



February 19, 2020

Kathy Kraninger  
Director  
Consumer Financial Protection Bureau  
1700 G Street  
Washington, DC 20552

Dear Director Kraninger:

Thank you for inviting Plaid to participate in the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records. Consumers' ability to easily access and share their financial account information allows them to choose financial products and services that fit their personal financial needs and take more control over their financial lives. The financial applications and services built on consumer-permissioned data are creating greater competition in financial markets, reducing rates and fees, improving the quality of financial products and services available to consumers, and expanding access to underserved consumers. These advances are contingent on the rights granted to consumers under Section 1033 of the Consumer Financial Protection Act of 2010 (CFPA). The Bureau's 2017 Principles for Consumer-Authorized Financial Data Sharing and Aggregation were critical in promoting a more stable foundation for the use of consumer-permissioned data, but as the market has evolved, so has the need for additional guidance. We hope the Bureau will use its Symposium to build on that work.

The importance of the Bureau's leadership on these issues is underscored by the continued rapid adoption of data-driven financial services by consumers, and the rise in innovative financial products and services being built to benefit those consumers.

- Roughly 1 in 3 US adults use a fintech product, such as Acorns or Venmo, and more than 2,500 consumer financial applications are powered by Plaid.
- Consumers rely on multiple third-party financial applications to meet their specific financial needs--many consumers who use Plaid to access and share their data are returning consumers connecting multiple applications.
- Consumers are using these connections to meet their core financial needs, with more than 100 million US consumers using digital financial services, including bank-offered services, to help them with things like payroll direct deposit, bill payment, investing, and savings.

As consumer use has grown, a number of stakeholders other than the Bureau have launched initiatives that could impact consumers' rights to their financial account data. These initiatives include:

- Aggregators have signed data access agreements with some of the largest banks that transition from credentials-based data access to API-based access, but also address issues like liability and consumer control.<sup>1</sup>
- Financial institutions have announced plans to block data access for any company that will not sign a data access agreement.<sup>2</sup>
- A group of banks, aggregators, and third-party providers established the Financial Data Exchange (FDX) to unify the financial industry around a common, interoperable, royalty-free API standard for consumers and businesses to conveniently and securely access their financial data.<sup>3</sup>
- The Clearing House published a model contract that would, among other things, give each bank the power to decide which apps its customers should have access to.<sup>4</sup>
- Plaid launched Plaid Direct, which allows any financial institution, including community banks and credit unions, as well as neobanks and fintechs to use APIs for more secure, convenient data transmission.<sup>5</sup>
- The United Kingdom implemented a comprehensive Open Banking regulatory structure, and began a consultation on expanding that mandate to Open Finance.<sup>6</sup>
- The European Union implemented the revised Payment Services Directive (PSD2), which provides consumers with the right to access and share data from their payment accounts.<sup>7</sup>
- The Canadian government completed a consultation on Open Banking with a recommendation to work on their own regulatory scheme to allow consumer directed financial data sharing.<sup>8</sup>

---

<sup>1</sup> <https://blog.plaid.com/chase/> and

<https://newsroom.wf.com/press-release/innovation-and-technology/wells-fargo-and-plaid-sign-data-exchange-agreement>

<sup>2</sup>

<https://www.americanbanker.com/news/jpmorgan-chase-moves-to-block-fintechs-from-screen-scraping>

<sup>3</sup> <https://financialdataexchange.org/pages/faq>

<sup>4</sup>

<https://www.theclearinghouse.org/payment-systems/articles/2019/11/~/-/media/d9894baa77894ca6b81b19b31d7bf3b7.ashx>

<sup>5</sup> <https://blog.plaid.com/plaid-direct/>

<sup>6</sup> <https://www.fca.org.uk/publications/calls-input/call-input-open-finance>

<sup>7</sup> [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_19\\_5555](https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_5555)

<sup>8</sup>

<https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html>

In light of the law and these developments, Plaid believes that the Bureau can pursue two complementary approaches to maintain its leadership and advocacy for consumers. First, the Bureau should update its 2017 Principles to reflect and inform the current state of consumer data access. Second, the Bureau should propose, and promptly work to adopt, an initial rule to implement consumers' rights under Section 1033 of the CFPA.

## **Updated Principles for Consumer Data Access**

The Bureau's data access principles were an innovative way for the Bureau to engage on an emerging issue under its jurisdiction. The 2017 Principles allowed the Bureau to signal the consumer protection issues it was prioritizing without engaging in premature or unnecessary regulatory intervention. It also created the opportunity for the Bureau to take a flexible, iterative approach, updating the principles at a pace that is responsive to rapid market developments and consumer interests. Plaid believes that this Symposium is an opportunity for the Bureau to consolidate feedback on the 2017 Principles, incorporate key market developments, and update the principles to reflect current consumer protection considerations.

The Bureau should update its principles on the consumer-authorized use of financial data to clarify that:

- Consumers are able to obtain the information from their financial service provider that they would otherwise be able to obtain through their online account with that provider.
- Financial account agreements and terms and conditions between financial institutions and consumers support safe, consumer-authorized access, and enable that access without undue friction or delay
- Authorized third-parties only access the data consistent with the consumer's authorization.
- Consumers are able to share and revoke access to their own account information for purposes of cash-flow underwriting or other eligibility determinations.

Plaid has provided suggested language, with explanations, that could be used to update these principles in Appendix 1. Plaid would be happy to engage on this topic further.

## **Section 1033 Rulemaking**

Updating the Principles is an appropriately dynamic response to a still-evolving ecosystem. However, there are several questions core to consumer data access that require a clear answer, so that consumers can have consistent expectations for how they can access and use their financial data even as the financial services continues to evolve. Plaid believes these questions are best resolved through a rule establishing a framework for a consumer's rights under Section 1033. A rulemaking need not be broad or complicated; rather, the rule should focus on defining the key consumer rights. Those issues include whether "covered persons" currently have an obligation to allow consumers to access their account information, whether the consumer can

access that information with the help of an intermediary, and what constitutes “account information” for the purposes of Section 1033.

Confirming that Section 1033 is in effect, and creates a consumer right that financial institutions must satisfy, should not be controversial. The Financial Data Exchange, representing almost 100 financial institutions, aggregators, and companies that use financial information, has among its core principles that consumers “should have access to their data” and “be able to permission their financial data for services or applications” of their choice.<sup>9</sup> But voluntary commitments, no matter how firm, do not have the strength and predictability of law. The Bureau should affirm that Section 1033 will continue to give consumers control over their financial data, so that consumers continue to benefit from these innovations.

A Section 1033 rulemaking should also address the U.S. Department of Treasury’s recommendation “that the Bureau affirm that for purposes of Section 1033, third parties properly authorized by consumers, including data aggregators and consumer fintech application providers, fall within the definition of ‘consumer’ under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.”<sup>10</sup> Consumers already rely on intermediaries to assist them with data access, with Plaid having helped connect more than 25% of US bank account holders with at least one application. And intermediaries like Plaid are developing additional tools, like consent management dashboards and one-click data deletion, to give consumers even more control over their data. Consumers’ choice to use intermediaries to help them manage their financial information should be protected.

The Bureau may wish to consider what practices intermediaries should implement as part of their relationship with the consumer. Plaid has identified three practices that we believe are essential to the intermediary role:

1. Intermediaries should not, directly or indirectly, sell to any nonaffiliated third party any of the consumer’s financial account information.
2. Intermediaries should implement physical, technological, and other relevant safeguards designed to ensure the accurate collection and transmission of the consumer’s financial account information. The protection would be designed to promote confidence among consumers that, by engaging one or more intermediaries, the consumer would be in a position to obtain an accurate profile for the consumer’s own financial wellbeing.
3. Intermediaries should offer appropriate disclosures and tools like online dashboards, so that consumers have transparency and control over consumers’ financial account information. The consumer should make the pivotal decisions regarding the types of data

---

<sup>9</sup> <https://financialdataexchange.org/pages/white-paper>

<sup>10</sup>

[https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation\\_0.pdf](https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf)

to access, the specific persons to whom the data is to be transmitted, and the scope or time limits for fulfilling the consumer's request.

Finally, consistent with the consumer's reasonable expectations, the Bureau should define the minimum scope of the financial account information to which a consumer should have access. The scope of account information covered by Section 1033 should be based on concepts that are intuitively clear to an ordinary consumer. For example, account information should, at a minimum, including all the information that the covered person makes available to the consumer through its online financial account, including any information used to facilitate the use of the account by the consumer (e.g., account and routing number).

I would like to thank you again for the opportunity to share Plaid's perspective on consumer-permissioned data. I look forward to a productive discussion of these issues at the Symposium.

Regards,



John Pitts  
Head of Policy  
Plaid

## Appendix 1

### Updated Principles for Consumer-Authorized Financial Data Sharing and Aggregation

#### Access

Consumers are able, upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider. Such information is made available in a timely manner. Consumers are generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.

Financial account agreements and terms support safe, consumer-authorized access, promote consumer interests, and do not seek to deter consumers from accessing or granting access to their account information. Access does not require consumers to share their account credentials with third parties.

#### *Explanation:*

We suggest a number of edits to the “Access” Principle to clarify that product and service providers must provide consumers and authorized third parties access to *all* available account information requested, and may not withhold information without a compelling, request-specific reason for doing so.

In our experience, using terms such as “trusted third parties” and “in a safe manner,” without further guidance as to what those terms mean, has led to a lack of clarity and uniformity in the industry. In particular, there is little consensus around what constitutes a “safe manner” of accessing consumer information, or under what circumstances a third party is sufficiently “trusted” such that the account provider should permit access. These terms also give excessive discretion to account providers to deny access for commercial or other reasons, even where there is not an identifiable risk of fraud related to the consumer’s or authorized third party’s access request.

Our proposed edits aim to resolve the ambiguity introduced by these terms and clarify that account providers should not withhold access from consumers or consumer-authorized third parties unless there is a material risk of fraud related to the particular information request. The “material risk” standard will ensure that account providers do not withhold or restrict consumer access to information without an evidentiary basis for doing so, and that they make these determinations on a case-by-case basis. Our edits further clarify that, short of a demonstrable risk, account providers should grant access to all available information responsive to the

consumer's request, and should not limit access merely because the consumer has directed a third party to act on the consumer's behalf.

#### Data Scope and Usability

Financial data subject to consumer and consumer-authorized access may include any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards. Information is made available in forms that are readily usable by consumers and consumer-authorized third parties. Third parties with authorized access only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary.

#### *Explanation:*

The Bureau should update the "Data Scope and Usability" Principle to ensure that consumers are neither limited in the scope of data they may access, nor in their use of data once accessed.

The original iteration of this Principle begins with a list of the types of financial data that may be subject to consumer access, but the Bureau should clarify that *all* information an account provider maintains about a consumer is subject to access. Without this clarification, account providers may take the view that only the enumerated categories of information are within scope, and that consumers may be denied access to any information that falls outside this scope. In addition, it has been our experience that some account providers limit the scope of information available for access when an authorized third party makes the request for access on the consumer's behalf. Our proposed edits clarify that the scope of available information should remain consistent regardless of whether the consumer personally requests access or directs a third party to act on the consumer's behalf.

We have also proposed edits to resolve ambiguity around how consumers and authorized third parties may use account information once accessed. The Principle, as originally drafted, permits third parties to use accessed information only to the extent necessary to provide the products and services the consumer has selected. Yet many consumers—for good reason—may want to permission their data to be used for the development of new and innovative products and services, separate from the products and services they currently use. Our proposed edits to this Principle resolve the ambiguity around how authorized third parties may use and store consumer-permissioned data, and clarify that the consumer should have ultimate control over data usability. The proposed edits further clarify that account providers should not restrict consumers' and authorized third parties' use and disclosure of data when such use and disclosure is directed by the consumer. This clarification will guard against situations where account providers override a consumer's choice of third-party products or services, or otherwise restrict the third-party products and services consumers can use because the account providers

either disapprove of those products and services in some way, or view them as a competitive commercial threat.

### Control and Informed Consent

Consumers can enhance their financial lives when they control information regarding their accounts or use of financial services. Authorized terms of access, storage, use, and disposal are fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer. Terms of data access include access frequency, data scope, and retention period. Consumers are not coerced into granting third-party access. Consumers understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data. Revocations are implemented by providers in a timely and effective manner, and at the discretion of the consumer, provide for third parties to delete personally identifiable information.

#### *Explanation:*

The Bureau should modify the principles of consumer control and informed consent to reflect a consumer's right to dictate the terms of access, storage, use, and sharing of his/her information, which can be as broad or as narrow as desired by a consumer. In practice this means that a consumer can authorize broad, recurring access to his/her information for multiple purposes, or can authorize narrow, restricted access to his/her information for a specific purpose.

We have also suggested edits that are less prescriptive about the type of information that must be provided to the consumer about the terms of access, and have instead suggested changes that convey that the information provided should be "sufficiently detailed" and "timely delivered" so that consumers can make meaningful and informed decisions about the treatment of their information.

### New Principle: Enabling Responsible Access to Credit and Financial Services

Consumers are able to share, or authorize a third party to share, their own information for purposes of cash-flow underwriting or other eligibility determinations. In such cases, the third party facilitating the information sharing acts as an agent on behalf of the consumer to further the consumer's initiated transaction. If consumers are able to decide whether to share their information and with which parties, select the financial institutions from which their information will be sourced, review the type(s) and scope of information to be shared, and later revoke consent to continued access such information, then the information shared through the third party will not be considered a credit report under applicable law. All parties that share such information, at the consumer's request, for underwriting or decisioning must take reasonable steps to ensure the integrity of the information, only enable the onward transfer of

such information in accordance with the consumer’s permission and reasonable expectations, and provide the consumer with disclosures, written in plain language, about how the consumer’s information will be accessed, used, shared, and stored.

*Explanation:*

The Bureau should add a new principle, “Enabling Responsible Access to Credit and Financial Services”, to promote the responsible use of consumer-permissioned information for cash-flow underwriting and other eligibility determinations, and should clarify that such use is distinct from the existing consumer reporting system. In contrast to the traditional consumer reporting system, when a consumer permissions his/her data for underwriting or a specific eligibility determination, the consumer controls the key flows that affect the treatment of their own information. More specifically, when connecting his or her financial accounts to a lender’s application or service, the consumer, and not a consumer reporting agency, selects the financial institutions from which their information will be sourced, and controls with whom their information is shared. In this way, the use of consumer-permissioned data for cash-flow underwriting and other decisioning is distinct from the traditional consumer reporting system, and can operate alongside the traditional consumer reporting system that is regulated by the Fair Credit Reporting Act.

Consumer-permissioned data can also enable the 45 million consumers in the United States who are “credit invisibles,” meaning those who lack sufficient information in their consumer reports to obtain access to credit, to overcome existing barriers to the financial marketplace. By empowering consumers to permission their data for cash-flow underwriting and other eligibility determinations, credit-invisible consumers can obtain access to better credit and insurance products, as well as housing and employment opportunities, where they otherwise may have been denied or offered less favorable terms.

In enabling access and use of consumer-permissioned data for underwriting and other decisioning, the Bureau should establish reasonable requirements related to the treatment of such information, including requirements that parties provide transparency about the information to be shared, as well as control over how and with whom such information is shared. Likewise, the Bureau should require such parties to undertake reasonable steps to ensure the integrity of such information, and require clear and concise disclosures to consumers about the treatment of their information.