December 29, 2023
The Honorable Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

SENT VIA ELECTRONIC MAIL TO 2023-NPRM-Data-Rights@cfpb.gov

Re: 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") Notice of Proposed Rulemaking ("NPRM" or "proposal" or "proposed rule") for the Required Rulemaking on Personal Financial Data Rights.

Plaid's mission, as a data aggregator[1] and third party, is to unlock financial freedom for everyone. By allowing consumers to safely and securely share their own financial data from the institutions with which they bank (data providers) with their chosen digital finance apps and services (third parties), Plaid accelerates greater choice and competition in the financial services marketplace – all of which furthers the CFPB's aims of opening and decentralizing this market and positioning consumers to benefit from lower switching costs to access to the best, most innovative financial products and services.

Plaid provides technology that allows for safe, secure, and reliable consumer-driven data sharing to over 8,000 authorized third party customers – which, in turn, provide critical financial products and services to millions of consumers. The diversity of the consumers being served is reflected in the diversity of Plaid's customer base, which includes national, regional, and community banks, credit unions, and large and small for-profit and nonprofit digital financial service providers. As part of our efforts to promote safety, security, and consumer control in the open finance ecosystem, we have signed data access agreements with many of the largest data providers (both banks and nonbanks), as well as medium and small data providers. As a result, today, nearly 75% of the data access facilitated by Plaid is exclusively on or committed to application programming interfaces ("APIs" or "developer interfaces").[2] Plaid actively participates in technical standards development with the Financial Data Exchange ("FDX"), with the goal of creating a single API standard for the United States, making it easier, cheaper, and

[1] Plaid uses "data aggregator" here as that is the term used in the NPRM. On page 5 we propose that the final rule instead adopt the term "data access platform." Plaid uses the term data access platform throughout the remainder of this comment.

[2] "Committed to" means that Plaid and the data provider have agreed to migrate all access to an API and are in the process of that migration but may not have yet completed it.

safer for consumers to benefit from financial data portability regardless of what financial service provider they use.

Consumer demand, technological innovation, and industry dynamics (both competition and collaboration) have led to significant advances in the United States open finance ecosystem, with hundreds of millions of consumers able to access and share their own financial information so that they can easily use their chosen services. 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. In particular, the NPRM's emphasis on fair and free consumer and third party access to data providers' developer interfaces, effective and transparent authorization managed by third parties, and the role Standard Setting Organizations ("SSO") can play in implementing data access at a technical level will, if finalized, dramatically improve data portability, competition, and consumer outcomes.

Plaid thanks the Bureau for its effort to secure financial data rights for consumers and respectfully calls attention to the following five areas that require further clarification or revision to achieve the goals of § 1033 and to prevent the Bureau from inadvertently undermining the very aims of the rulemaking – namely, to shift control to consumers, and to promote fair, transparent, and competitive marketplace that improves consumer access to better, more cost effective products and services of their choice:

- **The proposed implementation timeframes should be adjusted to avoid putting existing consumer account connections and consumers' statutory portability right at risk:** Plaid supports the Bureau's proposed developer interface mandate and the safe, secure, and reliable access it will provide to consumers. As detailed below, standing up a developer interface, and migrating and onboarding third parties to the interface, creates a risk of breaking consumers' existing connections (on which they currently rely to receive necessary and desired financial services) and limiting their ability to readily access their own data. We make a number of recommendations to mitigate these risks to consumers and encourage the Bureau to monitor the market throughout the implementation period to ensure that no covered entity reduces or eliminates currently-available data access or fails to satisfy the full scope of portability mandated by § 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

- **The proposed standards for authentication and authorization should be refined to eliminate unproductive friction and enhance consumer choice:** The Bureau correctly recognizes that third parties should be solely responsible for authorization because the consumer is *authorizing the third party to collect* financial information on their behalf, rather than *authorizing a data provider to send* information. We recommend a number of refinements to reduce unnecessary content

and redirects from data providers that may confuse or overwhelm consumers and to push the industry to improve its authentication and authorization methods so that consumers can have an increasingly successful, safe, and secure experience.

- **The proposed data privacy protections require revision to avoid undermining consumer choice and comprehension, interfering with anti-fraud efforts and innovative product development, and further entrenching incumbents**: Plaid applauds the Bureau's efforts to promote consumers' data privacy. However, restricting third parties' collection, use, and retention of covered data to only that "reasonably necessary" to provide a consumer's requested product or service denies consumers meaningful control over their data and many of the benefits third parties can provide. For example, the proposal's ambiguity means consumers may not be able to reliably count on third parties to perform commonplace and beneficial activities such as fraud prevention, troubleshooting, and product improvement. In addition, the innovation and competition the rule aims to promote will be stifled by the Bureau's proposed approach, particularly given that incumbent data providers are not subject to any of the rule's proposed protections and will be able to liberally market, cross-sell, and otherwise leverage their knowledge of which third party services their consumers are using. To avoid these problematic results, we recommend that the Bureau acknowledge common and beneficial activities as reasonably necessary for the collection, use, and retention of data, recognize that there are secondary purposes for the use of data that benefit consumers and the open finance ecosystem, and permit secondary use of data so long as there are notice and opt-out or opt-in safeguards in place to ensure consumer understanding and control.

- **The proposed approach to interface access requires clarification to avoid burden, inefficiency, inconsistency, and consumer frustration:** A straightforward process with clear expectations for third parties (and their consumers) to obtain developer interface access will enable growth of the open finance ecosystem, with the expected benefits for consumers. The current proposal will not accomplish this goal, however, as data providers will construe it as giving them discretion to grant or deny access based on purported "risk management concerns." This means that thousands of data providers, which are already inherently conflicted by the fact that they are competing with third parties for business, will apply thousands of different risk management standards in determining whether to grant or deny access. The Bureau's admonition against inconsistent and discriminatory denials of access is not sufficient to prevent conflicting or pretextual (anticompetitive) denials. Given the extensive proposed regulatory obligations on third parties, and the fact that a consumer has already made an informed decision to do business with a particular third party prior to the time of an access request, the Bureau should itself certify third parties for access and make clear that, with such a certification, access cannot be denied. If the Bureau opts not to do this, it should clarify that a third party's attestation that it maintains adequate security to safeguard consumer data is sufficient "evidence" to gain interface access and that the

burden is on a data provider to to meet a high bar in order to thereafter deny such a request, which can only happen in certain limited circumstances. We also recommend that the Bureau declare that efforts to interfere with consumers' data rights are a violation of the law and strengthen other parts of the proposal designed to prevent data providers from disrupting or interfering with access in other ways.

- **The proposal should clarify the Bureau's interest in enforcement of § 1033:** Although § 1033 is designed to benefit consumers, the impacts of non-compliance are more likely to be seen by third parties than individuals who are seeking financial services. Compliance with the final rule will be substantially bolstered by the Bureau stating that failure to meet the obligations under the rule is a violation of law, and that it will consider the complaints of industry participants when setting supervision and enforcement priorities. We recommend a number of transparency mechanisms that will help industry participants to identify and bring attention to non-compliance and that will incentivize compliance.

Plaid discusses each of these recommendations in greater detail below, as well as additional clarifications or modifications the Bureau should make to achieve the rulemaking's aims.

PLAID

Table Of Contents

I. Plaid's Role In The Open Finance Ecosystem

Plaid was founded in 2013 to solve a deep problem in financial services: lack of consumer choice left many consumers stuck with few options, and some consumers with no access to financial services at all. In theory, consumers should be able to easily switch financial service providers if the one they use does not have a product they need, or offers worse terms than other financial service providers. In reality, a consumer's incumbent financial institution has a number of advantages that make switching hard. First among these advantages is a technological and practical monopoly on the consumer's financial data and transactional records. Exclusive access to a consumer's financial history, often years of it, gives an incumbent a substantial advantage when it comes to pricing products, offering new ones, and personalizing services. Consumers may also be hesitant to switch, not wanting to lose their entire financial history when moving to a new financial service provider.

This is the problem that Plaid helps solve. By building technology that makes it easy for a consumer to safely, securely, and digitally access and share their financial data with any financial service provider they want, Plaid and similar companies help remove one of the largest barriers to a consumer shopping for, or switching to, a new financial service provider. Plaid and companies like it also enable third-party financial services companies to focus on their consumer products and services without having to dedicate significant time and resources to creating safe and secure methods to access and receive consumers' data, or negotiate for data access with traditional financial institutions. As a result, innovation and competition in financial services have exploded in the last ten years. Today:

- Plaid supports more than 8,000 third-party financial services companies (our customers), increasing competition and choice in financial services for consumers.
- Plaid allows consumers to share their data from more than 12,000 data providers.
- More than 1 in 3 consumers in the United States have used third-party financial services companies that rely upon Plaid to enable them to access and share their financial data.
- Plaid's data access platform is increasingly bi-directional. Three of the country's five largest traditional financial institutions, in addition to being data providers, use Plaid as third parties to improve their offerings to consumers.
- Financial technology companies ("fintechs"), such as digital wallets, are also increasingly important data providers on Plaid's platform. Of the 20 data providers from which consumers most frequently access and share their financial data, five of them are non-banks.
- 75% of the data access and portability on Plaid's platform currently relies on or is committed to API access that does not require the consumer to share their login credentials with third parties.
- The Financial Data Exchange ("FDX"), of which Plaid is a board member, has developed a common, interoperable and royalty-free technical standard for consumer-permissioned financial data sharing, and which currently supports financial data access for more than 65 million accounts in the US and Canada.

- Plaid has partnered with digital banking platforms and core service providers to make data access APIs available to over 7,000 community banks and credit unions.[3]

The Bureau's NPRM, if finalized, will secure and improve upon the consumer benefits that many third parties have fostered over the past ten years. Despite significant progress, including some data providers responding to consumers' demand for the ability to choose and use third-party financial services, absent a strong § 1033 rule too many consumers will continue to have their data trapped by certain financial service providers that actively block or hinder consumer attempts to share their data with third parties or only allow consumers to share limited data with third parties. And too many consumers have to use their login credentials in order to access and share their data with third parties to get the financial services they are seeking, all because their data provider has either created anticompetitive barriers to a third party accessing their developer interface or has otherwise been unwilling to create a developer interface that would allow third parties to access consumer-permissioned data more safely. The market has advanced consumer access rights as far as it can; regulation is needed to fully and consistently secure them.

II. Definitions (§ 1033.131)

A. The Bureau Should Use The Term "Data Access Platform" Instead Of The Term "Data Aggregator"

The NPRM's definition of "data aggregator" does not fully reflect the role that companies like Plaid play in the open finance ecosystem. While some companies only "enable access to covered data" on behalf of a third party, others do much more to benefit consumers and further their control and understanding, in line with the CFPB's aims. Plaid permits consumers to control their financial data by authorizing, or revoking, access to apps and services they have chosen. Plaid facilitates consumer-centric data practices by providing clear disclosures to consumers, promoting data minimization (i.e., ensuring Plaid and authorized third parties only collect data required for their product or service), and contractually requiring third parties to use consumer data only in accordance with the consumer's consent and applicable laws. Plaid also contractually requires third parties to delete consumer data upon the consumer's request, to protect consumer data with an information security program aligned to industry standards and best practices, to comply with laws and regulations applicable to their data handling (such as the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule), and to avoid engaging in the sale or rental of consumer data for things like marketing or behavioral targeting. Plaid has also developed products that allow consumers to get the benefits of data portability without having to share their underlying data (for example, by using tokenized account numbers that allow consumers to initiate payments without sharing their raw account numbers). Plaid also works extensively with data providers to manage and minimize data request volumes, troubleshoot problems with their

[3] Plaid is not acting as a developer interface in these partnerships. Once the core or digital banking platform has that API in place, any third party can connect to it without Plaid's involvement or knowledge, and without the data ever flowing through Plaid.

developer interfaces, and provide alerts on potential fraud and security issues. These value-added services beyond mere data access and transmission advance a safe, secure, and reliable open finance ecosystem that other market participants have not had an incentive to build.

Using the term "data aggregator" also risks confusion, as the term refers to companies outside of financial services and to companies that collect and sell data without consumer authorization. **The CFPB should define companies that manage financial data access under § 1033 as "data access platforms," a term that encompasses these companies' full set of services and disambiguates them from data brokers and other aggregators that act without consumer consent and authorization.** "Data access platform" is the terminology adopted by the Financial Data Exchange and used by its members, including the largest financial service providers in the United States. Using this market standard term will add clarity to the final rule.

B. The Bureau Should Revert To The Statutory Definition Of "Consumer" And Address Any Concerns In A More Targeted Manner

The Bureau's final rule should revert to the statutory definition of "consumer," rather than the modified version offered in the NPRM. Congress defined "consumer" to mean "an individual or an agent, trustee, or representative acting on behalf of an individual" when it created the CFPB.[4] The NPRM instead defines "consumer" as "a natural person." As an initial matter, it is unclear that the Bureau has the authority to redefine "consumer." The proposed definition will also define "consumer" differently under the § 1033 rule than in the rest of Title X, risking confusion and unintended consequences. The Bureau has other less disruptive ways to distinguish between an individual "consumer" and a "third party." For example, the Bureau could update the definition of "third party" to mean:

> any person or entity that is not **the natural person** about whom the covered data pertains or the data provider **or its developer interface service provider** that controls or possesses the consumer's covered data.

This approach avoids inadvertently interfering with personal financial management arrangements that are not addressed in this rulemaking, retains the clarity that a consumer has the right to authorize access on their own behalf, and is consistent with the concept that the "third party" under the rule is separate from the consumer and is only accessing data with consumer authorization. The connection between consumer authorization and data access is fundamental to the proposed rule, and the Bureau should not undermine it by stripping this relationship out of the definition of "consumer."

[4] 12 U.S.C. § 5481(4).

C. The Bureau Should Add "Developer Interface Service Provider" As A Defined Term And Clarify Its Obligations Under The Rule

In its Preamble, the Bureau makes clear that a data provider may either build its own developer interface or may contract with a service provider for a developer interface, but the rule itself does not directly address the latter approach. To the extent data providers choose the latter approach, the final rule should make clear both (i) the obligations of those service providers and (ii) the obligations of data providers with respect to such service providers.

Clarification is needed to ensure that service providers, which are contracted to build or maintain a data provider's developer interface, are subject to all the same requirements applicable to data providers, and that data providers are accountable for any non-compliance by those service providers. This will protect against incumbent data providers using contracted service providers as a means to end-run the CFPB's prohibitions on charging for access and data,[5] access requirements, performance standards and other requirements. Clarification would also address a current practice that interferes with data access: requirements for third parties to enter into separate contractual agreements with both a data provider and with the service provider providing its developer interface. The NPRM recognizes that some third parties and data providers may choose to contract with one another regarding terms of access to the extent there are benefits to doing so, but the Bureau also makes clear that such agreements are not a prerequisite to the access required under the rule. If the requirements for data providers and developer interfaces are fully concurrent, then there is no basis for a requirement that third parties must reach an agreement with a developer interface service provider for access.

In addition, the Bureau recognizes that, with respect to developer interfaces, "small institutions tend to rely on a few core service providers, and frequently report problems with the services that 'cores' offer."[6] Making clear that developer interface service providers are subject to the data provider requirements – and that the data providers engaging such service providers remain accountable – should help address the Bureau's concern.

Finally, clarification would address risks associated with entities attempting to act as both service providers (providing a developer interface) *and* data access platforms. One risk of an

[5] As one commenter has already noted, "if [an] aggregator is the only option for obtaining the information from a specific data provider . . . it could be problematic for the aggregator to charge fees." (Letter from U.S. Bank National Association to The Consumer Financial Protection Bureau, December 27, 2023.) We agree that it would be problematic for one company to have a monopoly on access to a data provider, with no other third party permitted to connect to that data provider, particularly if that company leveraged its forced monopoly position to charge fees that were not subject to competition. This is why the requirement that *any* third party be able to access a data provider's developer interface is such a critical part of the proposed rule. It is also why our proposal above regarding "developer interface service providers" is necessary to ensure that any entities acting as such service providers are not positioned to have monopoly access or control.

[6] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74798, (proposed Oct. 31, 2023).

entity playing both roles is that the prohibition against charging for data could be evaded by disguising costs data providers are expected to bear under the rule as "connectivity costs" charged by data access platforms to third parties, which would allow incumbents to make it harder for new entrants to compete. Another risk is that such an entity could use competitively sensitive information it learns about third parties in its capacity as a service provider in order to unfairly compete when acting in its capacity as a data access platform. Clarifying the restrictions imposed upon developer interface service providers can mitigate these concerns.

Plaid therefore recommends the inclusion of the following definitions and regulatory text.

- **Add "developer interface service provider" as a defined term**: Plaid proposes that the term developer interface service provider shall mean:

  > **an entity engaged by a data provider to build and/or maintain its developer interface.**

- **Clarify that a developer interface service provider is subject to the same requirements as the data provider that retained it, and that the data provider is accountable for its compliance**: Plaid proposes the addition of the following text within Subpart C, § 1033.311:

  > **(e) *Use of a developer interface service provider*. To the extent a data provider elects to comply with the obligations contained in Subparts B and C of this rule, whether in whole or in part, through its use of a developer interface service provider,**
  >
  > **(i) such developer interface service provider may not impose any conditions or restrictions on interface access that the data provider itself could not impose, and must comply with the provisions set forth in this rule regarding developer interfaces, including without limitation the requirements set forth in § 1033.301 and § 1033.311;**
  >
  > **(ii) such data provider must ensure its developer interface service provider complies with the provisions set forth in this rule regarding developer interfaces, including without limitation the requirements set forth in § 1033.301 and § 1033.311;**
  >
  > **(iii) such data provider and/or developer interface service provider may not require any third party to contract with a developer interface service provider as a condition of access; and**
  >
  > **(iv) such data provider shall be prohibited from disclosing information about third parties to its developer interface service provider except as is necessary for the developer**

interface service provider to build and maintain the developer interface; such developer interface service provider shall be prohibited from using any information about third parties except as is necessary for it to build and maintain the developer interface.

III. Compliance Dates And Standard Setting (§§ 1033.121, .141)

A. The Bureau Should Mandate Developer Interfaces, While Allowing A Smooth Migration From Legacy Screen Scraping To Those Interfaces

1. The Bureau Should Allow Additional Flexibility Beyond The Initial Six-Month Implementation Deadline

The CFPB has set necessary deadlines for data providers to make their developer interfaces available to third parties. The developer interface is the heart of this rulemaking, making data portability easier and more consistent, while eliminating screen scraping and credentials-based access.[7] In the absence of this regulatory requirement, very few data providers have built or otherwise stood up developer interfaces – despite their claims that the elimination of screen scraping is one of their top priorities.

In its SBREFA comment, The Clearing House articulated the industry's often-stated opposition to screen scraping and argued that "[t]he ban on screen scraping should go beyond the narrow definition of 'covered accounts' and encompass the practice in its entirety."[8] Absent any initiative by data providers to stand up developer interfaces, however, their calls for a screen scraping ban amount to calls for a ban on consumers being able to authorize third parties to access their data. Today, five years after JPMorgan Chase and Plaid agreed to switch to APIs for data access,[9] and over a year since JPMorgan Chase announced that it had fully eliminated screen scraping,[10] several of the 22 owner banks of The Clearing House – the largest banks with a highly concentrated percentage of overall consumer accounts in the United States – still do not have a developer interface. By contrast, in that same time, more than 140 fintechs have built

[7] To provide consumers with critical access to their own data, third parties like Plaid use credentials-based access when data providers lack a developer interface or refuse to make it available absent anticompetitive conditions or when third parties have not yet been able to negotiate a data access agreement.

[8] The Clearing House, *Comment Letter on Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights*, Jan. 24, 2023, available at www.regulations.gov/comment/CFPB-2023-0011-0043.

[9] Sima Gandhi, *Safe, convenient, and reliable data access for consumers*, Plaid, Oct. 22, 2018, available at plaid.com/blog/chase/.

[10] Miriam Cross, *JPMorgan Chase says it has fully eliminated screen scraping*, American Banker, Oct. 6, 2022, available at www.americanbanker.com/news/jpmorgan-chase-says-it-has-fully-eliminated-screen-scraping.

developer interfaces to allow their consumers to access and share their data. The market is enthusiastic to use developer interfaces, which offer higher quality data and better performance than data obtained by screen scraping, but for this to be realized, the majority of data providers still need to stand them up.

Yet as necessary as these deadlines are to force action, the Bureau should strongly consider additional flexibility, particularly to the 6 and 12 month deadlines. Many of the largest banks have invested significant resources into developing and deploying APIs, but these banks will need to modify their interfaces to comply with the rule. For some banks, conforming those APIs to a Qualified Industry Standard will require *significant* modification. While we are supportive of an expedient timeline for data providers to make available developer interfaces compliant with the rule, we recognize that this process may take more time than presently allotted under the CFPB's proposal. So that data providers have sufficient time to ensure, including through testing, that their developer interfaces comply with the rule's requirements and are otherwise fully functional and able to support volumes of traffic, Plaid believes **it is reasonable for the largest data providers – bank and non-bank – to be given 12 months to comply, with the next cohort of data providers to be given 18 months.** At the same time, because API implementations have gotten faster and less expensive over the last 5 years as data formats have standardized and data providers and third parties have gained more experience implementing APIs, the Bureau should expect costs and implementation times to continue to fall. Given these dynamics, it is also reasonable to extend compliance to 3 years for the third cohort of data providers, while maintaining a 4 year deadline for the remaining data providers.

2. The CFPB Should Allow Third Parties To Continue To Access Consumers' Data While Data Providers Work To Fully Implement And Migrate Traffic To Compliant Developer Interfaces

The NPRM wisely recognizes that consumers should benefit from being able to access and share their data, even as data providers work to implement compliant developer interfaces. The Consumer Bankers Association SBREFA comment has the dynamic right: "The Bureau's Section 1033 rule should work to eliminate the practice by prohibiting third parties from attempting to screen scrape *any information a data provider makes available via an API*."[11] (Emphasis added.) While screen scraping is not Plaid's preferred method of access, it is still essential to support the data access rights of tens of millions of consumers whose data providers do not yet have or make available developer interfaces. And it will continue to be essential until every data provider maintains and makes accessible a compliant developer interface. The CFPB's flexible approach, setting firm deadlines for the implementation of developer interfaces and permitting screen scraping until those interfaces are in place, minimizes consumer harm during this critical transition. If, for whatever reason, the final rule prohibits screen scraping before developer

[11] Consumer Bankers Association, *Comment Letter on Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights*, Jan. 25, 2023, available at www.regulations.gov/comment/CFPB-2023-0011-0011.

interfaces are in place, the CFPB should maintain or even accelerate the compliance timelines for making developer interfaces available.

The CFPB should, however, give data providers a transition period after their compliance date to migrate traffic from existing access methods to their developer interfaces. Such migrations can take several months, and typically involve significant technical testing and effort.[12] During this time it is essential to avoid harmful disruptions to consumers' existing data sharing with third parties. While the ideal migration approach would preserve existing connections, our experience has been that data providers do not build APIs capable of managing a seamless migration. Instead, often, a problematic element of transitioning from screen scraping to a developer interface involves deprecating healthy connections which consumers have previously created and are actively using. This often means that the consumer must return to the third party and re-complete the signup and authorization process, usually leveraging a data access platform again. In order to reduce sudden surges in volume to the data provider's new developer interface, as well as to minimize logistical challenges and unintended disruptions in service, data providers generally work with data access platforms and third parties to gradually transition groups of consumers in an orderly and sequenced fashion.

During this migration process, it is critical that the legacy access method, including screen scraping, remains functional and reliable, both as a primary means of access for consumers who have not yet been migrated, and as a backup access method in the event of a developer interface error during testing. It is common for critical bugs and other issues to be discovered during the initial migration to the developer interface, and in most cases one or more third parties will need to be temporarily reverted back to the legacy access method in order to prevent severe disruptions to their service while the issue is being fixed. **The CFPB should ensure that consumer access is maintained during migrations by requiring data providers, data access platforms, and third parties to manage them in a manner that minimizes the risk of a broken connection and the burden on consumers.**

[12] Today, when data providers and third parties transition to an API for access: 1. Third parties must test whether the data provider's API can support the traffic required to fulfill the use cases and data access requirements of their consumers. It often takes multiple months for data providers to ensure that their servers are sufficient to reliably serve this traffic, particularly when the API solution is initially launched and has not yet been properly stress tested in production. 2. Data providers must ensure that they have properly allowlisted third party requests to the data providers' APIs to avoid inadvertently blocking legitimate traffic due to mis-applied rate limiting, bot detection services, or other defenses. 3. If a third party is redirecting the consumer to the data provider through an OAuth consent experience so that the data provider can "confirm" the consumer's authorization, that redirect requires extensive testing and monitoring to ensure that it is compatible with the different devices, operating systems, and web browsers that consumers will use during the authorization process. 4. The data provider and third party devote significant time and effort to ensure that the API has been properly implemented and is returning data as expected prior to relying on it at scale. It is common for various bugs and edge cases to be uncovered in an API integration, which need to be addressed before all consumer access is moved to the API.

The final rule should explicitly recognize the complexity of implementation by requiring data providers to:

- **have compliant developer interfaces available by the proposed compliance deadlines;**
- **gradually migrate access from existing access methods to their developer interfaces on commercially reasonable timelines, ideally without breaking existing connections, after the interfaces are made available; and**
- **continue to invest in and support high quality data access outside of their developer interfaces, including supporting screen scraping integrations, until all access is migrated to a compliant developer interface.**

B. The Bureau Should Name An SSO To Ensure A Clear And Consistent Qualified Industry Standard

The Bureau can ease some of the challenges identified above related to the transition to developer interfaces by naming a SSO or multiple SSOs well ahead of the first compliance deadline.

Most data providers will be hesitant to build to *any* standard if they do not believe it will be a Qualified Industry Standard ("QIS") that is deemed to comply with the rule's format standardization requirements and which has the indicia of compliance with other requirements in the rule. Data providers may find themselves in a bind, whereby they have limited time to build a developer interface without assurance that the standard they are building to will be recognized by the CFPB. This may cause them to delay initiating their build in the hopes that the CFPB will identify an SSO, at which point they may rush to release it ahead of the deadline without appropriate testing or assurances that it will meet performance requirements.

The "fallback" provision in § 1033.311(b)(2) is not adequate to protect against this risk. As written, it only applies if no SSO meets the Bureau's requirements. If a data provider creates a developer interface using one standard, only to find that another standard is later deemed to be a QIS, that data provider will lose the benefit of § 1033.311(b)(2) and will need to replace its developer interface with another one, a wasteful and potentially expensive process. **The CFPB can avoid these problems, and incentivize faster deployment of developer interfaces and the increased quality and consumer protection they bring, by naming an SSO as soon as is practicable, ideally well ahead of the final rule.**

FDX has the most widely adopted API schema in the United States. Data providers using the FDX standard run developer interfaces providing access to more than 65 million accounts.[13] Plaid is a member of the FDX Board of Directors, has actively contributed to the development of

[13] This significant achievement demonstrates the quality of the FDX API schema. However, the CFPB should bear in mind that these 65 million accounts are overwhelmingly concentrated at a handful of the largest banks in the country.

its API schema, and believes it is well positioned to help the transition to open finance as a CFPB-recognized SSO. Because the FDX API was developed in the absence of regulatory requirements and, as a result, does not fully align with the NPRM, FDX will need to update its API to comply with the final rule. FDX could potentially accelerate a release to conform to the rule shortly after it is finalized, which will allow the largest banks relying on the FDX API to modify or adapt their developer interfaces to conform to the rule, while meeting their compliance deadlines. **In the event FDX or another SSO is not selected ahead of the final rule, it will be critical for the CFPB itself to be more prescriptive on a number of issues that the proposed rule leaves to an SSO; otherwise, market participants will face substantial uncertainty on how to comply with the rule, delaying its implementation and potentially harming consumers.**

IV. Obligation To Make Covered Data Available (Subpart B)

Establishing a standard scope of accounts and data elements that a consumer must be able to access will materially benefit consumers, who today face an uncertain landscape where the accounts and data they can authorize third parties to access often differ from data provider to data provider. Consumers' data portability rights under § 1033 should be consistent regardless of which data provider they use. That consistency ensures consumers can reap the benefits of true data portability, while also protecting competition. In particular, a strong rule on covered data will ensure that (i) no financial institution is able to avail itself of the benefits of data access as a third party, while simultaneously depriving other third parties of equal access when acting as a data provider, and (ii) no institution is able to use its incumbent bargaining power when acting as a third party to gain access to more or better data than other competing third parties. The NPRM provides a solid foundation for that consistency, but the Bureau should provide even more detail and clarity in the final rule.

A. The Bureau Should Specifically Enumerate Additional Types of Covered Data

The Bureau should consider listing more examples of covered data, or providing more expansive language, to ensure that the listed data fields in the NPRM are not narrowly interpreted by data providers in a way that limits consumer access. For example, when a consumer wants to access and share their account balance, they should also know whether that balance number is in dollars, pounds, or euros; absent that context, the number returned may not be useful to a consumer or a third party. Yet certain data providers have argued against this specific information being a necessary field, and without more granularity or broader language from the Bureau, a data provider might build a developer interface that excludes it. As a point of comparison, the FDX API schema lists 2,196 distinct data elements.[14] (See Appendix 1.)

[14] The Bureau should be aware that there is a real likelihood of continued disagreement among data providers and third parties about what data is needed and should be covered. A potential SSO identifying and listing possible data elements does not mean that the Bureau can rely on an SSO to determine what

B. The Bureau Should Clarify The Rule's Applicability To Covered Data Held By Data Providers Potentially Outside The Rule's Scope

The Bureau should clarify consumer data rights when an account is the same type of product as, or competes directly with, accounts subject to Regulation E, but the data provider is potentially outside the scope of the Bureau's jurisdiction. For example, many brokerage firms have deposit accounts covered by Regulation E, but these companies may argue that they are excluded from the Bureau's jurisdiction under 12 U.S.C. § 5517(i). These brokerage firms may also rely on underlying depository accounts at banks, which are clearly covered by the proposed rule, to hold consumer funds, and may even issue debit cards connected to these accounts. Consumers reasonably expect that a rule covering Regulation E accounts and products in fact covers all Regulation E accounts and products. The Dodd Frank Act's requirement that the Securities and Exchange Commission and the Bureau consult and coordinate on rulemakings for a consumer financial product or service indicates a congressional intent not to allow differences in a primary regulator to interfere with adequate consumer financial protections. **The final rule should clarify that these data providers must make the consumer financial data that they hold available to consumers and third parties for access and sharing.**

C. The Bureau Should Specify Additional Account Types Covered By § 1033 And State That § 1033 Is Self-Executing

The proposal requires that consumers have access to and the ability to permission third parties to access Regulation E asset accounts, Regulation Z credit cards, and products or services that facilitate payments from a Regulation E account or a Regulation Z credit card. However, there is nothing in § 1033 that suggests it is limited to data from Regulation E and Regulation Z covered products. The NPRM leaves out of the rule a number of accounts that are critical to consumers' financial lives, including mortgage, auto, and student loans, as well as specialty accounts like EBT cards that are vital to the most financially vulnerable consumers. In public comments, the Bureau has downplayed the implications of the limited NPRM scope and suggested that consumers can access important loan data even if the account is not covered, for example by seeing the transaction record of their mortgage payment in a Regulation E account. But, this is not the case. While transactions data from a Regulation E account would show a mortgage payment, other essential information *would not typically appear* in the transactions data, including the term of the mortgage, the interest rate, and what portion of each payment is going to principal and interest.

The CFPB's statement that it "intends to implement CFPA section 1033 with respect to other covered persons and consumer financial products or services through supplemental rulemaking" is helpful but, absent a clear timeline and commitment to this rulemaking, Plaid is concerned that the proposed rule's narrow scope could have unintended consequences. Today, data

---

data is necessary to comply with the rule. Many of the elements in the FDX API schema are optional, and financial institutions have in fact argued against making fields used by third parties today mandatory.

providers with developer interfaces generally make mortgage, auto, and student loan data available on them, to the extent they offer those products. A final § 1033 rule with a narrower account scope could result in data providers that already have developer interfaces *removing* those accounts, *failing to maintain* those elements of their interfaces, or *charging* consumers or third parties to access that data. For the majority of data providers, which do not have developer interfaces today, the narrower account scope in the NPRM could result in them building minimally compliant interfaces that *completely omit* these accounts. **For these reasons, the Bureau should specify additional account types covered by § 1033.**

If the Bureau maintains this limited rule scope, the final rule should state that § 1033 is a self-executing statutory provision that establishes a fundamental right for consumers to access all financial data that falls within the scope of the CFPB's regulatory authority and, thus, does not require regulatory action to be enforceable. The Bureau should also issue robust commentary to set expectations for the timing of supplemental rulemakings and explain how the Bureau expects data providers to handle access to non-rule-covered data in the meantime.

D. Recommendations Regarding Specific Data Types

Identity Data

Within the accounts covered by the NPRM, the Bureau has provided a helpful starting point by enumerating certain data fields that must be made available to consumers and third parties. In particular, including name, address, phone number, and email as explicitly required data elements in § 1033.211(f) will bring significant benefits to consumers and the market. These four identity data fields are currently some of the most inconsistently available data fields across data providers. They are also essential to protecting consumers. Today, third parties use these data elements to confirm that funds are being applied to the correct account, to mitigate fraud, and to facilitate payments – particularly emerging classes of payments that use identity elements as account identifiers instead of account and routing numbers. Companies like Zelle[15] and Shopify[16] use consumers' phone numbers to create a registry, which they then map to the consumer's payment credential. The consumer then uses their phone number to initiate future payment transactions. This use case, increasingly prevalent in fintechs, banks, and bank-owned companies, is only possible when the consumer is easily able to share their phone number.

Including in the final rule identity data elements, such as email, phone number, and address, will also be critical for third parties to be able to comply with their obligations under the final rule. Third parties may need a consumer's contact information to provide the consumer with a

[15] Zelle, *How it Works*, available at www.zellepay.com/how-it-works?gclid=EAIaIQobChMIzqqFktOKgwMVYF1HAR1C3ANTEAAYAiAAEgLUFPD_BwE.

[16] Shopify, *Set up Shop Pay*, available at help.shop.app/hc/en-us/articles/360060763151-Set-up-Shop-Pay.

record of their authorization as required by § 1033.421(g). Third parties, including data access platforms, also need this information to verify identity or locate information when a consumer contacts them to request assistance with their data or seeks to resolve a data accuracy question. Plaid encourages the Bureau to clarify the appropriateness of sharing identity data elements by also making explicit in the final rule that using consumer data to comply with the requirements of this rule, respond to consumer requests or complaints, or troubleshoot issues with the consumer or between data providers, data access platforms, and third parties, is a reasonably necessary purpose for collection, even if the data is not necessary to deliver the specific product that the consumer requested.[17]

Social Security And Driver's License Numbers

The Bureau's approach to a consumer's Social Security and driver's license numbers is also sensible. These data elements are not widely available in the market today and are particularly sensitive personal information. By keeping these data fields optional, the Bureau has left room for the market to continue to develop use cases and best practices around these data elements, and for data providers and third parties to create norms around their access and use in bilateral agreements. The Bureau should specify in the final rule that these two data elements, while optional, should be made available without charge as with covered data when the data provider elects to make them available.

Tokenized Account Number

The Bureau should also ensure that the final § 1033 rule reinforces pro-consumer and pro-competition payment developments, such as pay-by-bank functionality. Consumers in the United States increasingly are interested in having the option to pay-by-bank, with 86% of consumers seeing the benefits of having the option to pay-by-bank and 67% of consumers (72% of millennial consumers) open to using pay-by-bank even when credit and debit card options are available.[18] Despite this interest, the United States is far behind other countries on pay-by-bank availability and consumer adoption of this safe and inexpensive payment rail. Pix in Brazil has gone from 1,442,212,000 monthly transactions in December 2021 to 4,258,556,000 in November 2023.[19] Since India launched its Unified Payments Interface in 2016 to facilitate

[17] For example, a consumer wishing to fund a digital wallet may only need to share an account and routing number (to initiate the fund transfer) and balance (to ensure against NSF or overdraft), and not their name. Under the rule, the data provider can substitute a TAN, which the consumer does not know, for the actual account number. This means that, absent additional identity elements, if the consumer contacts a third party because they believe the balance amount provided was in error, the third party will have no way to identify the consumer who has contacted them and match that consumer to the disputed data elements.

[18] Kevin Young, *The Fintech Effect 2023: Consumer insights reveal growth opportunities ahead*, Plaid Blog, Nov. 16, 2023, available at plaid.com/blog/consumer-insights-reshaping-finance/ and Appendix 2.

[19] Pix Statistics, Banco Central Do Brasil, available at www.bcb.gov.br/en/financialstability/pixstatistics.

pay-by-bank transactions, it has grown to support over 300 million monthly active users and 2,348 transactions per second.[20] [21] And in 2022 the European Union moved to mandate that banks make pay-by-bank available at costs equal to or below the cost of credit and debit card payments.[22]

The competition benefits of pay-by-bank functionality are also clear. Cards are expensive for small businesses.[23] The ability to accept cheaper pay-by-bank payments will put pressure on other payment rails to reduce their prices. There is already a well-established market of consumers using access to their account information to facilitate payments – today more than 50% of Plaid account connections support payments, account funding, or other money movement use cases. This will only grow as new real-time bank payment rails like The Clearing House's Real Time Payments and the Federal Reserve's FedNow gain adoption.

Consumers' access to data necessary to facilitate a bank account payment is vital to continued innovation in this space. In particular, the NPRM's approach to permit data providers to replace a consumer's account and routing number with a tokenized account number ("TAN") could greatly assist with the development of pay-by-bank functionality, provided the Bureau makes several modifications in the final rule.

The use of tokenization *for account numbers* is a novel technology. Tokenization in other contexts has been helpful in reducing fraud – credit card networks use it to great effect, for example – but generally must be implemented consistently across an entire market in order to be effective and to ensure that hundreds or thousands of inconsistent and non-interoperable approaches to tokenization do not eliminate the functionality of the product.

TANs are intended to fight one type of fraud: a bad actor taking over a consumer's account, or stealing a consumer's account and routing number and using them to initiate unauthorized transactions. TANs solve this problem in two ways. First, if a consumer's account at a third party is taken over, the TAN can be revoked so that the compromised account can no longer be used to transact until a new TAN is issued. Second, if the TAN itself is stolen, the TAN can be revoked without having to revoke all of the other TANs associated with that consumer. By contrast, if the

---

[20] Khan, Aarzu, *NPCI's Voice-Based Payment Solution Could Be a Game Changer*, Dazeinfo, July 21, 2021, available at dazeinfo.com/2021/07/21/npcis-voice-based-payment-solution-could-be-a-game-changer/.

[21] Hemant Kashyap, *Record-Breaking Numbers Of UPI In 2022 Hint At India's Maturing Digital Payments Ecosystem,* Inc 42, Jan. 6, 2023, *inc42.com/features/record-breaking-numbers-upi-2022-hint-india-maturing-digital-payments-ecosystem/*.

[22] CNBC, *'Seismic shift' in bank payments to help business and consumers, says EU*, Oct. 26, 2022, available at www.cnbc.com/2022/10/26/eu-introduces-new-rules-on-instant-bank-payments.html.

[23] Shira Ovide, *Want to help a business you love? Don't pay with a credit card*, The Washington Post, Dec. 8, 2023, available at www.washingtonpost.com/technology/2023/12/08/credit-card-fees-small-businesses/.

original account and routing number is stolen, a data provider might need to replace it, which can be time consuming for the consumer, who would need to re-share the new account number with every third party using it.

Unfortunately, TANs also create a new risk of fraud because many existing fraud monitoring programs rely on being able to tie an individual to an account number in order to detect anomalies or concerning patterns. TANs prevent this widespread and effective fraud prevention use case. To take one example, an individual with an account at Bank A with $1,000 in it could open 10 accounts at App B and simultaneously transfer $500 into each. If Bank A is using TANs, App B would receive 10 different TANs substituted for the account and routing numbers with the transfer requests and would not know that they are, in fact, transfers from the same account. After checking the balance and seeing that there are adequate funds (i.e. $1,000), App B will initiate a transaction to move $500 from 10 accounts, not realizing that it is actually trying to move $5,000 from one account that does not have those funds. While all of these ACH transactions may not ultimately clear, many faster payment and account funding use cases exist to make funds available for the consumer to use right away. With no way for the app to tie every requested transaction to the same person/account, the bad actor can spend the $5,000 and close their account at Bank A before App B is aware of the problem. All TANs have done in this instance is *shift fraud risk from the data provider to the third party*.

TANs also do not work for every use case. Generally this is because when a data provider *unilaterally* deploys its own tokenization, other parties in the open finance ecosystem – banks, fintechs, payment processors, the Federal Reserve – cannot match the token to the correct account. Consumers *cannot*, therefore, reliably use them for recurring payments, wire transfers, or remotely created checks. Also, TANs may not be recognized by every bank, or work on every bank payment system (Plaid is unaware of any TANs that currently work for Fed ACH, The Clearing House ACH, FedNow, and RTP), thus limiting consumer choice, interoperability, and competition for clearing transactions over the best, least expensive rails.[24] To date, no entity has proposed a single, interoperable approach to TANs that can be adopted by every data provider, much less one that can be used by every third party.

If the CFPB is going to permit TANs as an exception to the requirement that the data provider make account and routing number available, the final rule should contain six additional requirements:

- **First, the data provider should be required to disclose to the third party when a TAN has been substituted for the consumer's actual account and routing number.**

[24] While it is outside the scope of this rulemaking, the CFPB should examine the implications of businesses using non-interoperable TANs on consumer access to competitive services. *See, e.g.*, Interoperability, Privacy, & Security, Staff in the Office of Technology and the Bureau of Competition, Federal Trade Commission, Dec. 21, 2023, available at www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security.

- **Second, the TAN should be required to support all use cases or, failing that, should only be supplied when it works for the third party's use case. For use cases where a TAN will not work – and only for those use cases – the third party should have the option to request the account and routing number.[25]**

- **Third, the Bureau should require data providers that opt to provide a TAN to also provide a unique user identifier, to allow third parties to match individual consumers to a TAN without using any personal information as a protection against first party or friendly fraud.**

- **Fourth, a data provider should not be able to expire a TAN that was provided to a third party absent a request from that consumer or third party to expire the TAN, and the TAN should function as long as the consumer's authorization lasts. Giving the data provider the ability to unilaterally expire a TAN would, in effect, give the data provider the ability to unilaterally terminate a consumer's authorization.**

- **Fifth, third parties should, with a consumer's authorization, be able to automatically request a new TAN from the data provider through the developer interface. This will allow third parties to immediately expire and replace TANs if there is a concern of fraud or other misuse, without the consumer losing access to their service.**

- **Sixth, data providers should provide a means on their developer interfaces for third parties to create new TANs for a particular account from an existing TAN without expiring the existing TAN. This is necessary to enable third parties to perform their own authorization management functions, such as managing annual reauthorization.**

These requirements are already easily met in the marketplace; Plaid currently works with data partners to provide TANs to some third parties, though only under circumstances where a TAN fully supports the third party's use case and where Plaid is able to use the true account number to identify and prevent fraud.

Credit Card Payment Information

The Bureau requested comment on whether certain credit card payment information should be in scope in the final rule. The rule should require data providers to make available payment information from Regulation Z credit and debit cards (e.g., card number, expiration date, pin) in

[25] If the Bureau adopts this approach, it would be appropriate for the final rule to also require a new obligation on the third party to only request an account and routing number in lieu of a TAN when it reasonably believes that a TAN from that data provider will not support its use case.

order to give consumers and merchants the flexibility to pay and be paid with whatever payment method they choose. This payment information would allow third parties to tie a consumer's account and routing number to their credit or debit card and allow consumers to pay with whatever rail best fits their needs. This would greatly increase competition in payments, driving innovation and lowering costs for consumers and merchants.

Account Terms And Conditions

As it finalizes the rule, the CFPB should also consider modifying the requirement for "terms and conditions" of the account to be made available. As written, terms and conditions could be understood to mean the full document that a data provider issues to the consumer, including substantial legal terms that are neither relevant for any existing use cases nor easily transformed into a machine-readable format that can be accessed through a developer interface the same way that other covered data categories can.[26] The CFPB should identify the data elements that may be maintained in the terms and conditions (which it has already done in the proposal) and require that those elements, rather than the full terms and conditions, be made available in a machine-readable format. In doing so, the CFPB should identify other data elements that typically reside in the terms and conditions, perhaps by referencing the FDX data elements in Appendix 1, and add them to the list of data elements that a data provider is required to provide.

Proprietary Algorithms

Finally, the Bureau's examples of data excepted from the rule are sufficient and appropriate. For example, the clarification that the exception for proprietary algorithms only applies to the algorithm itself, and not to the covered data that goes into or is an output from the algorithm, appropriately balances a data provider's right to protect its trade secrets and intellectual property with a consumer's right to data access and portability. Absent this clarification, the exception could swallow the rule, as today myriad terms, conditions, rates, fees, and features of an account are the result of some proprietary algorithmic decision making by the financial institution. **The Bureau should consider further reducing data provider concerns about confidentiality by specifying that third parties are not permitted to use any of the data a consumer authorizes them to access to reverse engineer, or attempt to reverse engineer, any proprietary algorithms or other types of proprietary information owned by the data provider**. Such a prohibition could be incorporated into the data privacy protections in § 1033.421(a)(2).

V. Data Provider Interfaces; Responding To Requests (Subpart C)

Plaid applauds the CFPB for mandating the use of developer interfaces. Despite the significant consumer benefits that these interfaces provide – first and foremost eliminating the need for

[26] For example, a data provider may choose to satisfy its obligation by providing the full terms and conditions as a PDF, which is highly inefficient and also inconsistent with data minimization, as the third party may only need to know a single term.

consumers to share their login credentials, while improving data quality and availability – the vast majority of data providers have not instituted them. Even so, 75% of Plaid's data access today is on or committed to APIs. We are eager to get to 100%, but cannot do so without data providers doing their part and implementing developer interfaces. Finalizing this requirement in the final rule is, in our judgment, necessary to drive this outcome.

Mandating the implementation of developer interfaces also is essential to ensure fair competition in the data access market. A developer interface gives every third party the ability to access data directly, without using a data access platform. That will ensure that data access platforms are only used when they do add value. As a general matter, the final rule should be structured to prohibit any entity from having unfair or exclusive direct access to data from a data provider, much less the ability to monetize that monopoly access.

A. The Bureau Should Safeguard The Presumption In Favor Of Access – Which Is Critical To The Open Finance Ecosystem – By Including Additional Protections To Prevent Pretextual Denials Of Access By Data Providers

In recognition of the aims of open finance, the proposed rule reflects a *default presumption* in favor of consumer and third party data access. That is, upon request by an authorized third party, a data provider *must* make covered data available through a developer interface that meets certain requirements. (§§ 1033.201(a), .301, .311.)[27] This requirement is subject only to very limited, enumerated exceptions – most notably when there are "risk management concerns" (§ 1033.321(a))[28] or a failure by the third party to "present evidence that its data security practices are adequate to safeguard the covered data" (§ 1033.321(d)(1))[29]. Despite specifying these exceptions, the proposed rule nevertheless lacks sufficient clarity and detail to effectively prevent data providers from inconsistently or pretextually denying access. It is important for the Bureau to address these concerns because consumers are entitled, under the law, to access and share their own data. This includes being able to choose third party financial services providers, as well as any data access platforms that support those third parties, without limits being imposed by data providers. Given the widespread disparity of access and the anticompetitive conduct of which the Bureau is aware of in the open finance ecosystem, the consumer right articulated in § 1033 cannot be fully realized without stronger and clearer protections.

---

[27] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74809, (proposed Oct. 31, 2023).

[28] To be a reasonable denial based on a "risk management concern," the denial "must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner." *Id.* at 74819.

[29] *Id.* at 74820.

While requiring a data provider to communicate the basis for a denial of access under § 1033.351(b)(2) could "reduce the potential for pretextual denials,"[30] this approach is insufficient to protect against anticompetitive behavior. It is not enough to require that access denials be communicated to third parties, or that they be for "risk management" or security concerns, or even that they be reasonable, specific, and non-discriminatorily applied. An incumbent data provider with discretion could still easily leverage "risk management concerns" in order to deny access to third parties based on a *specific* and facially-valid concern that is not relevant to that third party's data security posture, or is pretextual. Similarly, a data provider could intentionally require unduly burdensome "evidence" of a third party's security, or find that evidence insufficient in order to delay or subvert access. In fact, it is well-recognized that "dominant market participants use privacy and security as a justification to disallow interoperability and foreclose competition."[31] The Bureau also is well aware that data providers "may have incentives to deny access."[32] Indeed, the Bureau has an extensive public record to support concerns about anticompetitive conduct designed to interfere with consumer permissioned data sharing.[33] The end result is not just harm to competition; it is harm to consumers and an undermining of the entire open finance ecosystem.

To address these concerns, the Bureau should adopt a third-party certification standard and make clear that third parties which complete the certification cannot be denied access by a data provider.

In the absence of such a standard, the Bureau should adopt an attestation approach to access, whereby, prior to or at the time of requesting access, third parties submit an attestation of adequate security practices. Such an attestation should be subject to a rebuttable presumption in favor of access. In addition, in

---

[30] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74827, (proposed Oct. 31, 2023).

[31] Office of Tech. and the Bureau of Competition, *FTC, Interoperability, Privacy, & Security*, Dec. 21, 2023, available at www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security; Director Rohit Chopra, *Laying the foundation for open banking in the United States*, June 12, 2023, available at www.consumerfinance.gov/about-us/blog/laying-the-foundation-for-open-banking-in-the-united-states/ ("New digital banking technologies have the power to expand and open market access for American consumers. . . . [But,] powerful firms have sometimes looked to manage emerging technologies . . . . Control of the open banking system by such players threatens competition and the consumer's control of their own financial affairs.").

[32] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74820, (proposed Oct. 31, 2023).

[33] Fidelity & PNC Lead Akoya's Open Banking Land Grab. *CFPB's Chopra Not Amused. Public Statements Indicate*, Fintech Business Weekly, Jason Mikula, Oct. 1, 2023, available at fintechbusinessweekly.substack.com/p/fidelity-and-pnc-lead-akoyas-open; Alex Johnson, *8 Questions about the Future of Open Banking*, Workweek, Oct. 6, 2023, available at workweek.com/2023/10/06/8-questions-open-banking; Stakeholder Labs, *Fintech Giants Prepare for New Regulatory Paradigm*, The Roundtable Roundup, Oct. 11, 2023, available at blog.stakeholderlabs.com/p/the-roundtable-roundup-fintech-giants.

order to guard against any attempts to pretextually rebut this presumption and deny access, the CFPB should:

- **Confirm that data providers have only *limited* discretion to deny access, including by stating that data providers bear the burden to overcome the default presumption in favor of access;**
- **Provide examples of what constitute "risk management concerns" that may form the basis for a denial;**
- **Include, in addition to the "indicia of reasonable denials" section, a new section entitled "indicia of *unreasonable* denials" to clarify certain types of pretextual conduct;**
- **Require data providers to publish and submit to the CFPB certain information regarding any denials of access; and**
- **Strengthen the non-discrimination standard.**

1. The Bureau Should Adopt A Third-Party Certification Standard And Make Clear That Third Parties Which Complete This Certification Cannot Be Denied Access

For a third party to receive access to a data provider's developer interface, the rule contemplates that the third party will make a request for access, and the data provider will respond by either granting or denying the request. While the rule suggests that a third party must include certain information in its access request – e.g., information sufficient to: authenticate the consumer's identity, authenticate the third party's identity, confirm the third party has followed the rule's authorization procedures, and identify the scope of the data requested (§ 1033.331(b)(1)) – the rule does not expressly indicate the full extent of information that must be presented for a third party to gain access. Further adding to this ambiguity, the rule also suggests that a third party may need to provide "evidence that its data security practices are adequate to safeguard the covered data" (§ 1033.321(d)(1)) in order to prevent a denial of access, but does not specify what constitutes sufficient evidence or when such evidence should be submitted. Left open to interpretation by thousands of data providers, this ambiguity could lead to substantial burden on industry participants and delays in granting the access necessary to enable consumers' chosen financial services providers.

To address these ambiguities and ensure a consistent approach across the market, the Bureau[34] should adopt a uniform certification standard for third parties. Such a certification should be deemed sufficient evidence of "adequate security practices" and should entitle a third party to access, meaning a data provider cannot deny access to any third party that presents evidence of its certification. A

[34] While the Bureau may seek to outsource the development and administration of a certification standard to a recognized standard-setting body, in the absence of a recognized body, the Bureau should undertake to develop and administer a certification standard.

certification standard would ensure a balanced, consistent approach across thousands of third parties and thousands of data providers and would avoid the volume, burden, and inefficiency risks, particularly for smaller data providers, recognized by the Bureau. As the Bureau notes, this approach – where "a governmental or quasi-governmental body addresses these problems" – has been used in some other open finance regimes, including in Australia. (NPRM at 96-97.)

2. In The Absence Of A Certification Standard, The Bureau Should Make Clear That An Attestation Of Adequate Security Measures Entitles A Third Party To A Rebuttable Presumption In Favor Of Access And Satisfies § 1033.321(d)(1)

If the Bureau is not prepared to certify third parties for access, then the Bureau should take other steps to ensure that the process for requesting access does not become mired in delay and disputes. As discussed above, the third parties seeking access are businesses that consumers have already chosen to use. By the time a third party is seeking access under the rule, the third party will already have (1) provided the consumer with an authorization disclosure, (2) certified that it will agree to the obligations in the rule, and (3) obtained the consumer's express informed consent to access covered data on their behalf. The proposal includes specific details about the content and form of the authorization disclosure and the third party's legal obligations. With these significant regulatory requirements for third parties, and the consumer's informed decision to seek services from the third party, there should be an extremely high bar for a data provider interfering with a consumer's request by denying a third party's access request.

Accordingly, the Bureau should clarify that presentation of an attestation by the third party that its "data security practices are adequate to safeguard the covered data" is sufficient evidence to create a rebuttable presumption in favor of access. The attestation could describe specific compliance standards that the third party has met, such as ISO 27001 or (as applicable) another qualified industry standard related to data security, and the period of validity for the attestation.[35]

Once a third party submits an attestation, the data provider must satisfy a high burden in order to rebut the presumption in favor of access. **In order to codify this high burden – and protect the presumption in favor of access from any pretextual denials based on purported "risk management" concerns – the Bureau should take the following additional steps:**

[35] While such compliance standards may be appropriate in many circumstances, they may not be appropriate or applicable for all third parties, depending on the nature of the data they possess. Accordingly, attestation of adherence to a specific industry standard related to data security should not be deemed a prerequisite to an attestation being deemed sufficient to maintain the presumption of access.

a) The Bureau Should Confirm Data Providers' Limited Discretion To Deny Third Party Access

The proposed rule provides limited discretion to data providers to deny access in certain specified circumstances. However, even this limited discretion can be abused – in violation of the presumption in favor of access – without additional clarifications that more expressly cabin data providers' (limited) ability to deny access. These clarifications are needed because (1) third parties are *not* service providers to data providers; quite the opposite – data providers' interests are often in conflict with third parties' interests, given that they compete for business; and (2) incumbent data providers are therefore incentivized to interpret the rule as imbuing them with *extensive* discretion to deny access, particularly under the guise of "security" concerns. Allowing data providers to operate as if they have extensive discretion to deny access is untenable – and would amount to the Bureau giving incumbents more power over consumers' own data than the consumers themselves would have, while simultaneously empowering incumbents to act as "gatekeepers" for new entrants and innovative competitors.

For example, the proposal provides that a denial is "not unreasonable if it is necessary to comply with section 39 of the Federal Deposit Insurance Act, . . . or section 501 of the Gramm-Leach-Bliley Act." Data providers are likely to broadly interpret their ability to deny access as necessary to comply with these provisions. While the GLBA Safeguards Rule's "flexible, risk-based" approach may be an advantage when an entity is developing its own compliance program (NPRM at 88), that same flexibility can easily become an anticompetitive lever when wielded by thousands of incumbent data providers as an amorphous basis on which they can deny access.

The Bureau can more effectively protect the presumption in favor of access and prevent data providers from acting as if they have unfettered discretion to deny access by taking the following actions:

- ***Confirming that data providers are not responsible for protecting consumers' own data when a consumer has authorized that data to be moved to a third party***: The Bureau has the authority to regulate and supervise the open finance ecosystem, including third parties. If it determines that a third party – or a data provider, for that matter – poses a security risk to consumers, including through the collection and use of covered data, it has the ability to take action, including through its supervisory or enforcement authority. It is *not* the data providers' responsibility to investigate or police this risk, so the Bureau should clarify in its Preamble that data providers do not bear responsibility, *nor do they have the authority*, to protect consumers' own data when the consumer has authorized its access by and portability to a third party. Any other result implicitly imbues incumbent financial institution data providers with improper authority and implied veto power over the very third parties with which they compete – allowing those incumbents to stifle competition under the guise of consumer protection and ultimately resulting in an ecosystem in which

incumbents, *not consumers*, control the access and sharing of consumers' own data.[36] This approach should not conflict with interagency guidance on third party relationships, which covers business arrangements between a banking organization and another entity that provides services for the banking organization, such as outsourced services, independent consultants, referral arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, and joint ventures.

- ***Assigning data providers the burden of proof to overcome the presumption in favor of access***: When a third party approaches a data provider to seek access, and the third party provides evidence of authorization and an attestation to adequate data security practices, then there should be a presumption in favor of granting access, as the third party was chosen and authorized by the consumer. To appropriately clarify data providers' limited discretion to deny access, the Bureau should make clear that the data provider bears the burden of proof to demonstrate the reasonableness of any denial of the consumer's authorization, including, for example, demonstrating that such denial is based on a *known* risk management concern that will – or is likely to – cause substantial injury to consumers.[37] (As part of its required communications under § 1033.351(b)(2), the data provider must include proof of such knowledge and consumer injury to demonstrate that it has met its burden.) The knowledge and consumer injury requirements are critically important, given that the remedy permitted in such circumstances – i.e., the denial of a consumer's statutory right to data portability – is an extreme one being doled out by a data provider with an inherent conflict of interest. In other words, because the remedy itself is a harm to the consumer (denial of access), such harm must be substantially outweighed and justified by a known, likely risk of substantial injury *to the consumer* if access is permitted.

- ***Explicitly limiting "specific risk" to known security risks:*** The CFPB should clarify that "specific risk," as used in § 1033.351(b)(2), means a known security risk. This clarification is necessary because some data providers, particularly prudentially-regulated banks and credit unions, generally think of risk broadly, including all prudential risks, such as liquidity and reputational risks. In line with our recommendations in this bullet and the one above, the Bureau should include the following clarifications in § 1033.351(b)(2):

[36] The Bureau's framework for data providers to "vet" third parties draws on general third party risk management principles. However, third parties are not service providers to data providers; they have been chosen by consumers and have their own, independent relationships with consumers. Permitting data providers to oversee them as service providers is to disempower the consumers who choose to use those third parties – in many cases as a way to obtain financial services that consumers judge to be better than what their data providers offer.

[37] *See* Consumer Financial Protection Circular 2022-04, *Insufficient data protection or security for sensitive consumer information*, available at www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

Reasonable denials. To be reasonable pursuant to paragraph (a) of this section, a denial must, at a minimum, be directly related to a **known,** specific **security** risk ~~of which the data provider is aware~~ **that is likely to cause substantial injury to consumers**, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner. **The data provider bears the burden of demonstrating, prior to denying access, any such specific risk(s), including that such risk is known and is likely to result in substantial injury to consumers.**

- ***Requiring data providers to grant access as soon as a third party has established a remediation plan for the "known, specific security risk":*** The proposed rule does not state how a third party that has been denied access by a data provider may subsequently gain access. The final rule should clarify that denials are not permanent, and that data providers must grant access if the third party presents evidence that they are remedying the identified risk. Consistent with data providers' burden of proof to demonstrate the reasonableness of an initial denial, data providers should bear the burden of proof of demonstrating the inadequacy of the third party's remediation efforts. To avoid creating undue delays, data providers should be required to act as quickly as is practicable to review the third party's evidence of a remediation plan, and either immediately grant access or demonstrate such inadequacy. After all, when data providers' practices are themselves inconsistent with GLBA Safeguards or other data security rules, absent extraordinary circumstances they are permitted to keep servicing their consumers while they work to reestablish compliance.

- ***Specifying that data providers should "legacy in" third parties that already have access, or are in the process of migrating access, to those data providers' developer interfaces, at the time of the final rule:*** In order to avoid a chaotic result at the time the final rule becomes effective, the Bureau should also indicate that third parties that already have access to, or are in the process of migrating access to, a data provider's developer interface as of the effective date of the final rule are presumed to not present a known, specific security risk for purposes of this section. Absent this clarity, data providers may choose to withdraw existing access to their developer interfaces at the time the rule becomes final, which, particularly if done suddenly and at scale, would result in significant consumer harm. Even if a data provider does not withdraw existing access, the operational burdens of assessing access for thousands of third parties across data providers that are currently on APIs will be enormous.

b) The Bureau Should Provide Examples Of "Risk Management Concerns"

Beyond the reference to FDIA Safety and Soundness Standards and GLBA Safeguards Rule – neither of which provides specificity or clarity – the CFPB does not otherwise articulate what is meant by "risk management concerns." Although the NPRM refers to the possibility of Qualified Industry Standards related to data security or risk management, those standards do not currently exist and may take time to emerge. In the meantime, the NPRM's lack of specificity and clarity will allow data providers not only to act as if they have extensive discretion to deny access, but also to create inconsistent standards across the open finance ecosystem.[38] This will be worsened if there is not sufficient coordination among other regulators with jurisdiction over data provider risk considerations.[39] **As discussed above, we recommend the Bureau create a certification standard that would ameliorate these concerns. If the Bureau does not take this recommended approach, we respectfully suggest that the Bureau at minimum provide illustrative examples in order to encourage consistency, ensure denials are focused on ameliorating true security concerns, and otherwise prevent pretextual denials.**

c) The Bureau Should Include A New Section Entitled "Indicia Of Unreasonable Denials" To Clarify Certain Types of Pretextual Conduct

The NPRM currently includes a proposed section of the rule defining "indicia of reasonable denials." **In line with our recommendations above, the Bureau should add a new section setting forth indicia of *unreasonable* denials.** Security and risk are evolving fields, and data providers and third parties will have little clarity as to the line between denials

[38] For example, as exists today, every data provider will have its own interpretation of and tolerance for "risk," resulting in individualized and potentially conflicting standards across more than 10,000 data providers. This would create a fractured landscape, where third parties would have no predictable understanding of whether they will be permitted to connect to each interface. This challenge is exacerbated given that data providers' own data security regimes vary widely depending on the size and risk profile of the financial institution, with many of the largest financial institutions leveraging extremely robust security controls, while smaller institutions may lack security features such as multi-factor authentication to access consumer accounts.

[39] "Banks continue to leverage new technology and innovative products and services to further their digitalization efforts and to meet evolving customer demand and expectations. [T]hese products and services and their underlying technologies can offer many benefits to banks and their customers, they also contribute to a complex operating environment along with increasing compliance, reputational, strategic, and other risks. . . . Banks are also reminded to implement appropriate due diligence, change management, and risk management processes when considering changes to products, services, and operating environments." *See* The National Risk Committee, *Semiannual Risk Perspective*, Office of the Comptroller of the Currency, Dec. 7, 2023, available at www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2023.pdf.

that reflect known risks that are likely to cause substantial injury to consumers, and those that do not. Accordingly, Plaid proposes the Bureau include the following section in its final rule:

> § 1033.321 Interface access.
>
> * * *
>
> (c) **(1)** *Indicia of reasonable denials.* Indicia that a denial pursuant to paragraph (a) of this section is reasonable include whether access is denied to adhere to a qualified industry standard related to data security or risk management.
>
> **(2) *Indicia of unreasonable denials*. Indicia that a denial is not reasonable include that the third party has presented an attestation that its data security practices are adequate to safeguard the covered data, or provided information about: (i) compliance with a qualified industry standard related to data security or risk management, or (ii) certification(s) deemed by the Bureau to demonstrate appropriate security or risk management practices, or that are generally recognized as evidence of appropriate data security practices for a third party of its size, complexity, and risk profile**.

d) The Bureau Should Require Data Providers To Disclose To Third Parties And To the CFPB Certain Information About Denials, As Well As Publish Certain Related Metrics

Although § 1033.351(b)(2) requires a data provider to create records and to communicate to a third party when it denies access, this mechanism is not sufficient to accomplish the NPRM's intent to "reduce the potential for pretextual denials." In part, this is because even with this communication, a third party lacks the visibility to determine whether it is being treated inconsistently or in an otherwise discriminatory manner. It also does not enable the third party to take any remedial action *prior* to the consumer harm caused by the access denial. Further, while the NPRM suggests data about access denials will be used in "supervision and enforcement of the proposed rule by the CFPB, Federal and State banking regulators, State attorneys general, and other government agencies that supervise Data Providers," the practical reality is that there is likely to be a significant time delay between a denial of access and any oversight by regulators, during which time consumer harm will persist.

Additionally, the CFPB should clarify that data providers are not permitted to use information obtained for the purpose of assessing a third party's request to access a developer interface for any purpose other than to assess that request; otherwise the data provider may use this information for anti-competitive purposes, particularly absent a strong disincentive against pretextual denials of access.

To prevent pretextual or discriminatory conduct, the CFPB should require data providers to (i) provide more detailed information regarding any access denials to third parties, (ii) report those access denials, including any records created in

compliance with § 1033.351(d)(2), on a monthly basis to the CFPB, and (iii) only use information obtained by third parties to assess a third party's request to access the developer interface and thereafter maintain such access. This prospect of third-party- and regulatory- attention should incentivize more appropriate conduct without the CFPB or third parties having to take additional action.

Specifically, Plaid proposes the following changes:

> § 1033.351 Policies and procedures.
>
> * * * * *
>
> (b) Policies and procedures for making covered data available. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:
>
> * * * * *
>
> (2) *Denials of developer interface access*. When a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider:
>
> (i) Creates a record explaining the basis for denial; and
>
> (ii) Communicates to the third party, electronically or in writing, **its general policies and procedures governing the denial of interface access,** the **known, specific security risk(s) or other** reason(s) **relied on as a basis** for the denial**, and information sufficient to satisfy the data provider's burden of demonstrating the reasonableness of its denial, including that such denial is based on a known security risk management concern that is likely to cause substantial injury to consumers. The communication must disclose whether requests from other third parties have included the same specific risks and whether those requests were granted or denied.** ~~and that the~~ **The** communication **must** occur as quickly as is practicable.
>
> (3) *Denials of information requests*. When a data provider denies a request for information pursuant to § 1033.331, the data provider:
>
> (i) Creates a record explaining the basis for the denial; and
>
> (ii) Communicates to the consumer or third party, electronically or in writing, the type(s) of information denied ~~and~~**, its general policies and procedures governing the denial of information requests,** the **specific** reason(s) for the denial, **a description of the specific risk(s) involved or the specific information that the consumer or third party failed to provide, and an explanation of why the denial was justified. The communication must also disclose whether**

requests from other third parties have included the same specific risks or lack of information and whether those requests were granted or denied. ~~and that the~~ **The** communication **must** occur as quickly as is practicable.

(4) ***Use for any other purpose*****. Data providers shall be prohibited from using information about third parties that was provided in order to obtain or maintain access to a developer interface, except as is necessary to assess a third party's request to access the developer interface and thereafter maintain such access.**

(5) ***Access after remediation*****. If a data provider has denied an access request pursuant to § 1033.351(b)(2) or an information request pursuant to § 1033.351(b)(3), then the data provider must grant such access request or information request, as applicable, if the third party presents evidence of a plan to remedy the applicable risk. Data providers must act as quickly as is practicable to review the third party's evidence and either (i) grant immediate access or (ii) if the data provider reasonably believes the remediation plan is inadequate, then provide sufficient information to the third party demonstrating the inadequacy of the remediation plan.**

* * * * *

(d) Policies and procedures for record retention. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part.

* * * * *

(3) ***Certain records submitted to the Bureau*****. On a monthly basis, any data provider that has denied access to a third party in the most recent month must submit to the Bureau all communications of denials of a third party's requests for access to an interface.**

The Bureau should also publish aggregate data showing patterns of access denials by data providers. The CFPB has used transparency and public monitoring to incentivize appropriate conduct in several other areas under its authority, such as its consumer response program and HMDA reporting regulations. *See, e.g.*, 12 C.F.R. § 1003.1(b)(1)(iii) ("This part implements the Home Mortgage Disclosure Act, which is intended to provide the public with loan data that can be used: . . . *To assist in identifying possible discriminatory lending patterns and enforcing anti-discrimination statutes.")* (emphasis added). Differences in trends and practices among data providers will enable the Bureau and third parties to identify where denials of access may be based on pretextual explanations.

e) The Bureau Should Strengthen The Non-Discrimination Standard In § 1033.321(b)

In addition to the proposals in Sections IV.F and IV.G below, and since the record shows that consumer data rights and choice are currently being hindered by anticompetitive conduct, the CFPB should strengthen the language of § 1033.321(b) in the final rule as proposed:

> § 1033.321 Interface access.
>
> * * * * *
>
> (b) *Reasonable denials*. To be reasonable pursuant to paragraph (a) of this section, a denial must, at a minimum, be directly related to a **known,** specific **security** risk ~~of which the Data Provider is aware~~ **that is likely to cause substantial injury to consumers**, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner. **The data provider bears the burden of demonstrating, prior to denying access, any such specific risk(s), including that such risk is known and is likely to cause substantial injury to consumers. A denial is not reasonable when a data provider or developer interface service provider denies access to a third party based on a specific risk, but grants access to another third party where the same or materially similar risk is present, or when a data provider or developer interface service provider takes steps to mitigate a specific risk as to one third party but fails or refuses to take steps to mitigate the same or materially similar risk as to another third party.**

B. The Bureau Should Maintain The Current Proposed Prohibition On Data Providers (And Developer Interface Service Providers) Charging Consumers And Third Parties For Interface Development, Maintenance, And Access

Section 1033.301(c) prohibits data providers from "impos[ing] any fees or charges on a consumer or an authorized third party in connection with . . . [e]stablishing or maintaining the interfaces required" by the rule or "[r]eceiving requests or making available covered data in response to requests." Plaid agrees with the Bureau's determination that this "prohibition [is] necessary and appropriate to effectuate consumers' rights under CFPA section 1033 by ensuring that consumers and authorized third parties are not impeded from exercising consumers' statutory rights because of fees, which would be contrary to the objectives of the statute."[40] In short, the prohibition reflects the critical fact that the data at issue belongs to consumers, not to

[40] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74814, (proposed Oct. 31, 2023).

the data providers that may hold it – and that consumers have a statutory right to freely access and share that data (whether they do so directly or through a third party). The prohibition will also support the innovative, competitive open finance ecosystem the Bureau aims to cultivate.[41]

C. The Bureau Should Prescribe Additional Limits On Access Caps

1. The Bureau Should Make Clear That Any Access Caps Impede Consumers' Ability – Not Just Third Parties' Ability – To Access Their Data

Section 1033.301(c)(2) prohibits a data provider from unreasonably (or discriminatorily) restricting the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface. The fundamental principle that the consumer should be in control of their data, whether they are accessing it directly or through a third party, supports the NPRM's prohibition against data providers imposing unreasonable "frequency of access" restrictions. Different consumers have different needs. Some may use just one third party, while others may use dozens of third parties, to manage their financial lives. Some may only need to access their data once a year, perhaps to prepare and file their taxes, while others may need to access their data four times a day to receive personal financial management services. Still other consumers appreciate that they can engage in safer or faster on-demand transactions by having the ability to access and share data at the specific moment they need it. In all of these instances, the volume of data requests is dictated by the services the *consumer* has chosen, and by the data access the *consumer* has authorized. The Bureau's guidance for the final rule should reflect that reality, and reframe access caps to describe them as what they are: caps on a *consumer's* ability to access their data, not (as they are currently framed) as caps on *third parties'* ability to access data.

2. The Bureau Should Make Clear That The Frequency Of Consumer-Present Access Requests Can Never Be Capped And Batch Traffic Access Requests Are Subject To A Rebuttable Presumption In Favor Of Uncapped Frequency Of Access

In general, there are two types of data access requests. The first is when the consumer is actively trying to connect an account at their data provider to their chosen third party product or service. This type of real-time consumer access request is no different than the consumer trying to directly log into the data provider's website or consumer interface. The second type of traffic is when the consumer is not present, typically referred to as batch traffic. For these access requests, the consumer has permissioned their data on an ongoing basis to a third party, which

[41] As the Bureau recognizes, "Each data provider is the sole supplier of its customers' financial data and therefore able to exert market power over the prices or fees it charges for authorized access to consumers' data. Data providers have in the past restricted data access for third parties. These restrictions have anti-competitive effects and, by allowing data providers to charge prices for access that are in excess of marginal cost, may harm consumers and third parties." Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74814 , (proposed Oct. 31, 2023).

needs access to it with a certain regularity in order to support the product or service the consumer has requested. Today the majority of traffic on Plaid's network is batch traffic, and Plaid and other data access platforms have some ability to manage traffic volumes for batch traffic without interfering with consumer use cases.

With this distinction in place, **the Bureau should specify that it is never reasonable to restrict the frequency with which a data provider receives and responds to requests for covered data (whether from a consumer directly or a third party) when the consumer is present**, as a cap in this instance could be highly disruptive to the consumer's financial life and cause them to suffer harm. Capping this type of data request would also substantially frustrate third parties' ability to onboard new customers, creating substantial harm to competition.

With respect to batch traffic, Plaid recognizes that there may be rare instances in which it is not commercially reasonable for a consumer to be able to access their own data without limits, and the final rule should allow a data provider to rebut the presumption against access caps, while setting a high bar for such a rebuttal. **Specifically, the Bureau should make clear that the presumption against such access caps can only be rebutted – i.e., it is only reasonable to restrict the frequency with which a data provider receives and responds to requests for covered data – when the cap is:**

1. **Temporary;**
2. **In place for a fixed period of time (e.g. 6 hours);**
3. **Implemented in order to: prevent interference with access by other consumers or third parties acting at the direction of consumers or to protect the stability of the developer interface;**
4. **Communicated to third parties in advance, with commercially reasonable notice (particularly so that there is sufficient time for data providers and third parties to work together to manage traffic in a way that reduces the need for any cap), or, in an emergency, as soon as is practicable;**
5. **Used only after commercially-available solutions for managing access requests have otherwise been exhausted.**[42]

[42] Commercially-available solutions include: (1) for connections where third parties are using a data access platform, creating a developer interface architecture with a single access token for the data access platform, rather than individual access tokens for each third party; and (2) requesting that third parties voluntarily manage their traffic ahead of high-traffic events (for example the Super Bowl, when advertising can drive substantial consumer sign up, or tax day). With respect to the former, this allows the data access platform to make one developer interface request to cover multiple third parties, rather than each third party having to make duplicative developer interface requests for the same data. (See Appendix 3). With respect to the latter, third parties are in the best position to know which requests are critically important to support a consumer and which can be temporarily delayed. Plaid already does this voluntary traffic management with many of our data provider partners.

3. The Bureau Should Make Clear That Capping Access Based On Cumulative Data Requests Over Time Is Prohibited

Data providers also should not be able to restrict the total amount of data that a third party can request over a given time period. Because the consumer is the one requesting data, applying an access cap to an individual third party would punish consumers, by limiting their access to the third parties that consumers use the most, i.e. the ones that consumers find most valuable. It would also limit third parties' growth, directly undermining the pro-competition purposes of this rule.

4. The Bureau Should Make Clear That It Is Not Reasonable To Implement Access Caps Based On Data Provider's Size, As Access Requests Are Consumer Requests, Regardless Of Whether They Are Direct Or Through A Third Party

Smaller data providers should not be permitted to implement access caps based on their size, because the amount of data access traffic a data provider sees directly correlates to the number of consumers they have who wish to use digital or competitive services. The largest financial institutions, which have the most consumers, make up a substantial portion of data access requests. Accordingly, almost all of Plaid's traffic reflects requests to the 20 largest data providers. Contrast this to small community banks and credit unions, which have a much smaller customer base and thus receive far fewer data requests. In fact, on Plaid's network, approximately 9,100 data providers receive fewer than 1,000 data requests per day. Approximately 5,600 data providers receive *fewer than 100* data requests each day. These small institutions are unlikely to face any burden in servicing this volume of access requests. As a point of comparison, a top-10 financial institution today would typically permit 500 API calls *per second*. Smaller institutions can and should be expected to accommodate 0.00002% of this volume.

D. The Bureau Should Incentivize Commercially Reasonable Conduct And Continuous Technological Improvement By Requiring Data Providers To Include Access Cap And Other Performance Information In Their Monthly Performance Reports

To ensure that any access caps that are put in place are "commercially reasonable," the CFPB should expand the monthly reporting requirements in § 1033.341(d) to include:

1. **When an access cap was put in place; and**
2. **How long the cap lasted.**

Without transparency across data providers it will not be possible for third parties or the Bureau to determine whether access caps are commercially reasonable.

As a further transparency measure, the final rule should require that all performance metrics where the rule requires "commercially reasonable" performance, including developer interface uptime, latency, number of planned days of downtime, number of days of unplanned downtime, and number of days of notice for planned downtime should all also be included in a data provider's monthly § 1033.341(d) disclosures.[43] By requiring reporting on these metrics, the Bureau will enable its market monitoring and other functions to understand whether consumers are able to benefit from their consumer data rights and identify areas where further Bureau guidance or action may be advisable.[44] It also will allow third parties to assess whether they are being treated in a non-discriminatory manner vis-a-vis other third parties who seek authorized access to data.

E. The Bureau Should Include Additional "Commercially Reasonable" Performance Specifications In § 1033.311(c)(1)(i)

The Bureau notes that minimum standards "ensur[e] that data providers make available data on a basis that enables third parties to provide products and services, *including those that compete with products and services offered by the Data Provider*."[45] To ensure that competition is appropriately protected, the CFPB should more specifically identify performance specifications in § 1033.311(c)(1)(i), specifically by setting requirements for reasonable notice of downtime (§ 1033.311(c)(1)(i)(B)) and total amount of scheduled downtime (§ 1033.311(c)(1)(i)(C)). The proposed rule's structure does not require that an SSO take on determining these performance standards. And there are disadvantages to leaving these standards to an SSO: if an SSO decides only to standardize data format, then in the absence of clearer specifications from the Bureau data providers will not be able to benefit from an "indicia of compliance" protection for their developer interface performance.

For any performance requirements specified in the final rule, the Bureau should make clear that they are a floor, not a ceiling. For example, 3500 MS latency in the NPRM already trails the market; for common API calls like Balance or Authorization, the median latency is between 1350 MS and 1450 MS. All of these latency levels are *substantially*

[43] For the last six months, Plaid data shows the median notice of scheduled downtime from data providers with APIs was six calendar days, with some notices coming just 24 hours in advance. Such short notice presents an unacceptable disruption of consumer access and to the businesses that consumers rely on for their financial well being.

[44] It is possible that data providers will respond to the NPRM, or this recommendation, by arguing that it would be burdensome to regularly report to the Bureau on these matters. To the extent that data providers maintain written policies and procedures that are "reasonably designed to achieve the objectives" of the rule, submission of those policies and determinations to the Bureau would be a ministerial activity.

[45] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74816, (proposed Oct. 31, 2023).

below what commercial actors in any other area of the economy would expect from an API. Publicly available metrics on latency for cloud services providers from 2019-2020 shows a latency range of 300-480ms.[46] Granted, some data providers have legacy internal systems that make it harder to achieve this performance, but the Bureau should be cautious about giving financial service companies regulatory permission to have perpetually slower technology than the rest of the economy, and consider setting performance standards that ensure the ecosystem is held to an appropriate standard. The Bureau should want performance to increase over time as technology improves, rather than adhere to only the minimum specifications set forth in the NPRM.

In order to prevent a race to the bottom or stagnation, and to ensure that consumers benefit from consistent investment and improvement in developer interfaces, **the Bureau should create a regulatory mechanism under § 1033.311(c)(1)(ii)(B) for measuring whether a data provider's developer interface meets "the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers."** Such a mechanism could require that data providers not only publicly report their performance metrics, but compare their metrics with the metrics from other data providers in their cohort as defined by § 1033.121. For example, the definition of what is commercially reasonable could be defined as the median performance of data providers in any given cohort over the past 12 months, so long as the performance is not lower than in the previous 12 months.[47] This would ensure that, as technology improves, what is commercially reasonable will adjust at the same pace, and developer interfaces continuously will improve well after the rule is final.

F. The Bureau Should Broaden Its Non-Discrimination Protections To Address Other Tactics Used By Data Providers To Delay Or Interfere With Access

The NPRM confirms that consumers have data rights, but it does not declare efforts to interfere with those rights to be a violation of the law. While there are two non-discrimination provisions in Subpart C,[48] the proposed rule does little to prevent data providers from disrupting or interfering with access in other ways, such as by varying the performance, compatibility, or features of their interfaces, by implementing information technology systems in non-standard ways that limit interoperability, or by imposing excessive burdens or unnecessary procedures that restrict or delay access depending on which third party is requesting access.

---

[46] Dr. Paul M. Cray, *Performance by Latency (All services, all clouds)*, APIexpert, available at api-cloud-analysis.api.expert/data/performancebylatency/.

[47] This improvement standard could end once data providers meet a certain absolute performance threshold on par with other "instant" latency response times in the market, e.g. 50-200ms.

[48] One in § 1033.311(c)(2) that requires any frequency restrictions (access caps) to be applied in a manner that is non-discriminatory and consistent with the data provider's policies and procedures, and another in § 1033.321(b) that requires any denials of access to be applied consistently and in a non-discriminatory manner.

Several other consumer-facing industries have seen incumbents employ these tactics to prevent or delay open systems designed to increase competition and provide consumers with more choice. The Bureau already identified such practices related to electronic health information as an example of problematic conduct. In the telecommunications industry, Internet Service Providers have been accused of prioritizing or throttling certain types of internet traffic to undermine net neutrality rules, and telecommunications companies interfered with how easily consumers can transfer their data (such as contact lists, messages, or other personal data) from one telecom provider to another. Limits on interoperability leave consumers locked into a particular provider.

The Bureau asked "whether other language might be appropriate to achieve this [anti-discrimination] objective," such as through the articulation of "information blocking" as a specific practice it seeks to prohibit.[49] For the § 1033 rule to have its intended impact of shifting control to consumers, encouraging competition for consumer business, and stoking innovation that serves consumers, it is critical that CFPB anticipate and prohibit the kinds of tactics so commonly employed when incumbents seek to interfere with the transparency and openness advanced by modern regimes, including the open finance ecosystem. **Thus, in addition to our recommendations above, the Bureau should clearly state that denials of access, or other attempts to block or hinder access, are a violation of the law when they are anti-competitive or pretextual because they deny a consumer's statutory right of access:**

> **([X]) It is unlawful for any data provider or developer interface service provider to engage in, be a party to, or assist in, any discriminatory denial of consumer or third-party access, including through the application of any pretextual reason, including risk or security standards; or to otherwise engage in, be a party to, or assist in, conduct that, except as otherwise permitted under this rule:**
>
> > **(a) is likely to interfere with, prevent, or materially discourage access, collection, use, or retention of covered data by a consumer or third party; or**
> >
> > **(b) degrades, impairs, or creates barriers that would restrict or tend to restrict, or systematically impede, access by a consumer or third party.**

The Bureau should also specifically enumerate in the preamble some of the tactics that would unlawfully interfere with data access (including unfairly

[49] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74809, (proposed Oct. 31, 2023).

"preferencing" any particular entity).[50] The preamble should explain that there is a history of incumbent efforts to delay or interfere with open access to consumer data and provide examples of the types of conduct it seeks to prevent, such as through or by: (1) limits on access, approval, availability, disclosure, retention, or use of covered data; (2) requirements for authorization or authentication compensation requirements; (3) currentness, integrity, liability, performance, and reliability provisions; (4) provisions relating to third party oversight and risk management; or (5) implementing information technology systems in non-standard ways.

G. The Bureau Should Provide Mechanisms For Reporting Of, And Enforcement Against, Conduct That Violates The Rule

The NPRM does not provide any specific provisions to address enforcement, and the Bureau's general enforcement authority[51] does not contemplate industry participants monitoring compliance, reporting violations, or initiating proceedings. The provisions instead rely on the Bureau to take the initiative in conducting investigations and prosecuting violations of the Act.

Typically, the Bureau can rely on its consumer response program to hear directly from consumers about the challenges they face in the marketplace and bring those concerns to the attention of financial institutions. In the case of many of the requirements of the proposed rule, the consumer may have no way of knowing why they suffered harm – for example a broken connection that caused a payment to be late – or who is responsible. They may only know that they are not able to connect accounts or are required to use manual methods to gain access and obtain their data for sharing. Moreover, the broader market effects of anticompetitive conduct on innovation and availability of alternative financial services providers will not be easily visible to consumers, an indirect harm caused by the lack of access. In those circumstances, it is highly unlikely that the existing consumer response mechanism will be sufficient to alert the Bureau to violations of the final rule's deadlines and requirements.

[50] § 1033.331(e) – which requires that any authorization revocation mechanism provided by a data provider "at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party" – is modeled after 42 U.S.C. § 300jj-52, the "information blocking" provision in the Public Health Service Act. That provision allows DHHS to investigate any claim that a covered entity engaged in practices "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." See 42 U.S.C. § 300jj-52(a)(1)(A), (b)(1)(A)(ii). Section 1033.331(e), by contrast, only relates to revocation mechanisms and does not prohibit interfering with, preventing, or materially discouraging access more broadly. We therefore recommend inclusion of a broader provision above.

[51] Dodd-Frank Consumer Financial Protection Act. *See* 12 U.S.C. § 5561–63, § 5563(a).

To address these limitations, we recommend the final rule:

- **Encourage consumers to report any denial or failure of access to the CFPB, even if they cannot articulate a direct harm or identify the party that is to blame;**
- **Provide a mechanism for industry participants to report anticompetitive conduct, discrimination, or noncompliance with the rule's provisions;**
- **Articulate the Bureau's intent to review consumer and industry complaints about denials of, or other interference with, access when setting its supervisory priorities and making enforcement decisions; and**
- **Put industry participants on notice that the Bureau is willing to enforce the rule by providing that the requirements of the rule "shall be enforced under the Consumer Financial Protection Act."[52]**

VI. Responding To Requests For Information (§ 1033.331)

Section 1033.331(b) requires data providers to make available covered data to third parties when, among other things, data providers receive information sufficient to authenticate the relevant consumer's identity. The Bureau notes that this authentication requirement is needed to mitigate the potential for fraudulent data requests, which is a crucial goal for all stakeholders. Today, before a third party accesses covered data from a developer interface, the third party typically redirects the consumer to the data provider through an access delegation standard known as OAuth 2.0. The data provider then authenticates the consumer with login credentials.

A. The Bureau Should Address Certain Points Of Friction That Occur When A Consumer Is Redirected From A Third Party To A Data Provider To Authenticate Their Identity

The authentication redirect process often creates consumer friction and disincentivizes data portability for at least three reasons: (i) data providers may overwhelm and confuse consumers with unnecessary content across multiple screens instead of only conducting authentication, (ii) data providers typically authenticate with login credentials, which results in consumer frustration and risk due to forgotten, mistyped, or compromised login credentials, and (iii) data partners often do not implement readily available access delegation technology when conducting the redirect.

[52] Many CFPB regulations include enforcement provisions that reference statutory enforcement powers. *See*, e.g., 12 C.F.R. § 1003.6(a) ("A violation of the Act or this part is subject to administrative sanctions as provided in section 305 of the Act."); 12 C.F.R. § 1030.9 ("Section 270 of the act (12 U.S.C. 4309) contains the provisions relating to administrative sanctions for failure to comply . . ."); 12 C.F.R. § 1002.16 (referring to statutory provisions regarding enforcement, penalties, and liabilities); 12 C.F.R. § 1009.7 (Compliance with the requirements of this part shall be enforced under the Consumer Financial Protection Act of 2010, Public Law 111–203, title X, 124 Stat. 1955, by the Bureau of Consumer Financial Protection).

1. The Bureau Should Require That Data Providers Only Conduct Authentication With A Single Screen And Not Present Any Unnecessary, Non-Authentication-Related Content

To address the first point of friction, the Bureau should require that data providers only perform an authentication of the consumer during the redirect process, and prohibit data providers from presenting any content unrelated to authentication. The only exception should be when the data provider presents a single authorization 'confirmation' screen. As explained in Section VII.I below, data providers should only be able to present 'confirmation' screens if the third party does not make a record of the consumer's authorization available to the data provider at the time the connection is made. Data providers typically complete authentication within a single screen when a consumer attempts to login to their account directly through the data provider's consumer interface, and the Bureau should require data providers to meet the same standard for developer interface authentication. A second screen should only be added if required for a second factor of authentication. These proposed requirements would ameliorate existing consumer friction that disincentivizes data sharing created by many data providers that present multiple screens in the authentication process.[53]

2. The Bureau Should Require That Data Providers Use An Industry-Leading Authentication Method That Is Commercially Reasonable To Implement Given The Size And Resources Of The Data Provider

To mitigate a second point of friction and ensure steady progress toward more secure and less burdensome authentication, **the Bureau should require that data providers use an industry-leading authentication method that is commercially reasonable to implement given the size and resources of the data provider.** As the Bureau notes, data providers typically authenticate consumers with login credentials, which results in consumer frustration because they often forget, misremember, or mistype their login credentials.[54]

Implementation of authentication methods that address consumer frustration and security risks can unlock more seamless *and secure* open banking experiences. For example, biometric

[53] Typically, the additional screens contain authorization disclosures. As noted above, data providers should only be able to present a single authorization 'confirmation' screen in specific circumstances. The final rule should be clear that data providers should not add content unrelated to authentication.

[54] Further, when access fails during the redirect, data partners often do not communicate the reason to the third party. Therefore, third parties often cannot differentiate access failures resulting from consumers deciding to not share their covered data versus consumers encountering a credential-based roadblock. The Bureau is correct to require that, under § 1033.351(b)(3)(ii), data providers must communicate to the third party the reason for a denial of request for covered data. The Bureau should clarify in the final rule that such communication must occur in real-time or near-real-time with the denial or access failure so that the third party may, where feasible, immediately assist the consumer with troubleshooting data access.

authentication (e.g., FaceID, TouchID) is lower friction because it avoids the need to enter long and complicated login credentials, while also being more secure. Similarly, technologies such as Passkeys satisfy two of the three authentication factors in strong customer authentication or multi-factor authentication[55] while reducing friction by achieving both authentication factors in what appears to the consumer as a single step.[56] Such alternate authentication methods help mitigate security risks posed by login credentials. Consumers often reuse the same login credentials for multiple services, such as accounts with different data providers.[57] Data breaches and social engineering attacks, such as phishing, could result in bad actors compromising consumers' login credentials. Once compromised, even if via an unrelated service's data breach, bad actors could use credential stuffing and password spraying attacks to compromise consumers' bank accounts. The European Union mandated strong customer authentication for certain payment transactions as part of the Revised Directive on Payments Services (PSD2). By requiring that data providers invest in industry-leading authentication technologies, the Bureau can similarly incentivize adoption of more secure authentication methods such as biometrics and Passkeys, which create a more secure open finance ecosystem for all participants.

3. The Bureau Should Require Data Providers That Offer An Application On Mobile Devices To Implement App-To-App Redirects And Give Consumers The Option To Use Their Device's Biometric Authentication To Access Covered Data

Finally, if the data provider offers an application on mobile devices to consumers, the Bureau should require that the data provider implement readily-available access delegation technology built into those devices. This technology, commonly referred to as App-to-App authentication, redirects the consumer from the third party's application to the data provider's application and back. This avoids higher friction redirect transitions from applications to web browsers that can create disjointed consumer experiences. Crucially, when redirected to a data provider's application, the consumer can use their device's more seamless and secure biometric authentication, if it is enabled by the data provider. Together, these requirements would improve current access delegation and authentication practices and spur more seamless and secure data portability.

---

[55] The three authentication factors are (1) something the consumer knows (i.e., knowledge), (2) something the consumer has (i.e., possession), and (3) something the consumer is (i.e., inherence).

[56] Passkeys use the possession factor by generating a unique public and private key pair and storing the private key in the consumer's chosen device for use during authentication. They also use the inherence factor by having the consumer use biometrics (e.g., FaceID or Touch ID) to unlock their device that contains the private key to complete authentication. If the consumer instead chooses to use a passcode for their device that has the private key, then the knowledge factor is used (i.e., the consumer knows the correct passcode). The consumer only needs to unlock their device when prompted, and the Passkey authenticates the consumer in the background without the consumer needing to take additional steps.

[57] At least 65% of people reuse passwords for multiple online accounts. Google/Harris Poll, *Online Security Survey*, Feb. 2019, available at services.google.com/fh/files/blogs/google_security_infographic.pdf

B. The Bureau Should Clarify That A Data Provider Is Only Obligated To Authenticate A Consumer The First Time The Consumer Shares Covered Data From The Data Provider To A Third Party

When a consumer first shares covered data from a data provider to a third party, the data provider should authenticate the consumer because, at that time, only the data provider has sufficient information to verify that the consumer has the right to access that covered data. After this first authentication, the third party will have sufficient information to know that the consumer has that right to access the account. The third party can accurately identify this consumer when they return because the third party will have established an authentication method for the consumer's access to the third party's financial product or service. Therefore, if the consumer subsequently changes their authorization by, for example, authorizing that third party to access their other accounts or data types at that data provider, the data provider should not be required to re-authenticate the consumer because the third party will have authenticated them and will know that this consumer has the right to access that covered data.

As noted above, redirects to data providers for consumer authentication create consumer friction and disincentivize data portability. **Therefore, data providers should not be required to re-authenticate consumers in any situation in which a third party has already authenticated them.** If the final rule required otherwise, consumers would often need to undergo high-friction and redundant re-authentication redirects. This would pose additional inefficiencies when consumers use a data access platform such as Plaid, which provides a consumer-facing covered data sharing and management service, to share covered data across multiple third parties and use cases.

Consider, for example, a consumer who wishes to apply for a loan. In order to shop for the best terms, the consumer submits loan applications with five different lenders. As part of the application process and to determine loan terms to offer the consumer, the consumer must share covered data from their financial accounts; the consumer has a financial account at three different data providers. The five lenders may all use the same data access platform to allow the consumer to access and share data from their financial accounts with the lenders. To do this, at the first lender, the consumer would have to go through the account connection process three times to access and share data from each of their three different accounts; this means the consumer would be redirected to each of the three data providers' interfaces to enter their login credentials and redirected back to complete the loan application. The consumer would then repeat this process at the second lender, and the third, and the fourth, and finally, the fifth. This results in the consumer having to go through fifteen total redirect experiences.

However, the process would be significantly streamlined with our proposed rule clarification. Instead of having to repeat the redirect process a second, third, fourth, and fifth time, the consumer would only need to do it once. During the consumer's interaction with the data access platform to authorize sharing covered data with the first lender, if the data provider successfully authenticates the consumer, then the data access platform would know that this consumer has

the right to access their financial accounts held at these data providers. The data access platform would also establish an authentication method with the consumer to accurately identify them when they return. If, several minutes after sharing data with the first lender, the consumer subsequently seeks to share the same covered data from the same data providers with the second, third, fourth, and fifth lender in order to get multiple rates and select the best one, the data access platform is in as good a position to authenticate that consumer as the data provider, and multiple sequential redirects to the data provider add unnecessary friction for the consumer. In this example, the proposed clarification would reduce the number of redirect experiences for the consumer from fifteen to three. The final rule should, therefore, clarify that data providers are not required to re-authenticate the consumer for each new authorization to share that covered data so long as the third party securely authenticates the consumer.

This rule clarification would also be consistent with the NPRM's proposed authorization process, which gives third parties, not data providers, the responsibility to obtain consumers' authorization to access covered data. As explained in Section VII.I, third parties are able to share details of each authorization with the data provider. The same technology would allow third parties to share authentication records with the data provider, giving the data provider the option to receive information sufficient to confirm that the consumer has been authenticated.

As noted above, innovative authentication methods such as biometrics and Passkeys that address consumer frustration and security risks can unlock more seamless and secure open banking experiences. In addition to data providers, third parties can implement such authentication methods for consumer access to their financial products and services. For example, third parties could use Passkeys to accurately identify and authenticate consumers returning to data access platforms. Third parties implementing such technologies to authenticate consumers, combined with data providers not being required to conduct redundant re-authentication when the third party already does such authentication, could powerfully unlock streamlined data sharing experiences that greatly increase data portability for consumers.

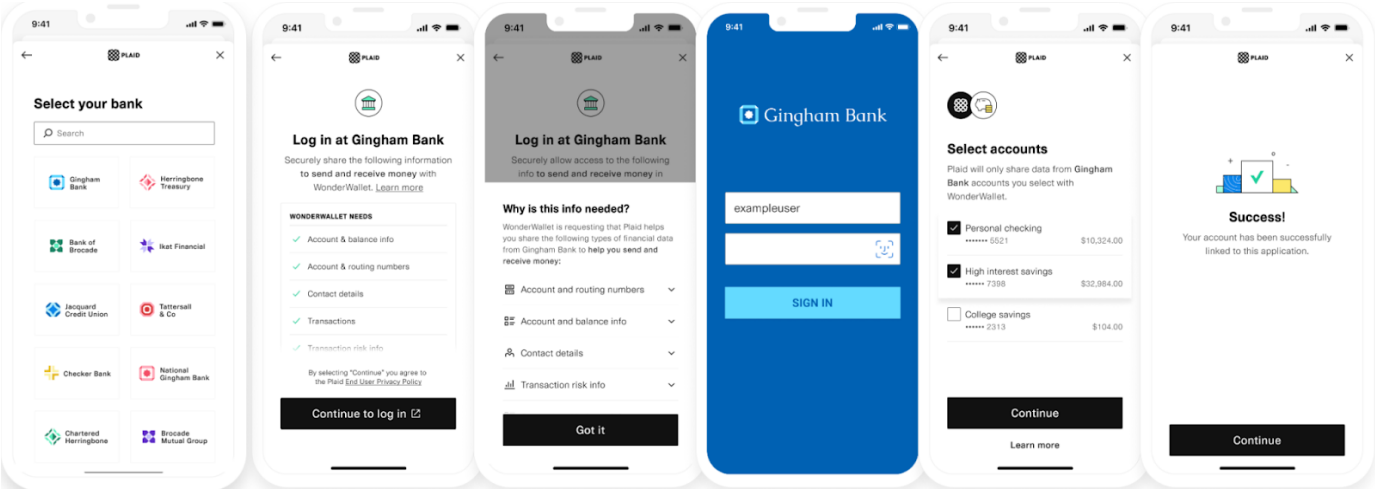
VII. Authorized Third Parties (Subpart D)

The authorization procedures proposed in the NPRM will help ensure that consumers understand and meaningfully consent when authorizing third parties to access financial data on their behalf. They are sufficiently specific for industry participants to understand their obligations, and the Bureau's principle-based approach means that there is sufficient flexibility for authorization disclosures to work on the myriad of digital devices that consumers use for account linking. The proposal's determination that third parties are solely responsible for authorization – that the consumer is *authorizing the third party to collect* financial information on their behalf, rather than *authorizing a data provider to send* information – places the responsibility in the right place to ensure accountability for consumer protection, minimize unproductive consumer friction, and protect against anticompetitive behavior by incumbents.

A. The Bureau's Proposed Authorization Requirements Balance Clarity and Flexibility

The authorization procedures in proposed § 1033.401 are robust and well structured to ensure that a third party seeking authorization is acting on behalf of a consumer. In particular, they are specific enough that authorized third parties can know what their obligations are toward consumers, yet flexible enough that third parties have multiple ways to satisfy the obligation. This flexibility is particularly important because technology is changing rapidly, and an overly prescriptive requirement might limit innovation or quickly become stagnant. Consumers access and share their data on an array of digital devices, and the final rule should maintain the proposal's principles-based approach so that third parties have the flexibility to provide compliant disclosures on desktops, mobile devices, or even augmented or virtual reality.

Plaid has begun piloting, with select customers, authorization flows that anticipate the specific requirements proposed in the NPRM. Plaid has enclosed copies of these screens below purely for illustrative purposes so that the Bureau has an example of how a third party can adapt the regulatory requirements of the proposal to a full consumer authorization experience.



We anticipate that these screens, with appropriate modifications to include other requirements imposed by the final rule, would be used by the majority of our 8,000 customers to comply with their authorization requirements. Plaid's name is displayed in these screens, and we do not believe there are any barriers for other data access platforms identifying themselves to consumers when they are managing the authorization process. However, several clarifications, described below, would help increase consumer protection while allowing for a more competitive market.

B. The Bureau Should Make Clear That Authorization From A Single Account Holder Satisfies Third Party Obligations

The Bureau should explicitly clarify that authorization from a single account holder is sufficient to obtain data access and, in that instance, there is no requirement to notify other account holders. Such an approach is not consistent with the rest of financial services. No such notice and confirmation process is required when, for example, a consumer writes a check from a joint account or logs in to a data provider's consumer interface to access covered data from a joint account. And providing other account holders with notice and an opportunity to object to another account holder taking otherwise permissible actions also raises serious legal questions and concerns. Finally, requiring notification to every account holder would create substantial consumer friction. For example, one account holder might try to sign up for an app to pay the babysitter, only to find that they have to wait for their joint account holder, who is on a business trip in another time zone, to "approve" their use of the app. The rule provides appropriate protections for consumers in the authorization process.

C. The Bureau Should Adopt A 13-Month Reauthorization Timeline

Plaid renews its previous recommendation that the Bureau adopt 13 months as the reauthorization window to avoid consumers inadvertently losing access to their data during critically important annual financial transactions like tax preparation and filing, which from year to year may take place on slightly different timelines. But whether the Bureau selects 12 or 13 months in the final rule, the existence of the reauthorization requirement is what matters, as it gives the consumer regular intervals to reconsider their decision to share data with the third party. It also creates an obligation for the third party to secure a compliant authorization in alignment with the law on a recurring and regular basis, increasing the incentive to do it well.

D. The Bureau Should Strengthen The Consumer Protections Provided By The Authorization Procedures

The CFPB can build on the consumer protections provided by the authorization procedures by clarifying two components of the authorization requirement in the final rule.

First, the Bureau should reconsider the impact of the certification requirement in § 1033.401(b). Disclosure of all third-party obligations in § 1033.421 would result in an extensive amount of legal information for consumers to read and understand in addition to the separate terms and privacy policies that consumers typically receive in connection with their chosen third-party product. Wading through various legal documents to understand how their data is used is, as the CFPB notes, an existing hurdle consumers navigate when using digital services. The certification disclosure in § 1033.401(b) could paradoxically exacerbate this challenge. Given that the rest of § 1033.411(b) succinctly captures the key components of authorization, such as the entities involved, the categories of covered data to be accessed, and how the covered data will be used, the Bureau should consider removing the certification disclosure. **The Bureau could more**

effectively ensure that third parties act on behalf of consumers by requiring the third parties to certify to the CFPB that they will abide by § 1033.201.

Second, the Bureau should clarify that a clear affirmative action that the consumer takes on a digital interface (e.g., clicking or tapping "Agree" or "Continue") after being presented with the authorization disclosure satisfies the electronic signature requirement in § 1033.401(c). Full electronic signatures are an unusual method of obtaining express informed consent from consumers on digital interfaces such as internet browsers and applications. In order to adapt to and reflect consumer experiences on digital interfaces, privacy laws such as the California Privacy Rights Act of 2020 require the "clear affirmative action"[58] standard for gathering consumer consent rather than requiring electronic signatures. The Bureau should adopt the same approach in order to ensure that consumers have a user-friendly digital experience when consenting to third parties accessing covered data. The Bureau appears aligned to this approach based on references in 1033.441(e)(1) to "authorization disclosure that is signed *or otherwise agreed to* by the consumer" and "consumer's signature *or other written or electronic consent*" (emphases added). The Bureau should apply the same consent standard in § 1033.401(c).[59] A more onerous electronic signature requirement would be discordant for consumers when seeking innovative products and services from third parties. This requirement could also create a barrier to use and may further entrench incumbents, including credit and debit card payments, which do not have similar requirements.

Finally, the Bureau should consider changing § 1033.411(b)(3)'s disclosure requirement to disclose how the covered data will be used for the authorized third party's product or service, rather than disclosing a description of the third party's product or service. Consumers will likely have already begun interacting with the third party and be familiar with its product or service before authorizing data access with a data access platform. At that point, a description of the third party's product or service would be redundant; a description of how the data will be used, by contrast, will provide additional guidance and clarity for consumers.[60] For example, an authorized third party requiring payment for a product sold to the consumer could state that covered data enables the third party to validate the connected bank account and initiate payment.

[58] Cal. Civ. Code § 1798.140(h).

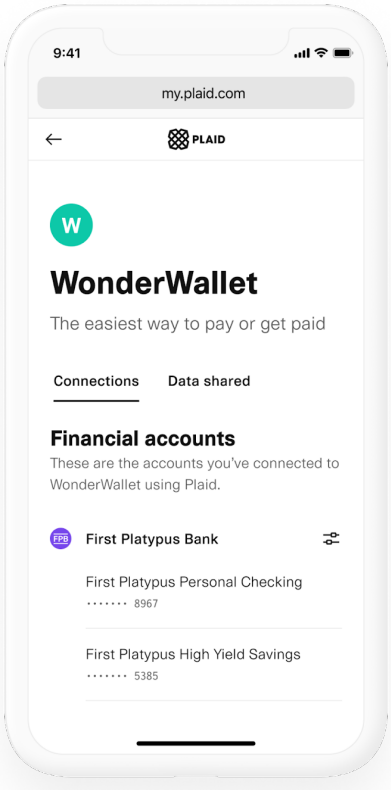
[59] The third-party record retention obligations in § 1033.441 would ensure that third parties are still required to maintain proper logs of when and how consumers took such clear affirmative actions on the third party's interface in order to provide their express informed consent.

[60] For certain use cases, such as payments on a merchant's website, the covered data is used to enable payment for the product or service purchased from the merchant, rather than for the product or service itself. In such circumstances, it is unclear whether the NPRM requires the merchant to describe its payment flow or the product or service being sold to the consumer.

E. The Bureau Should Clarify That Authorized Third Parties Can Rely On Data Access Platforms For Reauthorization

The Bureau should make explicit in the final rule that, just as an authorized third-party can rely on a data access platform for authorization, it can rely on a data access platform for periodically renewing the consumer's authorization.

This technology exists today and is well developed. For Plaid, it is the Plaid Portal.[61] Consumers who share data with an authorized third party through Plaid can create a Portal account with Plaid.[62] Once the consumer has a Portal account, they can use the Portal to see the data providers from which they have permissioned access to covered data via Plaid.[63]

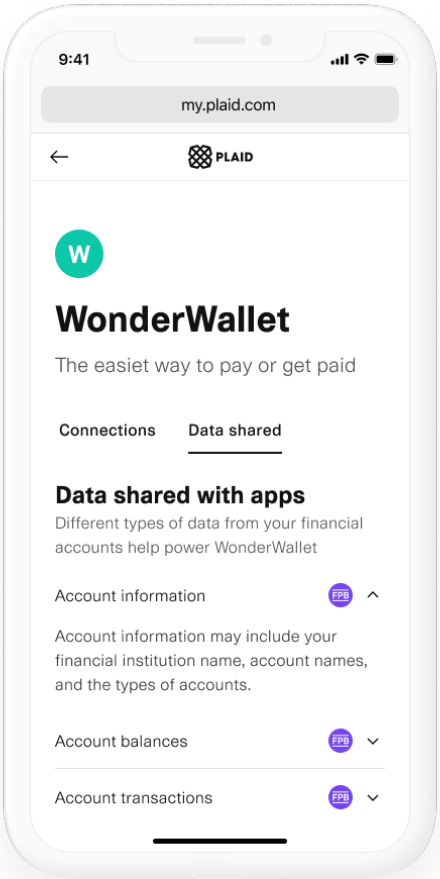


[61] Available at my.plaid.com.

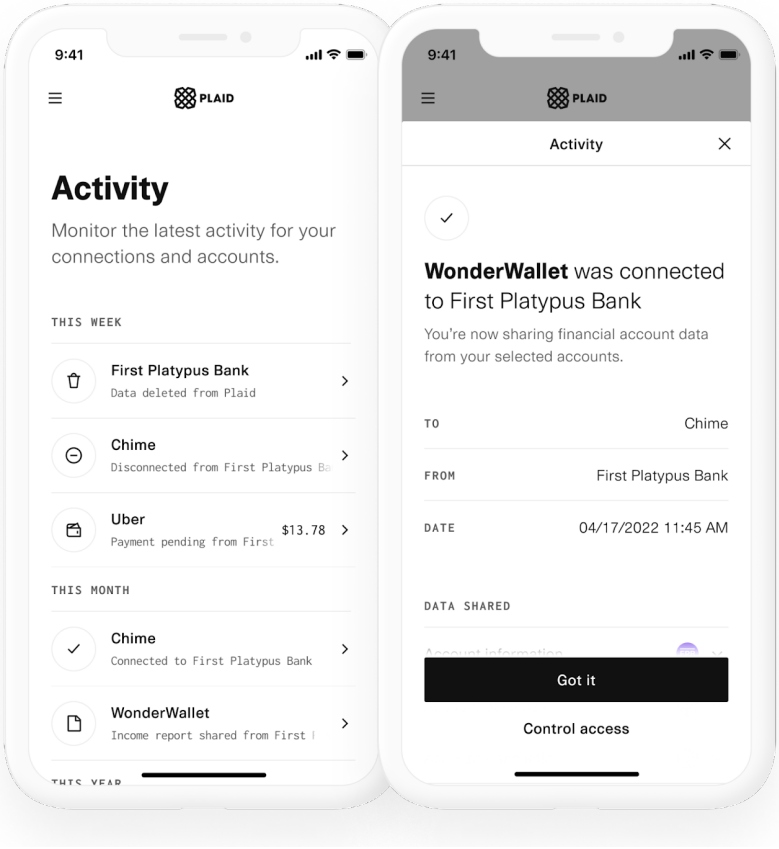
[62] Plaid offers this example only to demonstrate that the technology for data access platforms to support reauthorization exists. Although some identity verification process is necessary, consumers should not necessarily be required to create any sort of account in order to manage their reauthorization.

[63] Several data providers today contractually prohibit Plaid from displaying their institutions in Portal. This practice, which denies consumers an opportunity to see and manage their data connections wherever they find most convenient, should be prohibited in the final rule. Just as data providers are permitted to create revocation experiences in § 1033.331(e), third parties, whether data recipients or data access platforms, should be able to display information about data providers and data access on their own data management displays under § 1033.421(h).

The consumer can also see which third parties they have authorized to receive data from their data providers, as well as the types of data to which the authorized third parties have access. In the screenshot below, WonderWallet (a fictional app) is the authorized third-party, and its access to the consumer's data is displayed in Plaid Portal.



Consumers can also see a record of their data sharing activity, including a record of their authorization to share the data and when the third party last accessed the data.



Plaid Portal already automatically terminates an authorized third party's access if a consumer revokes their authorization, and makes it easy for the consumer to perform that revocation.

The Bureau requested comment on whether technology exists to automatically terminate access after a third party's authorization has ended. Plaid is developing a tool to automatically terminate data sharing every 12 or 13 months (depending on the reauthorization time frame in the final rule) unless the consumer reauthorizes the data access. Once the requirement is in place, we will be able to prompt a consumer to reauthorize multiple authorized third-parties at the same time on Portal, greatly reducing user friction and making it easy for the consumer to manage their data sharing, and for authorized third parties to comply with the reauthorization requirements in the rule.

F. Data Access Platforms Are Well Positioned To Communicate And Manage Data Access That Is Reasonably Necessary For The Use Case Being Provided By the Third Party

We are not aware of a tool that can automatically and completely limit the collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service, in part because the sources of data and tools used to collect the data are not uniform. In practice, companies put in place several data minimization techniques to avoid over-collection or retention of inadvertently over-collected data. For example, Plaid's products are designed to minimize the data accessed to what is reasonably necessary for a defined use case.[64] Data access platforms are in the position to communicate from an authorized third party to a data provider the covered data the authorized third party requires for the consumer's requested product or service, and to use technology to collect only that data for sharing with the authorized third party. For connections not involving a data access platform, the authorized third party should be required to provide similar information to the data provider on the data needed to provide its product or service, in order to ensure data minimization.

G. The Bureau Should Permit Data Providers To Build Authorization Revocation Tools For Consumers, Provided They Do Not Interfere With Consumer Access Or Competition

The CFPB is correct to give data providers the option to provide consumers with an interface allowing them to terminate their data sharing with the data provider. Consumers should be able to see and manage their data connections in whatever place best suits their needs. However, just as a data provider having a role in authorization could enable anticompetitive behavior and consumer confusion, so too could a data provider having a role in revocation. For this reason, § 1033.331(e) requires that any revocation method, "at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party." While the risks are lower in revocation because the consumer has already fully established a relationship with the authorized third party at that point and understands the full value proposition of its products or services, the Bureau should consider establishing some guardrails – in line with the general protections in subsection (e) – to ensure that data providers' engagement in revocation is solely for the consumer to have more and easier options to manage their data.

The Bureau should consider limiting data providers to reasonable communications with consumers about the revocation function. Contacting a consumer once a year to remind them to check their connections and decide whether they still want them would be commercially reasonable, particularly given the periodic reauthorization

[64] Notably, even in a screen scraping scenario, Plaid seeks to minimize the data being collected to that which is necessary for the use case that the customer specified. In situations where over-collection is not avoidable due to technical limitations with the integration with the data provider(s), Plaid's integrations adopt a "filter and purge" approach. This means that excess data is immediately discarded (i.e., not stored), and thus is not passed to the customer or used by Plaid for any purpose.

requirements in the final rule. Contacting a consumer more frequently, or using language about the risk of sharing data, particularly when sharing data is the consumer's right under § 1033 and is an approved and regulated activity, would not be commercially reasonable, and if done in a way to discourage consumers' exercising of their rights could even be unfair, deceptive, or abusive. Contacting a consumer about revocation for commercial reasons, for example to offer a consumer a product that competes with a product offered by a third party and suggesting they turn off the connection, also would not be commercially reasonable. These practices and others like them should be explicitly prohibited in the final rule.

The final rule should also require that the revocation function at a data provider not have any reauthorization functionality built into it. A data provider similarly should be prohibited from creating any way to expire data access automatically on their systems (for example access tokens that expire after a year). Reauthorization, like authorization, is the responsibility of the third party. Creating reauthorization experiences or tools at the data provider will lead to consumer confusion and a regulatory lack of clarity as to which party is responsible for reauthorization. Dueling reauthorization and expiration systems also create a risk that lack of coordination would result in unintended loss of access or conflicting instructions, and the potential for anticompetitive conduct. For example, a consumer might reauthorize at the data provider only to lose access because they did not complete their legally-required reauthorization with the third party. Similarly, a third party could decide to seek consumer reauthorization more frequently than every 12 or 13 months, in which case a data provider would be at risk of expiring a token and cutting off consumer access when there is still a valid authorization.

Finally, data providers, authorized third parties, and data access platforms should be required to communicate with each other when a consumer revokes access. The CFPB is correct to require in § 1033.331(e) that a data provider notify a third party when revocation has occurred. When a third party is using a data access platform for authorization, upon revocation the data provider should notify the data access platform, which should in turn be obligated to notify the third party. Those communications should be in near-real time to ensure that all parties can update their systems. When consent is revoked at a data provider or data access platform, they should have to provide 24 hours notice to the third party before terminating access, in case there is a pending transaction or other service that would harm the consumer if not complete, or in case of first party fraud attempts. In such instances, the data provider or data access platform should be required to notify the consumer of the 24 hour delay in revocation, so that there is no consumer confusion on when their data access terminated.[65]

[65] The Bureau could also consider creating an exception to this notice period when the data provider has substantial evidence that the consumer or authorized third party is engaged in ongoing fraud or other illegal activity, or when the consumer reports that they are a victim of account takeover or identity theft.

H. The Bureau Should Require That The Reauthorization Timeframe Run From The Time The Consumer Becomes Dormant, Rather Than From The Date Of The Initial Authorization

Allowing a third party to maintain access to a consumer's data so long as the consumer is still using the product or service (a "dormancy" test) is a compelling idea that the Bureau should adopt in the final rule, particularly for payments use cases. Consumers frequently use data access to set up recurring payments, such as rent or subscription payments. These payments are a substitute for other forms of recurring payment, such as those enabled by credit or debit cards, except that they use lower cost ACH payment rails, increasing competition and lowering costs in the payments market. Consumers reasonably expect such recurring payments to continue unless they decide to terminate them; that automation and convenience is the purpose of setting up the recurring payment in the first place. Indeed, consumers would be surprised, and at risk of direct harm, if their rent payment, which happened seamlessly and automatically for 12 or 13 months, failed because they missed a reauthorization notice. The CFPB recognizes the harm that such payment disruptions cause to consumers, and has fined companies for botching recurring payments authorized by the consumer.[66]

The final rule should explicitly recognize that the consumer's active use of a connection, including making a payment or maintaining authorization for a recurring payment, is a form of reauthorization, and permits ongoing data access without an additional 12 or 13 month reauthorization. Each payment would, then, reset the 12 or 13 month reauthorization clock. In instances where a data access platform is handling reauthorization on behalf of the third party, the Bureau should allow the third party to attest or certify to the data access platform that the consumer is still actively using their service and does not need to be reauthorized. To ensure their accuracy, the final rule should deem false attestations or certifications of non-dormancy to be a violation of the law.

I. The CFPB Should Take Additional Steps To Ensure That Consumers Do Not Experience Unnecessary Friction When Authorizing Data Access And That Third Parties' Authorization Processes Are Not Subject To Any Anti-Competitive Interference

Authorization is the most important step in the data portability process. It is the moment when the consumer is provided essential information about what data they need to access and share with their chosen third-party and for what that data will be used in order to receive the product or service they have sought. It is often part of the customer onboarding process for that authorized third party.

[66] Press Release, Consumer Fin. Prot. Bureau, Statement on Mastercard and UniRush to Pay $13 Million for RushCard Breakdowns That Cut Off Consumers' Access to Funds, Aug. 24, 2015, www.ftc.gov/news-events/pressreleases/2015/08/statement-ftc-chairwoman-edith-ramirez-appellate-ruling-wyndham.

The Bureau's proposed rule creates a clear set of consumer-friendly requirements for the substance of the authorization – i.e., disclosure and meaningful consumer control over the authorization process – to ensure that consumers understand and meaningfully consent to data access. The proposal also recognizes the authorization relationship is fundamentally between the consumer and their *chosen* third party, the one from which the consumer is seeking the product or service. The proposed rule recognizes that, if the goal is to foster increased competition among financial service providers to offer the best products to consumers, the competitive risk in permitting incumbents to handle authorization is unacceptable. Consumers should not have to give permission to their current data provider in order to obtain the services of a competitive third party. In practice, such a framework could easily turn into consumers seeking permission *from* their current data provider to switch to a competitor. And no company (i.e., a third party) should have to rely on another company (i.e., a data provider), let alone an incumbent competitor, for their customer onboarding process unless they freely choose to do so. The proposal takes the right approach, then, in assigning third parties the sole responsibility of authorization management, while also allowing third parties, should they choose, to delegate the authorization process to a data access platform. The Bureau can, however, further improve authorization management and its benefits to consumers and competition by making several adjustments to the final rule.

1. The Bureau Should Only Allow A Data Provider To Confirm The Consumer's Authorization When The Third Party Has Failed To Make A Record Of Such Authorization Contemporaneously Available To The Data Provider

The final rule should clarify that, if a consumer is redirected to a data provider's interface, the data provider may only present the consumer with a screen "confirming" that consumer's authorization if the authorized third party or their data access platform does not send or otherwise make available a record of the consumer's authorization at the time the connection is made, with sufficient details such that the "confirmation" screen would be superfluous.

There are two potential justifications for allowing a data provider to show the consumer a "confirmation" screen. The first is so the data provider can ensure that the consumer understands what they are agreeing to. However, third parties are already required to provide clear, understandable authorization disclosures under the rule, so there should be no need for a duplicative "confirmation" screen. To the extent data providers are concerned about the accuracy or legibility of a third party's authorization disclosures, those concerns can be addressed by the third party providing a record of the consumer's authorization to the data provider, which is something that Plaid does today for many of its data partners using an API, and plans to enhance when the complete authorization requirements are inscribed in the final rule. When a third party provides a record of the consumer's rule-compliant authorization to the data provider, the data provider can be sure that no additional "consumer understanding" is achieved by the data provider then "confirming" that same authorization to the consumer. This

is particularly the case when that authorization is done by a data access platform, and the language and screens used for it are consistent across thousands of third parties and millions of consumers. In such cases, all a "confirmation" would do is add a redundant step and introduce the risk that the "confirmation" is inconsistent with the compliant authorization the consumer has already provided.

The second justification for a "confirmation" screen is to enable data providers to satisfy their own compliance obligations. For example, certain regulators may want data providers to demonstrate that they have only allowed a third party to retrieve consumer data with a valid authorization. Again, this concern can be addressed by requiring the authorized third party, or their data access platform, to make available a record of the consumer's rule-compliant authorization at the time of the connection. If the third party does not make this record available, then the data provider should be permitted to use a "confirmation" screen as its record to satisfy its compliance obligations.[67] When an authorized third party or their data access platform does make this record available, a "confirmation" screen is unnecessary for compliance purposes, and simply adds unnecessary consumer friction.

The Bureau has anticipated this dynamic, and the technology necessary to resolve it. The preamble to the proposed rule recognizes that "a data provider would need to *receive information* sufficient to confirm the third party has followed the authorization procedures" (emphasis added), and proposes an alternative approach whereby "the final rule should instead permit data providers to confirm this information with the consumer only where reasonably necessary."[68] Today, the technology exists for data providers to reasonably confirm authorization without asking the consumer to confirm it – in fact many data providers already receive or can request, in real time, a record of the authorization Plaid receives from a consumer.[69] In circumstances where an authorized third party, or their data access platform, can

[67] This is another area where the CFPB may wish to engage in interagency consultation and coordination to ensure alignment with other regulators on how authorization works under the rule and the records a third party can provide to data providers of a compliant authorization.

[68] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74824, (proposed Oct. 31, 2023).

[69] Today, when Plaid handles data access authorization, we provide some data providers with authorization metadata, including the name of the authorized third party, a unique identifier for the authorized third party receiving the data, the time of when the authorization was granted, the data to which data the consumer authorized access, the accounts to which the consumer authorized access, the last time data was accessed, and when access for an authorized third party is disconnected. We also regularly share our authorization screens with data providers so they fully understand what a consumer sees during the authorization process. This information should be sufficient, under a final rule, for the data provider to confirm that a valid authorization exists. This approach allows "confirmation" by the data provider even in the context of an automated request to the data provider's developer interface, and should obviate the need for the data provider to confirm the authorization directly with the consumer.

provide this confirmation to the data provider, the final rule should not permit data providers to ask consumers to confirm this information.[70]

2. The Bureau Should Only Allow A Data Provider To Confirm The Consumer's Account Selection When The Third Party Has Failed To Make A Record Of Such Selection Contemporaneously Available To The Data Provider

The Bureau's proposal does not reflect the technical realities of how account selection is handled between a consumer, a data provider, and a third party. When a consumer is signing up for a third party's service, the third party knows what data is needed, and from what types of accounts, in order to provide the consumer's requested product or service. However, before a consumer has connected their data provider account(s) to the third party, the third party has no way of knowing exactly which accounts the consumer maintains with that data provider. For example, that consumer may have multiple checking accounts and may only wish to connect one of them to the third party.

The data provider, in contrast, knows what accounts the consumer maintains, but does not know what data is necessary for the third party's product or service and therefore does not know which accounts need to be available for selection. This can lead to friction in the consumer flow if, for example, a third party needs access to information in a checking account and the data provider presents an account selection screen that allows the consumer to select their savings account. If the consumer selects the savings account rather than the checking account, the third party will not be able to access the data it needs, and the consumer will need to restart the process, without necessarily understanding why it did not work the first time. This can be a frustrating experience and ultimately result in the consumer's abandonment of the third party, without getting the product or service they were seeking.

To address these issues, effective account selection today is generally handled with a two-step authorization process. In step one, the third party captures the consumer's authorization for the data necessary for their requested product or service. (This can include alerting the consumer to the general type of account the consumer will need to select in order to share the necessary data (i.e. checking vs. savings).) With the consumer's consent, the third party then connects to their data provider and is able to see the consumer's available accounts. In step two, the third party provides a second authorization screen to the consumer, listing only the accounts compatible with the consumer's requested product or service, and asks the consumer to authorize those

[70] The Bureau may also wish to consider alternate approaches, like permitting a data provider to send a "confirmation" email to the consumer after they have connected an account, rather than during the account connection process. This approach would give a data provider flexibility to confirm an authorization directly with the consumer if that is what their regulator requires, without interfering with a third party's customer onboarding. Particularly when paired with the right of a data provider to let consumers revoke their authorization at the data provider, this approach would better balance consumer protection, the regulatory needs of a data provider, and the competition concerns of the rulemaking than the "confirmation screen" approach.

accounts or, in instances where multiple accounts could independently satisfy the use case, asks the consumer to select which account(s) they wish to connect.

The Bureau should adopt language in the final rule that, if a third party, contemporaneous with the authorization process, provides or makes available to the data provider a record of the consumer's account selection (and authorization that is compliant with the 1033 rule), the data provider is not permitted to "confirm" the account selection directly with the consumer during the authorization process. The Bureau should also clarify that, for the purposes of the rule, authorization necessarily includes account selection, and is handled by the third party. The same technology used today to provide a record of the consumer's authorization is also used to provide a record of the consumer's account selection, and the Bureau should incentivize its adoption as the best approach to balancing consumer protection, eliminating undue friction, and competition concerns.

If the Bureau believes other types of information should be given to the data provider to satisfy the "confirmation" provision in the proposal, it should clearly identify them in the final rule. This clarity will allow third parties and data providers to understand the Bureau's expectations and to commit the resources to build tools to comply.

J. The Bureau Should Differentiate Between The Procedures For A Consumer's Initial Authorization And Those For A Consumer's Modification To Their Authorization

The Bureau should consider a specific set of authorization procedures for instances where the consumer, who has already authorized access, seeks to change that authorization, either by giving the third party access to less data, additional data (for example to enable a new product or service the consumer wants), or to permission data from an account to a second, third, or fourth (etc.) third party.[71]

When an authorized third party obtains consumer consent for an *additional* data field or fields, it should be able to use a streamlined set of authorization procedures that do not involve any redirection to the data provider (since the consumer has already been authenticated), so long as the authorized third party, or data access platform, provides a record of the change in authorization to the data provider contemporaneously with the change.[72] The same principle should be applied when multiple third parties use the same data access platform to manage the

[71] According to a nationally-representative survey conducted by the Harris Poll, 34% of consumers use between three to five fintech applications. This is an increase from 30% of consumers who reported using three to five apps in 2021, and reflects a general trend in consumers adopting a greater number of third party services over time. In fact, the same survey indicates that 20% of consumers will be using six or more third parties within the next six months. (See Appendix 2.)

[72] In these circumstances the third party is known to the data provider, and the consumer already is a shared customer between the two organizations.

account connection and authorization process. Data access platforms should be able to streamline the authorization process by handling authentication and authorization of a returning consumer, while providing a contemporaneous record of changes to the consumer's authorization to the data provider.

K. The Bureau Should Provide Third Parties With Additional Protections When A Developer Interface Is Temporarily Unavailable

The Bureau requested comment on the risk of data providers denying access requests if their developer interfaces are unavailable at the time the requests are made. The most important protection against this risk is to finalize the performance requirements in the NPRM requiring that the interface be available 99.5% of the time.[73]

The Bureau can help further reduce the risk by specifying in the final rule:

1. **A specific performance requirement for the total developer interface downtime per year that is commercially reasonable;**
2. **A mechanism, as described on page 42, for the definition of commercially reasonable to reflect the evolving upward performance of data providers' developer interfaces; and**
3. **A requirement that, if a data provider denies access because the developer interface is temporarily unavailable, the data provider notify the third party when the interface is back up so that it can re-submit the access request on behalf of the consumer.**

VIII. Third Party Obligations (§ 1033.421)

The CFPB has indicated its intent to promulgate a consumer data rights rule that promotes privacy and competition "by promoting standardization and not entrenching the roles of incumbent data providers, intermediaries, and third parties . . . ."[74] These goals are sensible and laudable given that § 1033 is fundamentally about consumers having control of their own data. Unfortunately, as presently formulated, the NPRM instead increases the risk of consumer confusion about their data rights, reduces consumer choice, and increases the likelihood that incumbents will be unfairly advantaged and able to extend their dominant positions in financial services.

The Bureau's consumer data rights rule does not exist in a vacuum. Companies serving consumers in financial services are already subject to various regulatory regimes governing

[73] Plaid's monitoring of API performance for the seven largest data providers over the three months before this comment indicates this is a readily attainable standard.

[74] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74800, (proposed Oct. 31, 2023).

consumer data, including most notably the Gramm-Leach-Bliley Act and some state privacy laws. None of these regimes goes so far as to prevent consumers from being able to control how their data is used or to deny them certain benefits (they instead promote consumer understanding and choice). Yet the proposed rule may – unintentionally – have this effect. While limiting data collection, use, and retention to only what is "reasonably necessary" to provide the consumer's requested product or service appears to be a simple rule, it overweights the implied correlation between the way the data is collected (i.e., by a third party) and consumer harm. The approach also under-appreciates benefits to consumers from reasonable data use that is not strictly necessary to deliver a specific product or service. It also artificially distinguishes between protections afforded to data that consumers choose to give to a third party and to data that consumers choose to give to a data provider. Without modification, the proposed rule will confuse consumers, prevent critical anti-fraud efforts, undermine underbanked and unbanked consumers' access to financial services, stifle innovative and competitive product development, and further entrench incumbents – all of which run counter to the very aim underpinning the rule: to put the consumer in the driver's seat as to how their data is shared and used.

To avoid these problematic results, we recommend that the Bureau focus its regulatory attention on the harms and risks it seeks to address – i.e., the targeting of consumers by businesses which profit from the undisclosed sale of consumers' data to other businesses that the consumer has not chosen. The Bureau can do this by ensuring meaningful consumer control and understanding, rather than by placing novel restrictions on consumer-permissioned data in a manner that actually harms both consumers and third parties (and serves to benefit only incumbents). Building on the Bureau's stated goals and the background of existing data privacy laws, for which the rulemaking process should account, we recommend the Bureau:

- **Clarify the "reasonably necessary" standard to work alongside current privacy law standards, general consumer understanding and expectations, and commonplace, beneficial data collection and use;**
- **Remove the blanket ban on secondary data use and replace it with an opt-out / opt-in structure that adheres to current privacy law standards and allows consumers to maintain meaningful control over their data;**
- **Make clear that fully anonymized data does not constitute personal information and thus is not subject to any use restrictions; and**
- **Ensure that any privacy protections in the rule are applied to covered data, regardless of whether that data is held by a data provider or a third party.**

A. The Bureau Should Clarify The "Reasonably Necessary" Standard To Ensure That Commonplace And Beneficial Collection, Use, And Retention Of Covered Data Are Permissible

Section 1033.421(a)(1) limits third parties' collection, use, and retention of covered data "to what is reasonably necessary to provide the consumer's requested product or service." Although the

Bureau provides some non-exhaustive examples of "reasonably necessary" uses, the CFPB does not otherwise define the term. Without further clarification as to the meaning of "reasonably necessary," this ambiguous provision could result in a number of commonplace and beneficial uses being treated as banned secondary uses, contrary to the CFPB's stated intent to ensure "third parties accessing covered data are acting on behalf of consumers, *while providing sufficient flexibility to third parties to provide consumers with their requested products or services*." (emphasis added).[75] In particular, the lack of clarity about routine and worthwhile uses of data creates a high risk of disputes between data providers and third parties as to what data is "reasonably necessary" to be collected, used, and retained, despite the fact that "[t]he CFPB has preliminarily determined that third parties are in the best position to determine what covered data are reasonably necessary to provide the requested product or service." Such disputes will hinder consumers being able to access the services they need in a timely manner, and will stifle efforts to manage risk, prevent fraud, conduct research, and improve products, consumer experiences, and available options for consumers.

The examples currently included as permissible in proposed § 1033.421(c) are not sufficient to protect against these risks because § 1033.421(c) applies only to the *use* of covered data, and not to its *collection or retention*, and it also leaves out or is ambiguous as to several commonplace and beneficial reasons for the collection and use of covered data that should be permitted under § 1033.421(a). These beneficial reasons include:

- **Allowing consumers to exercise their data rights**: Under the draft "reasonably necessary" standard, third parties arguably may not be able to collect or use identity information, even though the third party needs that information in order to act upon a consumer's data deletion or similar request. In many cases such identity information is used to locate the consumer's data within the third party's systems. For example, a personal financial management application may only require access to a consumer's transaction data to provide its service, but would need identity data to fulfill a consumer's request to correct or delete their data. A lack of identity information also hinders third parties' ability to send privacy and security notices to the consumer, which consumers have the right to receive and third parties have the obligation to provide.

- **Combating fraud and protecting consumers**: Although the NPRM lists "prevent[ing] actual or potential fraud, unauthorized transactions, claims, or other liability" as "reasonably necessary" uses, this definition is ambiguous, and too narrow to appropriately protect consumers. As drafted, the proposed rule might be interpreted by some ecosystem participants to permit data to be used only to prevent an individual fraudulent transaction. But beyond extremely basic fraudulent activities, preventing fraud in a complex system often depends on access to a wide range of data to enable anomaly detection, learn and identify patterns of fraud, and identify fraudsters operating in multiple areas of a system, among other strategies. These patterns and connections

[75] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74832, (proposed Oct. 31, 2023).

may also help identify other risks associated with complex systems and protect consumers and other participants across the open finance ecosystem. Moreover, the limit to merely "fraud" prevention could lead to other types of harms being overlooked, such as money laundering, trafficking, or other harmful activities. Further, although the CFPB recognizes that covered data can be *used* to protect consumers as detailed above, third parties need to be able to ***collect***, use, and ***retain*** covered data for such purposes. This is critical for the development of new or improved anti-fraud and security tools.

- **Offering consumers effective and improved products:** While the proposed rule allows covered data to be used for "servicing or processing the product or service the consumer requested," the Bureau should clarify the scope of this reasonably necessary use to ensure it encompasses third parties' routine collection and use of consumer data to personalize or tailor products, improve quality, support customers, and innovate based on usage, history, and preferences. This is not a new or novel business activity, although digitalization allows it to be done in ways that are more responsive to individual consumer needs. If businesses stop doing this kind of continuous improvement because of the ambiguity in the rule, it will reduce the quality and effectiveness of products offered to consumers over time.

- **Helping consumers and ecosystem participants troubleshoot**: It is typical for businesses to collect and use data for a primary purpose and then also use that data for ongoing troubleshooting. Covered data may be captured in error logs, debugging tools, user feedback and support tickets, or API logs in order to monitor for and address problems that arise during consumer use of services. The rule is unclear as to whether these are reasonably necessary uses, but without these kinds of data it would be impossible for companies to adapt to an ever-changing technical environment where consumers, data providers, and third parties are not operating in a uniform and consistent manner.

The Bureau should also make clear that third parties can use previously-collected and retained covered data as "reasonably necessary" to provide an additional product or service the consumer requests at a later time, without this re-use constituting a secondary use. For example, a consumer could sign up for a third party application that provides both personal financial management services and loans. If the consumer signs up for the personal financial management services, the third party will be authorized to collect and use the consumer's transaction data to track expenses and deliver other features. Six months later, the consumer could decide to apply for a loan from the same third party. If the third party uses cash flow underwriting, its use of the previously-collected transactions data, which has been regularly updated for the personal financial management service, should be explicitly designated as a "reasonably necessary" use. In other words, if a consumer decides – after receiving an initial product or service – that they would like to receive another product or service, the third party should be permitted to use the data that was previously collected and stored for purposes in

order to facilitate the consumer's request for the second product.[76] In such circumstances, where a consumer has chosen to do business with a firm, the consumer and the firm should be permitted to expand their interaction to include additional products or services without having to reauthorize a new collection of data.

In line with our comments above, the Bureau should clarify the proposed definition of "reasonably necessary" as follows:

> 1033.421 Third party obligations. (a) General limitation on collection, use, and retention of consumer data—(1) In general. The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service, **including**:
>
> > **(i) to provide, service, process, and improve financial products or services within the meaning of 12 C.F.R. § 1001.2;**
> >
> > **(ii) to effectuate a consumer's authorization, re-authorization, revocation, deletion, or other data rights request; or**
> >
> > **(iii) for additional reasonably necessary purposes, such as:**
> >
> > > **(a) fulfilling legal obligations;**
> > >
> > > **(b) preventing, detecting, investigating, or protecting against actual or potential fraud, money laundering, human trafficking, unauthorized transactions, claims, other liability, security threats, or other similar activities;**
> > >
> > > **(c) protecting third party rights and property;**
> > >
> > > **(d) protecting others in the ecosystem from harm;**
> > >
> > > **(e) supporting risk management; or**
> > >
> > > **(f) troubleshooting or to provide consumer or technical support.**
>
> **Nothing in this section shall be construed to limit a third party's re-use of covered data collected in accordance with this paragraph (a) to provide an additional product or service requested by the consumer.**

[76] The third party also, in this instance, should not have to allow the data provider to authenticate the consumer or confirm their authorization. The third party already has the data and is engaging directly with their consumer about a new product the consumer wants. No new data is being accessed on the data provider's developer interface.

B. Subject To Appropriate Consent Mechanisms And Consumer Protections, The Bureau Should Permit Processing Data for Secondary Purposes That Promote True Consumer Control And Competition

The proposed rule contains a blanket prohibition on third parties processing covered data for secondary purposes – i.e., any collection or use beyond what it is "reasonably necessary" to deliver the product or service requested by the consumer. The CFPB acknowledges that "[o]ther options would have allowed third parties to ask consumers to opt in to or opt out of processing for secondary purposes, including an approach that would not have permitted third parties to ask consumers to opt in to certain 'high-risk' secondary uses," but opted for a blanket prohibition to ensure the "third parties accessing covered data are acting on behalf of consumers." This prohibition goes further than other data privacy laws – and further than necessary to accomplish the CFPB's aims of consumer control and benefit. In fact, the blanket prohibition on secondary use, in certain cases, may actually have the unintended consequence of denying consumers the very control and benefits the CFPB is attempting to secure through its rulemaking.[77]

1. The Blanket Prohibition On Collection, Use, Or Retention Of Covered Data For Secondary Purposes Goes Further Than Any Other International Or US Federal Or State Privacy Law

Reference to other privacy laws makes clear that the CFPB's proposal is at odds with other US federal and state privacy laws – and even European privacy law.

Chart Demonstrating § 1033's Divergent Positions Compared to Other Laws

	1033	GLBA	CCPA/ CPRA	CPA	VCDPA
Jurisdiction	Federal	Federal	California	Colorado	Virginia
Entities subject to restrictions	Third parties only.	All Financial Institutions (which includes	For-profit businesses that do business in	Legal entities that conduct business in CO	Persons that conduct business in VA

[77] As Chairman Patrick McHenry wrote in his December 13, 2023 letter, "[C]ompletely prohibiting the use of secondary data does not benefit consumers. It would prevent financial institutions and third-party service providers from improving on existing products or services (including the very product or service the consumer has requested); or building new products or services (including products and services that may be substantially similar to the product or service the consumer has requested). Not only does this risk harm to consumers who may benefit from these new and/or improved products and services, it hinders innovation – the very innovation that allows the United States to be a global leader in the financial services industry." *See* United States, Congress, House, House Financial Services Committee, *RE: 12 CFR Parts 1001 and 1033, Notice of Proposed Rulemaking: Docket No. CFPB - 20230052*, Chairman Patrick McHenry, Dec. 13, 2023, available at financialservices.house.gov/uploadedfiles/2023-12-12_1033_letter_12.12.2023_final.pdf.

		§ 1033 data providers and many third parties).	CA (and meet additional criteria); with carve-outs for data collected, processed, sold, or disclosed subject to GLBA, regardless of what type of entity holds it.	or produce / deliver commercial products / services to residents (and meet additional criteria); with all GLBA Financial Institutions carved-out.	or produce products / services to residents (and meet additional criteria); with all GLBA Financial Institutions carved-out.
Purpose limitation?	"Reasonably necessary" to provide a product or service a consumer requested.	No.	"Reasonably necessary and proportionate" to achieve the purposes for which the personal information was collected or processed, OR "for another disclosed purpose that is compatible."	No, but must specify express purpose in notice. Consumer consent required to process "sensitive data," with some exemptions.	Reasonably necessary and compatible with disclosed purpose. Consumer consent required to process "sensitive data."
Restriction on secondary use?	Blanket prohibition.	No.	Consumer consent required. For "sensitive personal information," a consumer also has the right to limit use to that use which is necessary to perform the services or provide the goods reasonably expected.	Consumer consent required beyond uses that are reasonably necessary or compatible with the specified purpose.	Consumer consent required.
Restriction on advertising?	Yes.	No.	No – as long as compatible with purposes for which the data was collected.	Opt-out right for targeted advertising.	Opt-out right for targeted advertising.
Restriction on cross-selling products and services?	Yes.	No.	Consumer consent required. "Business purposes" include "advertising and marketing services, except	Opt-out right for targeted advertising.	Opt-out right for targeted advertising.

			for cross-context behavioral advertising."		
Restriction on sale of data?	Yes.	Opt-out right, subject to numerous exceptions.	Opt-out right.	Opt-out right.	Opt-out right.
Restriction on use of deidentified data?	Yes – blanket prohibition.	No.	No.	No.	No.

The above chart demonstrates that existing privacy laws[78] imbue consumers with meaningful controls over and choices with respect to their data by focusing on the reasonable expectations of consumers and otherwise requiring consent or the opportunity to opt-out as a means to limit expansive data collection and use.

2. The Blanket Prohibition On Secondary Data Use Has The Potential To Inadvertently Thwart The Proposed Rule's Consumer Benefits And Procompetitive Effects

The CFPB's stated aims are undermined by a blanket secondary use prohibition:

- **Consumer control and understanding**: The CFPB relies on the assumption that any "collection, use, and retention of covered data beyond what is reasonably necessary for the product or service the consumer requested would undermine the consumer's understanding of the authorizations they provided . . . [and] undermine a consumer's ability to control their data."[79] However, other state and global privacy laws recognize consumers' agency to either opt-in to or opt-out of certain secondary uses. By depriving consumers of this agency, the CFPB in turn deprives them of true control over how their data is used, as well as the potential benefits of such use, described below.

- **Benefits to the consumer**: Implicit in the CFPB's blanket secondary use prohibition is the assumption that processing data for secondary purposes *cannot* benefit consumers, but this is not the case. To the contrary, certain secondary uses – beyond

[78] In addition, under GDPR, personal data can be processed on the basis of consent or some other legitimate basis "taking into consideration the reasonable expectations of data subjects based on their relationship with the controller." *See* GDPR, Recitals 40 and 47. This could include when "necessary for the purposes of preventing fraud" or "for direct marketing purposes." *See* Recital 47. Further, processing of personal data for purposes other than those for which it was initially collected is explicitly allowed (1) with consumer consent or (2) when compatible with the purposes for which it was initially collected. *See* Recital 50.

[79] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74833, (proposed Oct. 31, 2023).

those reasonably necessary to provide the specific product or service the consumer requests – are expressly intended to provide consumer benefits, yet would not be permitted under the rule. For example, research and development and personalization services are often secondary uses that specifically benefit consumers.[80]

- **Innovation and competition**: Although the CFPB notes "that an expanded range of third party products and services would increase competition and innovation, offering important secondary benefits to consumers, including improved credit access and lower prices," its prohibition on secondary data use undermines this aim.[81] In particular, as currently structured, covered data cannot be used by third parties "for the development of new products outside the scope of the original authorization."[82] This places third parties at a distinct disadvantage – particularly in light of the fact that data providers are not subject to the same restriction – by limiting their ability to innovate. The competition driven by open banking has hinged in large part on third parties using covered data to innovate and craft new and competitive services, to improve existing products, and to develop new use cases. In general, incumbents have innovated only in response to the competitive threat posed by innovations introduced by challengers.[83] A blanket restraint on general product development and improvement – without even allowing for an opt-out or opt-in – is akin to a blanket restraint on innovation and trade.

[80] For example, Saverlife is a nonprofit and advocacy organization focused on improving the financial health of people living on low-to-moderate incomes. Saverlife does this in three ways: (1) a fintech product offering to consumers, (2) research and insights, and (3) policy and advocacy efforts. These three pieces work in tandem with one another. As part of Saverlife's fintech product offering, consumers can share data from their financial accounts in order to receive personalized financial content and savings rewards and incentives. In addition, Saverlife uses this data to (i) refer its consumers to trusted resources and products that may help them to lead better financial lives and (ii) perform research that in turn informs its policy and advocacy efforts – all of which are aimed at giving consumers greater control and voice. Without the "secondary" use of their consumers' data, Saverlife's social impact goals and advocacy efforts – both of which are expressly intended to benefit consumers – would be negatively impacted, if not fully stymied. *See* about.saverlife.org/.

[81] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74858, (proposed Oct. 31, 2023).

[82] *Id.* at 74855.

[83] For example, Venmo launched its peer-to-peer payment service in 2009. CashApp launched its peer-to-peer service in 2013. Incumbent-owned Zelle launched its peer-to-peer service in 2017. If challengers are not permitted to use data to innovate their products, incumbents have much less competitive incentive to innovate themselves, even if regulation locks in an uneven playing field that gives them the right to innovate where challengers cannot. *See also* Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74798, (proposed Oct. 31, 2023). ("While many major use cases began as innovative offerings by third parties, incumbent financial institutions have adopted many of them in response to consumer demand.").

3. Following Models Adopted By Other Regulators, The CFPB Should Allow Secondary Data Uses That Promote Consumers' Meaningful Control Over Their Data

In line with the SBREFA Panel's recommendation "that the CFPB consider where it can give flexibility to third parties while still achieving its consumer protection objectives," **we respectfully suggest that the following alternatives to a blanket secondary data use prohibition (applied uniformly to data providers and third parties) would allow the CFPB to more fully realize its objectives:**

- **Require third parties to allow consumers to opt-out of secondary uses compatible with the primary purpose**: For uses that extend beyond the "reasonably necessary" standard, but which are still compatible with the consumer's primary purpose in sharing data, the CFPB should permit consumers the ability to opt out. Such compatible uses include, for example, 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. This type of ongoing commercial relationship between a consumer and a business is common across all industries, and is explicitly permitted, with the right to opt out, in jurisdictions such as Canada, the European Union, and Australia.

- **Require third parties to allow consumers to opt-in to secondary uses beyond those related to the primary purpose**: For other secondary uses, the CFPB should permit consumers the ability to opt in, and should make clear that such opt-ins must be freely given and informed. This puts the consumer in the driver's seat and fully in control over how their data is used, and will prevent the use of dark patterns to mislead consumers into granting consent. Examples of such uses could include lead generation or for marketing by an entity other than the company with which the consumer is already a customer.

To ensure that consumers "understand the scope of [their] authorization and [are] not reluctantly acquiescing to data collection, use, and retention that they do not want," the CFPB should ensure that opt-out and opt-in rights are paired with strong authorization disclosures[84]. The CFPB can rely on its UDAAP authority to ensure the clear disclosure of material information and to prohibit misleading statements, omissions, or dark patterns. The CFPB can also ensure that a consumer's meaningful control is protected by expressly prohibiting any entity from discriminating against the consumer for deciding to opt-out or refusing to opt-in. This will protect the consumer's ability to seek and receive their requested product or service. Finally, the Bureau should consider focusing any ban on secondary uses on the negative consequences that it seeks to prevent, such as harmful targeting of consumers when their data is sold without their

[84] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74832, (proposed Oct. 31, 2023).

informed consent, which also will reduce the likelihood that the Bureau's rule will hinder competition.

C. The CFPB Should Exclude De-Identified Data (Anonymized) Data From Any Use Restrictions

As the SBREFA panel noted, de-identified data can be used for a broad range of research, development, and product innovation purposes that benefit consumers and support a healthy marketplace. To restrict the use of this data would hinder the consumer-centric innovation and choice this rule aims to promote and would be at odds with global precedent.

De-identified data is, by its very nature, anonymous and not associated with any consumer. Given this, it does not have any privacy implications and therefore should not be considered personal information or subject to privacy restrictions under the final rule. This is consistent with global precedent, including state and European privacy laws. Data that is re-identifiable has *not* been truly de-identified; put differently, core to the definition of de-identified data is the fact that such data cannot be reasonably re-identified. Given there are well-accepted global standards for de-identification, the CFPB could set a clear standard for de-identification in its final rule.[85]

Subjecting de-identified data to use restrictions severely restricts third parties' ability to use that data to improve their products and develop new products, including building fraud mitigation and security tools that make the open finance ecosystem safer. This is particularly the case when third parties and data providers are arbitrarily subjected to different use restrictions with respect to the *same* data sets. As "financial institutions" under the GLBA, data providers routinely package and distribute de-identified information for marketing purposes, and placing restrictions on third parties (including when data providers act as third parties) sets an inconsistent standard that further enshrines incumbents' competitive positioning in the market.

[85] *See, e.g.,* CPRA § 1798.135(m) (defining "de-identified"); Irish Data Protection Commissioner, Guidance Note: Guidance on Anonymisation and Pseudoanonymisation, June 2019, available at www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf ("Where data has been anonymised to such an extent that it would not be possible to identify an individual in the anonymised data even with the aid of the original data, the data has been fully anonymised and is not considered personal data.").

D. The Bureau Should Ensure Consumers Benefit From Consistent Protection Of Their Data By Applying Any Privacy Requirements To Third Parties *And Data Providers*

1. The Uneven Application Of Privacy Protections To Consumers' Data Undermines The Bureau's Aims Of Consumer Benefits, Consumer Control, And Competition

The NPRM applies data privacy protections only to third parties with respect to their collection, use, and retention of covered data. Specifically, § 1033.421(a)(1) provides, "The *third party* will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service." (Emphasis added.) Although data providers also collect, use, and retain this *same data* in the normal course of their business, they are not subject to the privacy protections in the NPRM. Instead, they are generally only subject to those restrictions in the GLBA – which, unlike the NPRM, do not contain any restrictions on the use of that data. (See chart below.) In short, when a data provider holds consumers' data, it is subject to limited use restrictions under the GLBA, yet when a third party holds that same data because the consumer has affirmatively chosen to give it that data, it would be subject to extremely stringent requirements under the NPRM. The result would be that consumers have inconsistent protections for the same data, depending solely on whether they permissioned it to a data provider or a third party.

Plaid supports the CFPB's efforts to promote the primacy of benefits to consumers and their meaningful control over the collection, use, and retention of their data. However, the application of privacy protections only to third parties, and not to data providers, undermines these efforts and subjects consumers' own data to incongruous treatment simply depending on who "holds" it – even where the holder is a company to which the consumer has affirmatively chosen to give their data.[86] The CFPB acknowledges that there are consequences to – or, as the Bureau puts it, "indirect effects" of – the inconsistent treatment of consumers' same data and participants in the open finance ecosystem.[87] But while the CFPB appears to view these indirect effects as somehow unavoidable or acceptable, that is not the case. There is no reason a consumer should have to bear these *significant* indirect effects, including having fewer rights, when they allow a data provider to collect and use their data than when they do the same with respect to a third

[86] When a consumer signs up to use a bank, they are agreeing that the bank will have access to their financial data, namely the data they generate by using that bank's financial service. When a consumer signs up for a non-bank, they are agreeing that the non-bank will have access to their financial data, namely the data they generate by using that non-bank financial service. This choice is no different than when the consumer chooses to share some of their financial data from the non-bank to the bank, or from the bank to the non-bank.

[87] "The proposed rule would also have some indirect effects on the value of first party data held by data providers. . . . While the CFPB does not have data to quantify the benefits to data providers, all else equal, this is likely to increase the value of first party covered data held by data providers, which generally does not have these restrictions." *See* Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74855, (proposed Oct. 31, 2023).

party collecting and using the same data. Nor is there any reason why the market should have to bear these indirect effects, not least of which is the potential for incumbent data providers to leverage their less-restricted use of consumers' data to market, cross-sell, and otherwise engage in conduct designed to increase switching costs and effectively discourage consumers from availing themselves of competing, innovative services.

Chart Demonstrating The Incongruent Treatment Of The Same Covered Data

Nature of consumer protection	**GLBA (Applicable to Data Providers)**	**Proposed Section 1033.421 (Applicable to Third Parties)**
Restriction on primary use?	No.	Yes.
Restriction on secondary use?	No.	Yes.
Restriction on targeted advertising?	No.	Yes.
Restriction on cross-selling products and services?	No.[88]	Yes.
Restriction on disclosure of data to non-affiliated entities?	Sometimes. Notice and a reasonable opportunity to opt-out are required prior to disclosure. However, there are a number of exceptions to the need to provide an opt-out.[89]	Yes. A consumer is prohibited from consenting to any uses that are not "reasonably necessary," regardless of what they might want.

[88] 12 C.F.R. 1016.13(b) ("The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.").

[89] Exceptions under 12 C.F.R. 1016.13-.15 include sharing for service providers and joint marketing; for processing transactions at consumer's request or as necessary to effect, administer, or enforce a transaction; with the consent or at the direction of the consumer; to protect the confidentiality or security of records; to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; for required institutional risk control or resolving consumer disputes or inquiries; to persons holding a legal or beneficial interest relating to the consumer; to persons acting in a fiduciary or representative capacity on behalf of the consumer; to provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating you, persons that are assessing your compliance with industry standards, and your attorneys, accountants, and auditors; to the extent permitted or required by law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.) to law enforcement agencies; to a consumer reporting agency in accordance with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) or from a consumer report reported by a consumer reporting agency; in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit; to comply with Federal, state, or local laws, rules and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance, or other purposes as authorized by law.

While the CFPB's inclusion of data privacy protections in the NPRM may be driven by a belief that GLBA provides insufficient protections for consumers,[90] unevenly-applied protections actually subvert the very consumer benefits the CFPB aims to achieve, while risking consumer confusion and harm to competition:

- **Subversion of CFPB's efforts to create consumer benefits and control through the NPRM**: A consumer cannot benefit from data privacy protections if they are inconsistently applied to the same data. The result of the uneven applicability of the NPRM's proposed data privacy protections is that consumers sometimes have control over their data, but sometimes not. Their data is sometimes subject to use restrictions, but sometimes not. Their data cannot be sold by third parties, but may be sold by data providers. Their data cannot be used for targeted advertising by third parties, but can by data providers. Because the privacy protections do not apply to data providers, consumers' covered data will still be used and shared by data providers in ways that are directly at odds with the text and intent of the rule – and data providers will paradoxically be treated with more agency over consumers' data than consumers themselves.

- **Risk of consumer confusion**: By creating incongruous standards applicable to the same data, the CFPB risks creating consumer confusion as to what protections consumers are afforded with respect to that data. Consumers may generally expect that the same data – their data – will be afforded the same protections regardless of whether an incumbent data provider or a competing third party are providing the service to the consumer. Confusion as to the protections afforded their data may lead not only to a lack of understanding of who can do what with their data, but also to inconsistent exercise of the rights and controls consumers have over that data. It will also result in longer, more confusing privacy notices for entities acting as both data providers and third parties.

- **Risk of unfair competition as a result of incumbent data providers' unrestricted use of consumers' data**: If third parties are restricted in their use of covered data, *but data providers are not*, then those data providers will be able to use consumers' same data to market and cross-sell to consumers[91] in ways that promote their

[90] Director Chopra has stated, "The Gramm-Leach-Bliley Act requires that consumers are provided with a notice and a right to opt out of certain data collection and sharing practices. I am concerned that this privacy notice is ineffective." *See* Prepared Statement of Director Rohit Chopra before the House Committee on Financial Services, Dec. 14, 2022. Available at www.consumerfinance.gov/about-us/newsroom/prepared-statement-of-director-chopra-before-house-committee-on-financial-services/.

[91] A review of data providers' GLBA consumer privacy notices confirm that many data providers disclose to consumers that their data will be shared for, among other things, (i) the data provider's marketing purposes (to market the data provider's services to the consumer); (ii) joint marketing with other financial companies (i.e., a formal agreement between non-affiliated financial companies that together market financial products or services to the consumer); and (iii) their affiliates' everyday business purposes (with

products above the competitive, innovative ones being offered by third parties. This uneven treatment will also allow incumbents to develop and improve their products in ways that third parties attempting to compete under the proposed rule cannot. In turn it will prevent consumers from easily deepening their relationships with their chosen third parties, further entrenching incumbents and risking the very competition that the CFPB hopes to engender by virtue of its proposed rule. It also will create an opportunity for regulatory arbitrage, creating a competitive advantage for data providers that may encourage the additional monetization of consumers' data.

- **Risk of unfair competition through unrestricted access to third party data**: Under the NPRM, data providers will be entitled to receive significant information about the third party services consumers are choosing to use (*see, e.g.*, § 1033.321(d) (basis for denials), 1033.331(b)(2) (ability to confirm scope of authorization)). There are no restrictions on data providers' use of this information, including no restriction that such information can only be used by data providers in line with the purpose for which it was collected. As a result, data providers will have detailed insight into what third party services their consumers use, how many of their consumers use a particular service, what data is needed for that service, and more. They can take action based on that data (i.e. secondary uses of that data), including targeted advertising and other product efforts designed to shift consumers away from those competing services.

- **Technical burdens and costs on small (and other) businesses**: Many data providers already act as third parties (i.e., as both providers and recipients of covered data). Incongruous treatment of the same type of data will impose technical burdens and costs on those entities, which would incur the costs of building and maintaining the technological capabilities and databases to appropriately segregate and restrict use of the same data, depending solely on whether they hold that data as a data provider or third party. Smaller banks, credit unions, and digital wallets will struggle to "steal the lunch" of bigger banks if they can only do so while building and maintaining separate databases to house identical types of data.[92]

These are real risks that, at best, diminish consumer benefits and, at worst, cause consumer harm. To take one example, imagine a consumer who is in the market for a mortgage and who uses a third party's service to comparison shop and ultimately select the best rate, all of which is made possible because the consumer can share data from their data provider bank with their chosen third party. Based on the same data the consumer shared with the third party to receive their requested service, the third party can also see that, at the consumer's data provider bank,

---

respect to information about the consumer's transactions and experiences). Consumers generally cannot opt out of sharing with respect to these particular purposes.

[92] John Heltman, *Chopra: Open banking helps small banks 'steal the lunch' of big banks,* American Banker, Oct. 20, 2023, available at www.americanbanker.com/news/chopra-open-banking-helps-small-banks-steal-the-lunch-of-big-banks.

the consumer's current savings rate is far below the national average and their checking account charges a monthly fee for not maintaining a minimum balance.[93] However, given the NPRM's blanket prohibition on secondary use, the third party cannot use that data to offer the consumer a market-equivalent savings rate or even a free checking account. At the same time, the consumer's data provider-bank can see which third party the consumer is using and what data the consumer shared and, knowing the consumer is in the market for a mortgage, may provide this information to a non-affiliate marketing company, which could then target the consumer with direct mail for unwanted home warranty products – something the consumer cannot opt-out of and which is not prohibited under GLBA. The end result is that the third party is prevented from providing a beneficial service to the consumer (even if the consumer wants that service), while the data provider is free to monetize its knowledge that the consumer is seeking services from a third party.

As discussed below, there are ways the Bureau can protect against the risks outlined above, while still protecting both consumers and competition.

2. The Bureau Should Use Any Of A Number Of More Effective And Comprehensive Alternative Approaches Available To Advance Consistent Data Collection And Use Restrictions Across The Entire Open Finance Ecosystem

In § 1033 of the Consumer Financial Protection Act of 2010, "Congress explicitly recognized the importance of personal financial data rights."[94] The CFPB, by issuing a rule to implement § 1033, "intends to accelerate the shift to a more open and decentralized system" for facilitating access to personal financial data. (*Id.*) This can only happen if consumers benefit from congruent, consistent protections of their data. **In order to avoid the consequences outlined above, Plaid respectfully suggests the following:**

- **Encourage Congress to pass a federal privacy law or to amend GLBA**: GLBA is the federal privacy law that requires "financial institutions" to explain their information sharing practices to consumers. It applies to data providers and many (if not all) third parties. Instead of putting in place new limitations applicable only to data collected by third parties (even though that very same data is also collected by data providers in the normal course of their business and should be entitled to the same protections), the Bureau should encourage Congress to amend the already-existing GLBA framework and apply one improved standard across the entire financial services industry. Such an

[93] Ann Carrns, *Many Banks Pay High Rates on Savings. So Why Aren't You Moving Your Money*, The New York Times, Feb. 3, 2023, available at www.nytimes.com/2023/02/03/your-money/savings-account-rates-banks.html.

[94] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, (proposed Oct. 31, 2023).

amendment would ensure a consistent standard that consumers could rely on, and parity in terms of the treatment of consumers' data.[95]

- **Undertake a GLBA rulemaking**: The CFPB could undertake a GLBA modernization rulemaking as it has several times in the past[96] to ensure the uniform application of any data privacy restrictions to all "financial institutions."

- **Issue broader guidance regarding the intersection of data privacy and UDAAP**: The CFPB could issue an advisory opinion, circular, or bulletin analyzing primary and secondary data uses under a UDAAP framework. The CFPB has previously taken such an approach with respect to information security standards.[97]

- **Apply any 1033 data privacy restrictions to all ecosystem participations**: Finally, to the extent the CFPB believes that the § 1033 rulemaking is the appropriate vehicle for new privacy protections, Plaid respectfully suggests, at minimum, that the CFPB ensure those protections apply uniformly to both third parties and data providers.

IX. Remaining Considerations

A. The Final Rule Will Reduce The Cost Of Negotiating Data Access Agreements, And The Bureau Should Confirm That Such Data Access Agreements May Not Be Used To Circumvent The Proposed Rule's Broad Access Rights

The Bureau requested information on whether the rule will reduce the time and cost of negotiating these agreements. It will. Plaid estimates that at least 30% of negotiating time on historic data access agreements was on matters that would be subject to consistent standards under the proposed rule. Other areas of negotiation could arise as a result of the final rule, but this is unknowable until the rule is finalized.

The proposed rule will limit the costs of negotiating data access agreements, but the CFPB's final rule should state that data access agreements between a third party and a data provider are not required as a condition of accessing a data provider's developer interface, and that a data provider may not require a third party to sign any contract, either with the data provider or with a developer interface service provider, as a condition of access. The proposed rule does not

[95] The CFPB could also encourage Congress to leverage work already performed in this regard. Indeed, as recently as earlier this year in February 2023, Representative Patrick McHenry introduced a bill (H.R. 1165) proposing to amend GLBA via the creation of the Data Privacy Act of 2023.

[96] *See, e.g.*, Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P), 12 CFR Part 1016, proposed Jul 10, 2016, www.regulations.gov/docket/CFPB-2016-0032.

[97] Consumer Financial Protection Circular, *Insufficient data protection or security for sensitive consumer information*, Aug. 11, 2022, available at www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/.

identify a data access agreement as a requirement for access, but absent an affirmative statement that they are not required, data providers could argue that they are required, resulting in inefficient and lengthy contractual negotiations, which would significantly delay the CFPB's proposed timeline for migrating access to developer interfaces, and obviate many of the benefits of consistency and predictability set forth in the NPRM.

While we urge the CFPB to explicitly state that data access agreements are not a condition of access, some parties may still wish to enter into them, for example to provide clarity on certain terms not directly addressed by the proposed rule. The final rule should state that any data access agreements must be between the data provider and the third party. Data providers have an obligation to create a developer interface, and third parties have the right to connect to that interface. Data providers may, of course, rely on service providers to create a developer interface, but any such developer interface remains the data providers' obligation to create and maintain – and third parties retain the right to connect to that interface directly, and not through a service provider.

B. The Bureau Should Include Mortgage And Student Loan Accounts In The Final Rule

The Bureau requested comment on data fields that could become less available as a result of the transition away from screen scraping. The most important fields relate to mortgage and student loan data. In the three months before filing this comment letter, Plaid facilitated 15 million data access requests for mortgage or student loan information. If these data fields are left out of data provider's developer interfaces and data providers generally move to block access via screen scraping, millions of consumer access requests would go unfulfilled. Prohibiting screen scraping blocks for these data fields or accounts may not be practicable, as technology to block screen scraping typically is all or nothing – everything is blocked or nothing is.

C. The Proposed Rule's Requirements for Developer Interfaces Will Reduce The Frequency Of Data Requests Per Connection

The NPRM requested data that could inform the Bureau's estimate of additional costs a data provider might incur related to receiving requests through a developer interface. Plaid has examined data on our requests to data providers with developer interfaces. The data shows that access requests overall grew in a smooth and predictable manner, consistent with increasing consumer demand for data access. The availability of an interface does not appear to spike access requests in any way for a data provider. Instead, the greater reliability of developer interfaces actually *reduced* the number of developer interface requests per connection, largely because fewer requests failed and Plaid was able to better coordinate requests with the data provider. (See Appendix 4.) These reductions in requests per connection significantly reduced the relative demand (and presumably the cost of meeting that demand) for access at a data provider from what demand would have been without the developer interface.

D. The CFPB Should Expand Data Access To Cover EBT Cards

The NPRM asks for comment on whether the most appropriate way to solve issues related to Electronic Benefit Transfer (EBT) data accessed directly by the consumer is through § 1033, and whether it should do so as part of this first rulemaking or through a subsequent rule. We strongly urge the CFPB to allow this vulnerable population to benefit from the rapidly advancing technology that exists to assist households in managing and improving their financial health, and from the strong, new consumer protections encompassed in the proposed rule. We see no reason for delay.

Delay would cause needless harm to over 41 million individuals who rely on public benefits like those administered through the Supplemental Nutrition Assistance Program. These lower-income individuals must manage limited resources, including time, and may be unbanked or underbanked. Data can be a powerful tool to help households facing such challenges to manage their day to day finances, and make decisions that ultimately improve their financial health.

EBT accounts are designed as debit accounts with access devices, including cards and online portals, but there are currently no requirements for EBT processors to provide electronic access to consumers' data, and no requirements for third parties to provide adequate protections to consumers' data. EBT accounts are pivotal for low-income households and play a similar role to Reg E-asset accounts in supporting frequent transactions. Data from these accounts should, therefore, be accessible in order to allow consumers to benefit from holistic displays of their financial state, and other innovations powered by customer-controlled access.

E. The Bureau Should Include Account Statement PDFs As An Additional Data Field

As the Bureau considers additional examples of data fields to include in the final rule to help minimize disputes and facilitate standardization and compliance, it should include "account statements" as an enumerated data type. Account statement PDFs are critical to powering a number of use cases in the open finance ecosystem. While some large institutions with developer interfaces already provide an endpoint for PDF statements, many still do not, and likely will not, absent regulation. Bank-branded PDF statements are typically required by lenders in the credit space for loan underwriting. Accordingly, ensuring they are included in the final rule will benefit consumers by supporting lending use cases powered by data access, and will make it easier for consumers to fulfill documentary requirements to obtain credit that may otherwise require them to print or manually upload statements.

F. The Bureau Should Clarify That Push-Based Developer Interfaces Provide The Freshest Data For Consumers And Reduce The Number Of Developer Interface Calls

The CFPB's proposed definition of "current data" is sufficiently clear, particularly with the addition of pending but not yet settled transactions.[98] The CFPB may also wish to include language clarifying that developer interfaces that "push" new data to a connected authorized third party, without the authorized third party having to request the data, complies with the obligation to provide current data. Such push-based developer interfaces are better for the consumer, as they ensure the freshest data, and are relatively easy to implement through common technologies like webhooks. And because they only provide new data when consumers engage in new transactions, they generally reduce the number of API calls (and thus cost) on a data provider.

The CFPB's safe harbor of 24 months for historic transactional data is appropriate and should be maintained in the final rule. Many use cases require up to 24 months of data, so in the absence of a qualified industry standard this safe harbor reinforces current market practices.

X. Conclusion

Plaid again thanks the Bureau and its dedicated staff for the thought and care that went into this proposal to better secure consumers' access to their financial data and ability to use that data to increase choice and competition in financial services. With the following adjustments, the CFPB can issue a final rule that gives the United States the best open banking regulation in the world.

- The proposed implementation timeframes should be adjusted to avoid putting existing consumer account connections and consumers' statutory portability right at risk, and the Bureau should monitor the market throughout the implementation period to ensure that no covered entity reduces or eliminates currently-available data access or fails to satisfy the full scope of data access mandated by the rule.

- The proposed standards for authentication and authorization should be refined to eliminate unproductive friction and enhance consumer choice and to push the industry to improve its authentication and authorization methods so that consumers can have an increasingly successful, safe, and secure open finance experience.

- The proposed data privacy protections should be revised to avoid undermining consumer choice and comprehension, interfering with anti-fraud efforts and innovative product development, and further entrenching incumbents. The Bureau should acknowledge common and beneficial activities as reasonably necessary, recognize that there are secondary purposes for the collection and use of data that benefit consumers and the

[98] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796, 74872 , (proposed Oct. 31, 2023).

open finance ecosystem, and permit secondary collection and use of data so long as there are notice and opt-out or opt-in safeguards in place to ensure consumer understanding and control.

- The proposed approach to interface access should be clarified to avoid burden, inefficiency, inconsistency, and consumer frustration, and the Bureau should itself certify third parties for access or, if it declines to create a certification standard, should clarify that a third party's attestation that it maintains adequate security to safeguard consumer data is sufficient to gain interface access, and that the burden is on a data provider to deny such a request in certain limited circumstances.

- The proposal should clarify the Bureau's interest in enforcement of § 1033, that failure to meet the obligations under the rule is a violation of law, and that the Bureau will consider the complaints of industry participants when setting supervision and enforcement priorities.

Best regards,

John Pitts
Head of Policy
Plaid

Data Appendix

1. **Attachment 1**- Complete list of data elements in Financial Data Exchange Version 6.0
2. **Attachment 2**- 2023 Fintech Effect Consumer Survey
3. **Attachment 3**- Access request volume using data access platform token vs. third party token
4. **Attachment 4**- Developer interfaces do not increase access requests and reduce access requests per connection