.pdf.

Appendix A: Consumer harms stemming from lack of reliable data access

The below list is intended to illustrate the range of consumer harms that can result from a lack of authorized third-party access to consumer-permissioned data. This list is not exhaustive.

- **Missed payments:** If a consumer or their authorized third party cannot effectively access or utilize information required to initiate a payment – such as account and routing number, permanent account number, personal identity information, balance information, or otherwise – then that consumer or authorized third party would not be able to effectuate a timely payment.

- **Higher interest rates on loans:** If a consumer cannot access and share their information directly or with an authorized third party, then they lose the ability to timely and easily compare rates across potential lenders.

- **Fees and penalties levied by the consumer's financial institution (overdraft fees, late fees, missed payment fees)**: If a consumer cannot share their current account balances with an authorized third party when initiating a transfer, there is an increased risk that the third party might initiate a debit transaction against the consumer's account when that consumer would not have sufficient funds to cover the transaction, resulting in an insufficient funds charge by their account provider.

- **Denial of credit or loan applications:** Lenders increasingly incorporate consumer-permissioned information into their underwriting practices, including historical transactions, balances, and recurring payments, that are otherwise not reported to credit bureaus. If a consumer is unable to access and share that information with a third party lender, then that lender may reject that consumer's application.

- **Exposure to increased fraud when initiating transactions:** The consumer's inability to verify information about payment recipients puts them at higher risk of falling victim to a fraudulent transfer. (See our response to Q25 for details on the usefulness of sharing bill pay information to verify the payment counterparty.)

Appendix B: Data elements not covered in this Proposal that consumers currently access via authorized third parties

The below data categories and illustrative data elements are ones accessed and shared by consumers and that might be put at risk if the Proposal does not expand its scope of coverage:

Investments/Brokerage/Retirement accounts:

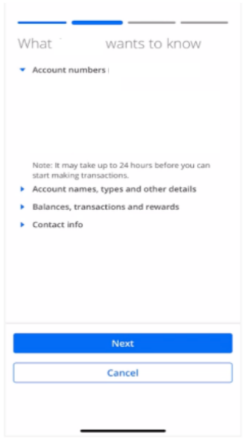
- Holdings
- Holdings information for Stocks, equities, mutual funds, index funds, crypto, NFTs, Bonds, Cash, options, margin, etc.
- Name, identifiers (CUSIP, ISIN)
- Quantity
- Cost basis
- 2 years of investment transaction types (buy, sell, splits, dividends, reinvestments, send, receive, fees, etc.)
- Current and available balance
- Account type (i.e., 401, HSA, Roth IRA, Traditional IRA, etc)
- Tax lots
- Security hold time
- Security exchange (i.e., NYSE, NASDAQ, etc.)
    i. Sell strategy (FIFO, LIFO, HIFO)
    ii. All investment transaction types (buy, sell, splits, dividends, reinvestments, send, receive, fees, etc.)
    iii. Account and routing numbers for brokerages
    iv. Regular recurring purchases (i.e., daily recurring buys on Robinhood)
    v. Brokerage open date
- Liabilities accounts (auto, mortgage, personal)
    i. Loan types: Student Loan, Mortgage, Auto loans, Personal loans, BNPL, Medical loans, Payday loans, HELOC, second mortgage, home equity loans
    ii. APR (APR %, APR Type, interest_charge_amount)
    iii. Loan details
    iv. Principle amount
    v. Interest amount
    vi. Fees
    vii. Payment details
    viii. Last payment details
    ix. Last payment date
    x. Min payment
    xi. Next payment date
    xii. Escrow balance

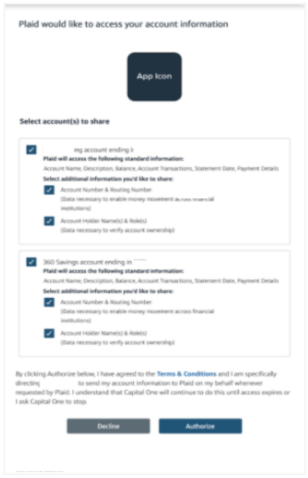
xiii. Prepayment penalty
xiv. Loan type
xv. Loan payoff details
xvi. Amount
xvii. Instructions
xviii. PSLF info
xix. Repayment plan for student loans
xx. Escrow information for mortgages

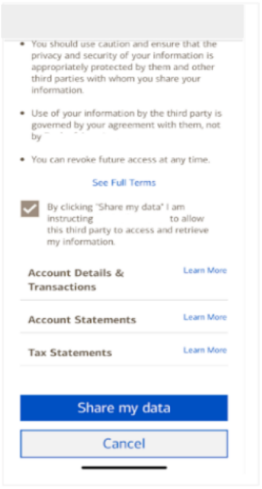
- Payroll information
  i. Gross and net income
  ii. Hours worked
  iii. Pay frequency
  iv. Start date/ end date
  v. Employment status
  vi. Tax withholdings

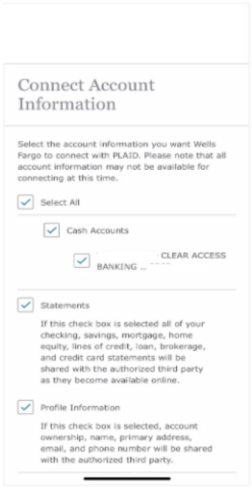
Appendix C: Data Provider Permissioning Experiences

See below for examples of disparate permissioning experiences across data providers who currently serve third-party access portals.



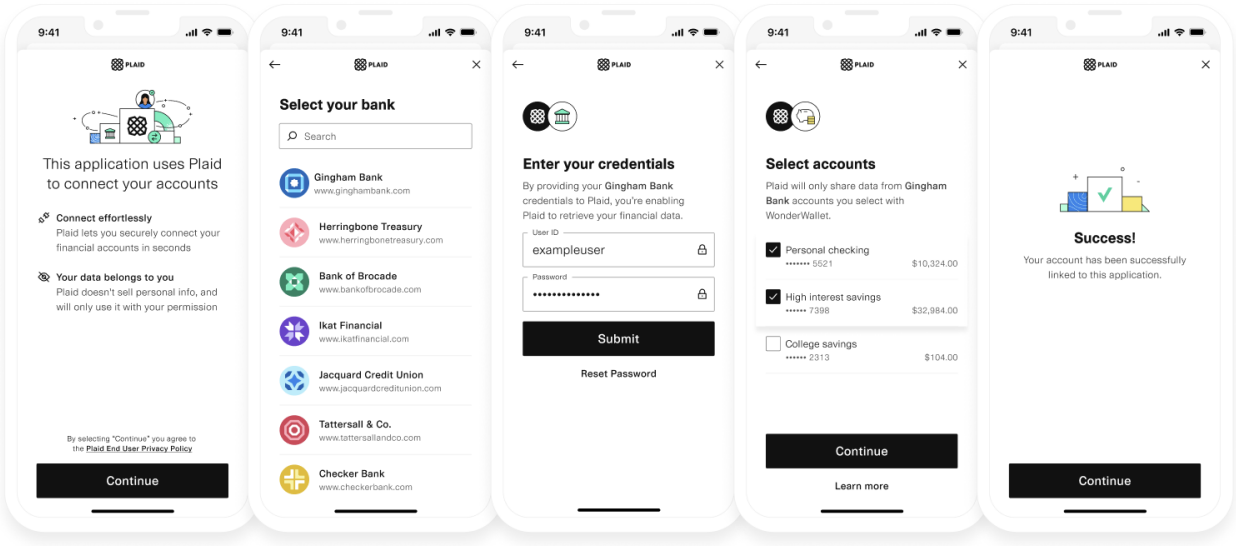






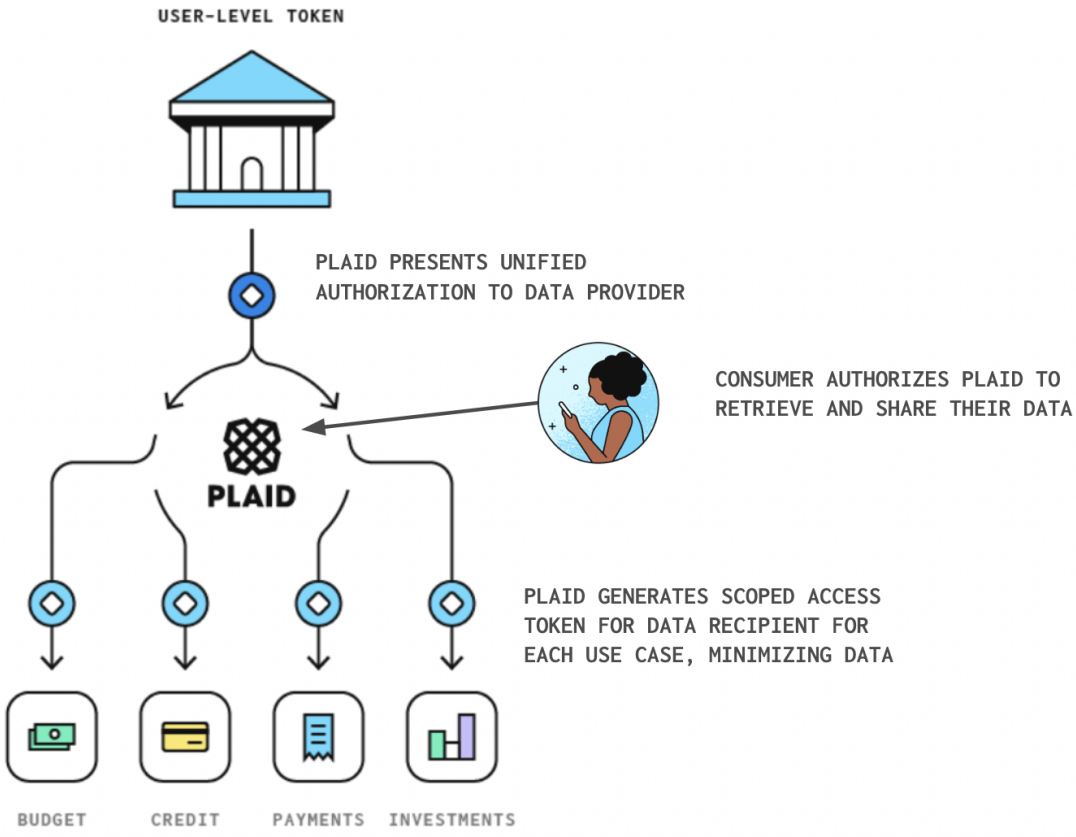
Appendix D: Example of Plaid's Account Linking Experience

The below is an example of screens consumers could see while connecting their financial accounts via Plaid.



Appendix E: Traffic management via a data aggregator

The below visual depicts a scenario in which a consumer authorizes multiple data recipients via the same third-party data aggregator to collect data from their data provider. The data aggregator can collectively present the individual authorizations to the data provider, fulfilling its requirements, and then gather the same data and pass it downstream to its multiple data recipient clients. This saves the data provider from having to share multiple copies of the same information, cutting the costs of serving authorized data requests.



Appendix G: Example of Plaid Portal