PLAID

October 21, 2025

Mr. Russell Vought
Acting Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

SENT VIA ELECTRONIC MAIL TO:
2025-ANPR-PersonalFinancialDataRights@cfpb.gov

Re: Personal Financial Data Rights Reconsideration, Docket No. CFPB–2025–0037

Dear Acting Director Vought and Bureau Staff,

Plaid appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (the "CFPB's" or "Bureau's") Advance Notice of Proposed Rulemaking ("ANPR") related to its Reconsideration of the Personal Financial Data Rights Rule (the "PFDR Rule").

With our mission to unlock financial freedom for everyone, Plaid helps people to take control of their financial lives and to access competitive and innovative financial services. Our technology allows individuals to securely access and share their financial data from over 12,000 financial institutions (also referred to as "data providers" or "covered persons") with over 7,000 of their chosen digital financial services providers (also referred to as "authorized third parties" or "authorized third-party representatives"). These providers, which include fintech apps and banks alike, rely on secure, permissioned access to consumers' financial data in order to deliver the services that consumers have requested from them. For example, a personal financial management app needs access to a consumer's transaction history to provide individualized budgeting services, and a lender needs access to a consumer's current loan rate and income in order to provide a competitive offer.

Consumers' ability to access and share their financial data—a right codified in Section 1033 of the Consumer Financial Protection Act ("CFPA")—is foundational to their freedom to choose the digital financial services that best meet their needs, whether those be investing in crypto, making peer-to-peer payments, obtaining credit, or even finding a new bank. When consumers can easily do so, competition and innovation thrive. Indeed, Plaid's technology, and the data access we support, will become even more critical as America's leadership in AI opens up additional financial opportunities and services for individuals and the market. But, without a strong Section 1033 data access right, backed by an equally strong PFDR Rule, individual consumers are at risk of being de-banked and denied access to the services they want. And the same incumbent banks that have time-and-again sought to quash the competitive and innovative third parties that threaten their bottom lines will exploit any limitation on consumers' data access right to gain even more market share and control over the financial lives of American consumers.

To that end, the CFPB should ensure that the PFDR Rule continues to protect the broad right of American consumers to access and share their own financial data, giving them choice and control over their financial lives and unlocking continued competition and innovation in the digital financial services marketplace.

Section 1033 puts financial choice back into the hands of Americans.

Section 1033 gives the American people a fundamental right to access and share their financial information, including with their chosen third-party representatives (be they fintech apps, crypto platforms, or even other banks). As Americans go about their daily lives, they generate financial data about themselves, ranging from information about their purchases and their income, to their debts and loan rates and more. That information is typically held by the financial institution with which a consumer banks, but is *always* owned by the individual consumer. When a financial institution refuses to make a consumer's own information available to them or their chosen authorized third parties, then the consumer is robbed of control of their data and effectively thwarted from obtaining competitive, innovative, and critical financial services.

Take, for example, a crypto investor: in order to invest, their first step is to fund their crypto wallet by connecting their financial institution account to their chosen crypto exchange. To do that, the individual needs to be able to digitally access and share some of their financial information, like their account and routing number, from their financial institution with their exchange. If the financial institution blocks access to this information, the individual will not be able to fund their wallet to invest in crypto.[1] The same is true of an individual trying to switch banks. This person may want to switch for a variety of reasons—perhaps they have been denied access to financial services on the basis of political or religious beliefs or lawful business activities that the incumbent bank deemed reputationally risky,[2] or perhaps they were denied credit or are simply looking for more competitive loan terms, higher interest rates, or better customer service. Whatever the reason, without the ability to access and share their information—like name and address, account balance, recurring payments, transaction history, loan rates, and so on—with their chosen authorized third party, the consumer's financial history is effectively locked up at their financial institution, cutting off their ability to easily comparison shop, switch providers, or select new or better services that meet their needs.

---

[1] *See* Rashan A. Colbert (@Rashan), X (Oct. 7, 2025, at 11:58 AM ET), https://x.com/rashan/status/1975591681735954763 ("Accessing crypto usually starts with a fiat on-ramp—connecting a traditional bank account to a crypto exchange like Coinbase or Kraken. Without seamless, low-friction access to their own financial data, users are stuck. They can't bridge into the blockchain world. They can't experience the very innovation crypto promises."); *cf.* Strengthening American Leadership in Digital Financial Technology, Exec. Order No. 14,178, § 1(iii), 90 Fed. Reg. 8647 (Jan. 23, 2025) ("The digital asset industry plays a crucial role in innovation and economic development in the United States, as well as our Nation's international leadership. It is therefore the policy of my Administration to support the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy, including by . . . protecting and promoting fair and open access to banking services for all law-abiding individual citizens and private-sector entities alike.").

[2] *See* Guaranteeing Fair Banking for All Americans, Exec. Order No. 14,331, § 1, 90 Fed. Reg. 38,925, 38,925 (Aug. 7, 2025).

Section 1033 puts control and choice back in the hands of the American people. Whether an individual banks with a Top 10 Wall Street firm, a mid-sized credit union, a neobank, or other financial services provider, Section 1033 makes clear that their financial institution has a legal obligation to make certain financial information available to the individual and the individual's authorized third-party representatives whenever they request it.

A strong Section 1033 right protects and promotes competition and innovation.

As the CFPB observed in the ANPR it issued during President Trump's First Administration:

> In recent years, the number and usage of products and services that utilize or rely upon consumers' ability to authorize third-party access to consumer data have grown substantially and rapidly. This growth in authorized data access has been accompanied by expansion in the number of distinct applications or "use cases" for authorized data, including, but not limited to, personal financial management; financial advisory services; assistance in shopping for and selecting new consumer financial products and services; making and receiving payments; assisting consumers with improving savings outcomes; identity verification and account ownership validation; credit profile improvement; and underwriting. ***This type of consumer-authorized data access and use holds the promise of improved and innovative consumer financial products and services, enhanced control for consumers over their financial lives, and increased competition in the provision of financial services to consumers.***[3]

Consumer-authorized data access has delivered on this promise, with the stability and protection provided by Section 1033 playing a large role in its success. Indeed, thanks to new entrants and challengers to the dominant financial institutions' incumbency, the financial services market has become one where crypto and digital-asset investments are accessible to all Americans, where consumers are no longer reliant on outdated payment forms (like checks) to move money quickly,[4] where cashflow underwriting has made credit more accessible to underserved individuals, and where AI-driven solutions are helping Americans to lead better financial lives. These innovations and services, and the many others that sit alongside them, would not have developed without the statutorily protected right of individuals to access and share data with their authorized third-party representatives.

Incumbent financial institutions are deploying campaigns of fearmongering and pretextual concerns to undermine competition and innovation.

As the First Trump Administration observed, "[t]hese competitive dynamics mean that data holders [financial institutions] may have an incentive to restrict access by certain data users

[3] Consumer Access to Financial Records, 85 Fed. Reg. 71,003, 71,005 (Nov. 6, 2020) (advance notice of proposed rulemaking) (emphasis added) (citations omitted) (hereinafter "Nov. 2020 ANPR").

[4] *See* Modernizing Payments to and From America's Bank Account, Exec. Order No. 14,247, 90 Fed. Reg. 14,001 (Mar. 25, 2025) (announcing that the federal government will phase out paper checks for most federal payments by September 30, 2025).

[authorized third parties]."[5] Indeed, in the face of the competition and innovation that consumer-authorized data sharing has engendered, dominant financial institutions have attempted to choke off consumers' Section 1033 access right. Interference with this right has been both overt—with large banks shutting off or degrading data access[6]—and insidious—with banks claiming pretextual security and safety concerns as a reason for denying access.[7] Recently, a trade group representing the nation's largest financial institutions went so far as to sue the CFPB to vacate the PFDR Rule, directly attacking the access right at the heart of Section 1033.[8] Claiming that Section 1033 is, at most, a narrow right that allows only an individual—not their authorized third parties—to access their financial data, the bank trade sought to render Section 1033 a nullity. That litigation was put on hold—over the bank trade's objection—pending the CFPB's current rulemaking process.[9]

With their litigation efforts currently paused, these dominant financial institutions and their trades remain actively engaged in tactics to thwart data access. For example, seeking to take advantage of perceived regulatory uncertainty, some institutions have threatened to effectively "paywall" consumers' own data by refusing authorized third-party access unless anticompetitive fees are paid.[10] Others have weaponized false partisan rhetoric—inaccurately framing Section 1033 as a Biden-era priority to mislead consumers into advocating against their own interests.[11]

---

[5] Nov. 2020 ANPR, 85 Fed. Reg. at 71,006.

[6] *See* Daniel Huang & Peter Rudegeair, *Bank of America Cut Off Finance Sites from Its Data*, Wall St. J. (updated Nov. 9, 2015, at 7:47 PM ET), https://www.wsj.com/articles/bank-of-america-cut-off-finance-sites-from-its-data-1447115089; Peter Rudegeair, *J.P. Morgan Warns It Could Unplug Quicken and Quickbooks Users*, Wall St. J. (Nov. 24, 2015, at 9:39 AM ET), https://www.wsj.com/articles/j-p-morgan-may-unplug-some-customers-access-to-account-data-1448375950; Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, Wall St. J. (Nov. 4, 2015, at 7:30 PM ET), https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450.

[7] It is well-recognized that "dominant market participants use privacy and security as a justification to disallow interoperability and foreclose competition." Off. of Tech. & Bureau of Competition, FTC, *Interoperability, Privacy, & Security*, Fed. Trade Comm'n (Dec. 21, 2023), www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/12/interoperability-privacy-security.

[8] *See* Complaint, *Forcht Bank, N.A. v. CFPB*, No. 5:24-cv-304 (E.D. Ky. Oct. 22, 2024), ECF No. 1.

[9] Order at 2, *Forcht Bank* (July 29, 2025), ECF No. 83 (staying case); *see* Motion to Stay Proceedings at 3, *Forcht Bank* (July 29, 2025), ECF No. 80 (noting plaintiffs' opposition to stay).

[10] *See* Alex Rampell (@arampell), X (July 16, 2025, at 12:12 PM ET), https://x.com/arampell/status/1945516918489981027 ("[N]ow the banks are about to implement their own Chokepoint 3.0—charging insanely high fees to access data or move money to crypto and fintech apps, and more concerningly blocking crypto and fintech apps they don't like . . . ." (emphasis omitted)); Tyler Winklevoss (@tyler), X (July 19, 2025, at 8:28 PM ET), https://x.com/tyler/status/1946728768443150740 ("[T]he banksters are trying to kill fintech and crypto companies. They want to take away your right to access your banking data for FREE . . . .").

[11] *See Myth vs. Fact: What the Big Bank Lobby Gets Wrong About Open Banking and Security*, Fin. Data & Tech. Ass'n (Aug. 13, 2025), https://fdata.global/blog/2025/08/13/myth-vs-fact-what-the-big-bank-lobby-gets-wrong-about-open-banking-and-security.

And others have mischaracterized authorized third parties, including companies like Plaid, as untrustworthy middlemen, in an attempt to discredit the very entities helping Americans to better manage their financial lives.[12]

The incumbent financial institutions' goal is clear: eliminate the statutory protection for consumer-authorized data sharing. Dismantling the core provisions of the PFDR Rule will hand these financial institutions even greater power to de-bank at will by putting them—not American consumers—in control of access to the competitive digital financial services provided by authorized third parties. The First Trump Administration initiated the PFDR rulemaking process to empower Americans and protect competition and innovation; it made clear that "narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[13] That is exactly right.

The Bureau has an opportunity to reinforce consumer choice and control, while strengthening American leadership in the digital financial services market.

The CFPB has an opportunity to finish what the First Trump Administration started, and we applaud its decision to invite feedback on certain key portions of the PFDR Rule.

Plaid respectfully submits the following recommendations:

1. **The Bureau should confirm that any third-party representative properly authorized by the individual consumer is entitled to access data under Section 1033**: The definition of "consumer," as used in Section 1033, means an individual, agent, trustee, or *representative acting on behalf of the individual*.[14] Up to this point, "representative" has widely been interpreted to include digital financial services providers acting on an individual's behalf to access their data. Indeed, the Trump Administration expressed agreement with this reading in its 2018 Treasury Report.[15] Unsurprisingly, though, in a bid to eliminate competition from these digital financial services providers, certain incumbent financial institutions and their trades have advocated for a narrow interpretation of "representative"—one that would require a fiduciary relationship between the individual and their representative, even though the incumbents themselves rarely have such a relationship. Not only is this narrow interpretation incorrect and contrary to statutory text and historical context, it is also blatantly anti-consumer and anticompetitive. The consequence of such a narrow interpretation is to exclude the vast majority of digital financial services providers—which do not have and cannot shift to a "fiduciary" business model—from Section 1033's coverage. If dominant financial institutions have no statutory obligation to make data available to these providers, those institutions, not consumers, are effectively placed at the helm of who gets access,

[12] *See id.*

[13] U.S. Dep't of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* 31 (July 2018), https://home.treasury.gov/system/files/136/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf (hereinafter "2018 Treasury Report").

[14] 12 U.S.C. § 5481(4).

[15] 2018 Treasury Report, *supra* note 13, at 31.

putting them in a position to hinder consumers' ability to use their chosen providers and to suppress competition and innovation.

2. **The Bureau should confirm that fees are prohibited under Section 1033**: Section 1033 makes clear that individuals and their authorized third-party representatives are entitled to receive information "upon request"—not "upon the payment of a fee." The statute is not written conditionally, nor does it contain any allowance from Congress for fees. The CFPB therefore does not have the jurisdictional authority to permit fees, let alone to set prices. The Bureau should view the recent push for fees by dominant financial institutions with skepticism. With Section 1033's protection, the market has successfully developed over more than a decade without fees for data access. Dominant financial institutions are pressing for fees now, not because of some new-found need to recover "costs" on the very API technologies they insisted the market adopt, but rather because fees are yet another competition-killing weapon in their arsenal. Banks already recoup infrastructure-related costs through account fees, interest, and service charges, and dominant institutions have been operating their proprietary APIs without fees for years. Allowing fees would contradict Congressional intent, lead to double-charging, and hand incumbent financial institutions an anticompetitive lever to throttle access, putting individuals, authorized third parties, and smaller community banks and credit unions at a distinct disadvantage.

3. **The Bureau should confirm GLBA Safeguards as a proper means to protect individuals' financial information and should more strongly incentivize the elimination of screen scraping**: The Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule and equivalent FTC standards provide an appropriate security framework for the PFDR Rule because they ensure a consistent approach to data security across data providers and authorized third parties. The Bureau should confirm this approach and avoid creating a patchwork of inconsistent requirements in response to pretextual "concerns" around security raised by certain Wall Street banks. At the same time, the Bureau should also recognize that the Rule does not go far enough to eliminate screen scraping and should incentivize financial institutions to build and expand their APIs (also referred to as "developer interfaces") by making clear that, when those interfaces are otherwise compliant with the PFDR Rule's access and performance requirements and make available data elements covered by Section 1033 (including those not explicitly covered by the Rule), then screen scraping for those data elements is prohibited.

4. **The Bureau should focus the privacy provisions within the PFDR Rule on authorization, certification, and revocation, while eliminating other anti-innovation provisions that overstepped the Bureau's legal authority**: Section 1033 is a statute about *access*: it codifies an individual's right, including through representatives acting on their behalf, to access their financial information. The PFDR Rule's general authorization, certification, and revocation requirements ensure that third-party representatives accessing data are doing so on the individual's behalf, and these requirements should thus be retained. But, beyond these access controls, the PFDR Rule went too far, effectively attempting to enact a broad privacy regime that would make a European bureaucrat blush—one that could be interpreted to prohibit the use of data for beneficial purposes, *regardless of a consumer's authorization*. In so doing, the CFPB not only substituted its own political and moral

judgments for those of individual consumers, but it also went beyond the bounds of Section 1033 and undermined the very competition and innovation it should have been championing. Plaid is an avid proponent of consumer control, transparency, privacy, and security, and firmly believes that innovation and competition can and should go hand-in-hand with those protections. We believe that the PFDR Rule's authorization, certification, and revocation requirements are a step in the right direction and, with respect to any need for broader privacy protections, support the passage of a federal privacy law that will impose uniform standards on the market.

Plaid provides responses to the specific sections and questions included in the ANPR below.

* * * * *

Scope of Who May Make a Request on Behalf of a Consumer

Construing the terms "consumer" and "representative" narrowly would effectively deprive individuals of their right to use the digital financial services of their choosing and upend longstanding market protections and the competition and innovation they have enabled. That is exactly why dominant financial institutions have advocated for a prohibitively narrow interpretation of those terms.

Large financial institutions have argued that (1) the term "consumer," as used in Section 1033, means only an individual, or (2) in the alternative, if "consumer" is given the definition ascribed to it in the CFPA ("individual or an agent, trustee, or representative acting on behalf of an individual"[16]), that definition necessarily requires a representative to have a fiduciary relationship with the individual. Both of these arguments run counter to Congress' clear intent: under either argument, digital financial services providers—which act as authorized third-party representatives of an individual—would have no statutory protection under Section 1033 to access data at the individual consumer's direction. The majority of digital financial services providers—such as peer-to-peer payment companies, crypto exchanges, or budgeting applications—do not have, do not need to have, and could not shift their business models to create a fiduciary relationship with the individual. If the Bureau adopts either argument, an individual's ability to share financial data with their chosen digital financial services providers will become entirely dependent on whether incumbent financial institutions allow it, as opposed to whether the individual requests it. This will put banks in control of whether individuals can access competitive or innovative services—and, to the extent they allow it, at what cost. Competition, innovation, and consumer choice will all suffer.

The ANPR's questions focus primarily on the second argument—whether a representative acting on behalf of an individual must be a fiduciary of that individual. In addition to the practical implications of requiring a fiduciary relationship, the text of the CFPA and the purposes for which it was enacted make clear that individuals' authorized third-party representatives must be able to access those individuals' financial information upon request. Dominant financial institutions may argue that the imposition of a fiduciary duty is the only way to ensure that a representative is indeed acting on behalf of an individual. ***This is a red herring***. Those same

[16] 12 U.S.C. § 5481(4).

financial institutions act on behalf of their millions of customers day in and day out, yet in almost all cases do not have a fiduciary relationship with them.

Authorization, certification, and revocation mechanisms—all of which are included in the PFDR Rule—ensure that a third party is acting on an individual's behalf, while keeping that individual, not their financial institution, in control. This is the interpretation and approach that the market has successfully relied on up to this point. The benefits are readily apparent: fintech apps and other digital financial services providers have engendered greater competition, forcing dominant institutions to compete on merit, while individuals reap the benefits of innovation and more accessible financial services. The cost of reversing this interpretation would be tremendous dislocation for individual consumers and the providers they presently rely on for services.

The CFPB should disregard the Wall Street banks' anticompetitive attempts to shoehorn a broad statutory right into a forced, narrow definition and should instead confirm Congressional intent and the longstanding interpretation of "consumer" and "representative" that includes third parties authorized to act on an individual's behalf, regardless of fiduciary relationship.

> ***1. What is the plain meaning of the term "representative?" Does the PFDR Rule's interpretation of the phrase "representative acting on behalf of an individual" represent the best reading of the statutory language? Why or why not?***

Under Section 1033(a), data providers are required to make certain financial information available to a "consumer" upon their request.[17] "Consumer" is, in turn, defined as "an individual or an agent, trustee, or *representative acting on behalf of an individual*."[18] ***And that is exactly what a representative is: someone who acts on behalf of another.***

In the context of Section 1033, the term "representative" encompasses fintech, crypto, and aggregation companies—and increasingly banks themselves—acting on behalf of individuals to access their financial data. This interpretation reflects both the plain language and clear intent of the law by giving individuals control over their own financial data and eliminating bank gatekeeping—and has been widely accepted and adopted in the market. Indeed, at the time Congress passed the CFPA, aggregation and fintech companies already existed and were opening the markets for financial services.[19] The First Trump Administration's Treasury Department itself explained that the definition of "consumer" is "best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data

---

[17] *Id.* § 5533(a).

[18] *Id.* § 5481(4) (emphasis added).

[19] *See* Microsoft Corp. et al, Press Release, OFX Consortium Expands With Bank of America, Citigroup, Corillian, E*TRADE and TD Waterhouse (Oct. 2, 2001), https://news.microsoft.com/source/2001/10/02/ofx-consortium-expands-with-bank-of-america-citigroup-corillian-etrade-and-td-waterhouse (Microsoft, Intuit, and Nasdaq's CheckFree created Open Financial Exchange consortium in 1997, with participation from Bank of America and Citigroup); Maria Trombly, *Citibank's Aggregation Portal a Big Draw*, Computerworld (Sept. 18, 2000), https://www.computerworld.com/article/1371594/citibank-s-aggregation-portal-a-big-draw.html (Citi announced aggregation service in September 2000, followed by Wells Fargo and Chase).

aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies."[20] It recognized that any narrower reading "would *do little* to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[21] As of 2018, digital financial services providers were already delivering transformative innovations to millions of consumers—innovations made possible by Americans' statutorily protected ability to authorize those companies, as their representatives, to access their financial data. The same holds true today—but on an even greater scale: well over a hundred million individuals rely on the ability, under Section 1033, to authorize their chosen third-party representatives to access their data.[22] Any reversal of this interpretation would not only be contrary to the plain meaning and purpose of Section 1033, but would jeopardize the market competition the law has generated by placing control back in the hands of the very banks seeking to stifle it.

This interpretation—one that focuses simply on whether a representative is acting on behalf of an individual—is also supported by other established authorities that define the term. For example, *Black's Law Dictionary* defines a "representative" as "[o]ne who stands for or acts on behalf of another."[23] The *Oxford English Dictionary* defines "representative" as one "who stands for, speaks, or acts on behalf of another person or group of people."[24] When an individual authorizes a third party to access their financial information on their behalf, the third party acts as the individual's "representative" under the plain meaning of that term.

Arguing for an interpretation that finds no support in any dictionary, legal source, or case—let alone the actual text of Section 1033—some dominant banks have nevertheless attempted to impose a fiduciary requirement on the term "representative." This is nothing more than an ill-guised, anticompetitive attempt to strip digital financial services providers of the statutory protection that they and the market have enjoyed up to this point.

The PFDR Rule correctly applied the only defensible definition of "representative" rather than impermissibly rewriting the law to require a fiduciary relationship. The Rule's general approach, which employs authorization, certification, and revocation as the means to ensure a representative is acting on behalf of an individual, is the correct one. In particular, under the PFDR Rule, third parties are considered "representatives" if they "compl[y] with the authorization procedures" set out in the Rule.[25] Among other requirements, the PFDR Rule requires authorized third parties to provide "readily understandable" "authorization disclosures"; obtain the individual's "express informed consent" to access data; and permit consumers to

---

[20] 2018 Treasury Report, *supra* note 13, at 31.

[21] *Id.* (emphasis added); *see id.* (discussing banks' argument that the term "consumer" should be limited to an individual consumer).

[22] *See* Ellie Duncan, *FDX API Adoption Hits 114m Customer Connections*, Open Banking Expo (Apr. 28, 2025), https://www.openbankingexpo.com/news/fdx-api-adoption-hits-114m-customer-connections.

[23] *Representative*, *Black's Law Dictionary* 1416 (9th ed. 2009).

[24] *Representative*, Oxford English Dictionary (3d ed. rev. 2009) (entry noun.I.3.a), https://www.oed.com/dictionary/representative_adj?tab=meaning_and_use#151974496.

[25] 12 C.F.R. § 1033.131; *see id.* § 1033.401.

easily revoke third-party access.[26] These procedures ensure that third parties are indeed acting on behalf of those individuals when accessing their data.[27]

2. Are there other provisions in Federal statutes or financial services market practice in which third parties authorized to act on behalf of an individual encompass, on an equivalent basis, both those having fiduciary duties and those who do not?

Yes. Third-party representatives authorized to act on behalf of an individual routinely include non-fiduciaries.

In general, banks do not owe fiduciary duties to their ordinary account holders and the relationship instead is governed by contractual terms.[28] Furthermore, depository institutions frequently act on behalf of individual consumers in a payments context without having a fiduciary relationship. For example, when an individual authorizes a merchant to initiate recurring debits from their checking account (perhaps to pay their utility bills), under the Electronic Funds Transfer Act ("EFTA") and the CFPB's Regulation E, their bank will act pursuant to the payment instruction received from the payment network, without any fiduciary duty being imposed.[29] An individual may also instruct their bank to send funds to a third party or to another account. Although an individual *could* delegate these tasks to a fiduciary, the bank's ability to act at the individual's direction does not require the existence of a fiduciary relationship. Instead, it only requires that the consumer authorize the transfer,[30] or provide the bank with instructions per the contractual terms in place that govern the bank account, and that the bank adhere to applicable consumer-protection requirements.

Similarly, under Regulation Z, which implements the Truth in Lending Act, a primary credit cardholder can designate authorized users who can make purchases. These authorized users are not required to be fiduciaries of the primary cardholder. Instead, "[a] card issuer may issue a credit card to the person who requests it, and to anyone else for whom that person requests a card and who will be an authorized user on the requester's account."[31] An unauthorized use occurs

---

[26] *Id.* §§ 1033.401, 1033.411, 1033.421.

[27] *Cf.* Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838, 90,921 (Nov. 18, 2024) ("PFDR Rule").

[28] *See, e.g.*, *Legore v. OneWest Bank, FSB*, 898 F. Supp. 2d 912, 918 (D. Md. 2012) ("[T]he relationship between a bank and a borrower is contractual, not fiduciary, in nature."); *Ahrendt v. Granite Bank*, 740 A.2d 1058, 1061 (N.H. 1999) ("As a general rule, the relationship between a bank and a customer is not a fiduciary one . . . ."); *Bank Leumi Tr. Co. of N.Y. v. Block 3102 Corp.*, 580 N.Y.S.2d 299, 301 (App. Div. 1992) ("The legal relationship between a borrower and a bank is a contractual one of debtor and creditor and does not create a fiduciary relationship between the bank and its borrower or its guarantors.").

[29] *See* 12 C.F.R. § 1005.10.

[30] *See id.* § 1005.2(m) ("'Unauthorized electronic fund transfer' means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.").

[31] 12 C.F.R. pt. 1026, Supp. I, at 536 (2025) (comment 6 of official interpretation of 12 C.F.R. § 1026.12(a)(1)).

only when a third party lacks "actual, implied, or apparent authority for such use."[32]

Other statutory schemes and market practices work similarly. For instance, the GLBA and Regulation P expressly contemplate that financial institutions and their affiliates may share or receive consumer financial information based on the consumer's consent, again without requiring any fiduciary duty.[33] Regulation P also permits sharing with "persons acting in a fiduciary ***or*** representative capacity on behalf of the consumer," indicating that a representative may act on the consumer's behalf without any fiduciary duty.[34]

> ***3. Does the statutory reference to an "agent, trustee, or representative" indicate that "representative" is intended to encompass only those representatives that are serving in a fiduciary capacity? If a "representative" under 12 U.S.C. 5481(4) is interpreted to be an individual or entity with fiduciary duties, what are the distinctions between an "agent" and a "representative" for purposes of section 1033?***

No. The statutory reference does not require a representative to serve in a fiduciary capacity.

Reading a fiduciary obligation into the term "representative" would depart from the word's ordinary meaning and Section 1033's plain text and purpose. To act as a "representative" simply means to act on another's behalf; without more, it does not connote a fiduciary relationship.

Some of the dominant Wall Street banks have argued the terms "agent" and "trustee" imply a fiduciary relationship and, because those terms sit alongside the term "representative," that term too must imply a fiduciary duty. This argument is incorrect.

First, the premise is wrong: the word "agent" does not necessarily imply a fiduciary relationship. *Black's Law Dictionary* defines an "agent" as "[o]ne who is authorized to act for or in place of another; a representative," and makes no reference to a fiduciary relationship.[35] While some agency relationships are fiduciary in nature, legal and commercial usage shows that the term "agent" is also applied to authorized relationships that are non-fiduciary in nature.

Second, even if the term "agent" might sometimes involve a fiduciary relationship, it does not follow that a fiduciary relationship must be read into the word "representative." The common characteristic of the terms "agent," "trustee," and "representative" is that all three must act on behalf of the individual—not that all three are fiduciaries. This interpretation is grounded in the statutory text, which expressly requires that the third party act on behalf of the individual.[36]

---

[32] 12 C.F.R. § 1026.12(b)(1)(i).

[33] *See* 15 U.S.C. § 6802(e)(2).

[34] 12 C.F.R. § 1016.15(a)(2)(v) (emphasis added).

[35] *Agent*, *Black's Law Dictionary*, *supra* note 23, at 72.

[36] Some banks have argued that such an interpretation would render the terms "agent" and "trustee" superfluous since both would be encompassed within the term "representative acting on behalf of an individual." They have therefore argued that because, according to them, "agents" and "trustees" are fiduciaries, "representative" should be narrowed to include a fiduciary requirement. As the Supreme Court has recently made clear in a remarkably similar case, that is not a persuasive argument. Congress

Third, a reading requiring a fiduciary relationship would cause two statutory terms to have the same meaning. The CFPB asks, if a fiduciary duty is imposed, "what are the distinctions between an 'agent' and a 'representative' for purposes of Section 1033?" **The answer is *none*.** "Representative" must be given its own independent meaning, not one that is narrowly constrained to merely be co-extensive with the preceding terms.[37]

Finally, where Congress intends to refer to a fiduciary relationship, it knows how to do so. For example, a federal statute governing the Comptroller of the Currency's power to grant permits to national banks states that the Comptroller may grant "the right to act as trustee, executor, administrator, registrar of stocks and bonds, guardian of estates, assignee, receiver, *or in any other fiduciary capacity*."[38] This statute provides an exhaustive list of fiduciary relationships, yet Congress still saw fit to make explicit its intent to refer to fiduciary relationships. Given Congress's explicit approach to referencing fiduciary relationships in other statutes, it is clear that it did *not* intend to refer to such a relationship in the CFPA's definition of "consumer." Quite the opposite. As discussed in response to Question 8, in the Dodd-Frank Act (which contains CFPA Section 1033), Congress used the term "legal representative" to refer to relationships requiring something more than simply acting on behalf of the individual. Had Congress intended to impose a fiduciary obligation in defining "consumer" to include "representatives," it knew the language necessary to do so—but that is decidedly not the language it chose to use.

The Bureau should stick to the plain meaning of "representative," which effectuates both the plain-text requirements of Section 1033 and its underlying purpose. Under a plain-meaning approach to "representative," the three enumerated terms—"trustee," "agent," and "representative"—have different meanings: some agents are not trustees, and some representatives are not agents, but all three are united by a common thread: third parties acting on behalf of an individual.

---

frequently drafts statutes with enumerated lists in which some listed items are broad enough to encompass others. For example, Rule 60 of the Federal Rules of Civil Procedure includes the phrase "judgment, order, or proceeding." Fed. R. Civ. P. 60(b). There, a litigant attempted to argue that "[s]ince a 'judgment' and 'order' both involve some judicial determination of rights, . . . a 'proceeding' should at least involve some judicial action or conclusive determination of rights." *Waetzig v. Halliburton Energy Servs., Inc.*, 604 U.S. 305, 317 (2025). The Supreme Court rejected that argument, holding that "[a]lthough it is true that statutory terms must be read in the context of their neighbors, that rule cuts the other way here. To read 'proceeding' to require a judicial determination would strip it of any independent meaning." *Id.* Instead, the Supreme Court held, to ensure that each term carries an independent meaning, "proceeding" should be construed *more broadly* than the preceding terms: "[E]ach term should be read as broader than what came before. Just as 'order' encompasses and exceeds 'judgment,' 'proceeding' should encompass and exceed 'order.'" *Id.* Here, too, rather than construing "representative" to *duplicate* the prior two enumerated terms, bedrock principles of statutory interpretation require interpreting it to be *broader* than the two enumerated terms, in line with its dictionary definition.

[37] *See Waetzig*, 604 U.S. at 317–18.

[38] 12 U.S.C. § 92a(a) (emphasis added).

4. In seeking the best reading of the statutory language, what evidence or interpretive principles should the Bureau consider with respect to the term "representative?"

The Bureau should apply traditional principles of statutory interpretation.

The first key principle is that the term "representative" should be read to have its plain or ordinary meaning,[39] and should not—and cannot—be interpreted to mean the same thing as "agent" or "trustee."[40] The outcome of applying this principle is that "representative" should be construed to mean "one acting on behalf of another," without any forced, extra-textual application of fiduciary principles.

The second key principle is that the Bureau's statutory interpretation must account for the "broader context" of the statute as a whole.[41] Other portions of Section 1033 suggest that "representative" includes more than an individual or their fiduciary and extends to third parties offering digital financial services. For example, Section 1033(a) requires that "information shall be made available in an electronic form usable by" individuals, agents, trustees, and representatives,[42] and Section 1033(d) requires the CFPB to prescribe "standards . . . to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to" those same individuals, agents, trustees, and representatives.[43] Given that aggregators and fintech companies were burgeoning at the time Section 1033 was enacted, it makes sense that the statute would protect individuals' right to authorize these third parties to digitally receive individuals' financial information.[44] The broader statutory context of Section 1033 thus necessitates an interpretation of "representative" that gives effect to those adjacent provisions.

Finally, though Section 1033's text and context are clear enough to resolve the interpretive question before the CFPB, the Bureau may also take into account contemporary understandings of the statutory text. The interpretation of "representative" as including authorized third parties is

---

[39] *See* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 69 (2012).

[40] *See TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) ("It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'" (quoting *Duncan v. Walker*, 533 U.S. 167, 174 (2001))).

[41] *Fischer v. United States*, 603 U.S. 480, 486 (2024) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)).

[42] 12 U.S.C. § 5533(a).

[43] *Id.* § 5533(d).

[44] *See* Fiona Fleck, *Aggregation or Aggravation?: The Pros and Cons of Simplicity*, Wall St. J. (Dec. 27, 2002, at 12:01 AM ET), https://www.wsj.com/articles/SB1040930833845714193; Microsoft Corp. et al., *supra* note 19; Off. of the Comptroller of the Currency, Bank-Provided Account Aggregation Services: Guidance to Banks, OCC Bulletin 2001-12 (Feb. 28, 2001), https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html (hereinafter "Feb. 2001 OCC Bulletin"); Trombly, *supra* note 19.

consistent with the general industry understanding of Section 1033(a)'s scope following the CFPA's passage.[45]

5. If a "representative" under 12 U.S.C. 5481(4) is interpreted to mean an individual or entity with fiduciary duties, to what extent would it limit customers' ability to transfer their transaction data to third parties under section 1033 or the ability of financial technology and other third-party service providers to compete with incumbent market participants?

If the term "representative" were interpreted to require a fiduciary relationship, it would drastically limit Americans' ability to share their data with their chosen digital financial services providers. Digital financial services providers—which, up to this point in time, have acted as authorized third-party representatives under Section 1033—generally operate based on contractual agreements, terms of service, and various federal and state consumer protection laws and regulations; they do not, as a matter of course, form fiduciary relationships with individuals in order to provide their services. Nor would it be practical, or in many cases possible, for these providers to restructure their businesses to establish fiduciary relationships. Certainly this is not the model that traditional banks and other financial institutions employ; the vast majority of the services they provide are pursuant to accountholder and customer agreements, not fiduciary relationships. Likewise, an individual's chosen crypto exchange, budgeting app, cash-flow underwriter, peer-to-peer payment platform, and so on, are not structured to act as fiduciaries, even where they are otherwise acting on the consumer's behalf (including to access information); requiring a fiduciary duty would disrupt the viability and competitiveness of these services, and, in turn, individuals' ability to use these services.

Shifting to a fiduciary standard would require digital financial services providers to implement "consumer best-interest" analyses and assume liability for individuals' decisions, effectively converting these providers into personalized advisers. That transformation would vastly expand litigation, raise costs, change the nature of the services provided, and generally deter new market entrants. Meanwhile, incumbent banks would be able to offer facially similar services without the limitations and overhead created by the imposition of a fiduciary duty. This would almost inevitably result in the failure of some digital financial services providers and the severe reduction in competitive pressures that bring innovation and lower prices into the financial services market.

Given that many digital financial services providers, including banks, do not typically act as fiduciaries, a framework where a representative can only gain Section 1033's statutory protection when acting as a fiduciary would prevent almost every company from accessing financial data on an individual's behalf—unless the financial institution holding the data decided to allow the individual to share their data. This puts financial institutions in a position to deny access to

[45] *See, e.g.*, 2018 Treasury Report, *supra* note 13, at 31; Michael S. Barr et al., *Consumer Autonomy and Pathways to Portability in Banking and Financial Services* 4 (Univ. of Mich. Ctr. on Fin., Law & Pol'y Working Paper No. 01, 2019), https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf (noting that a "drafter of the provision that became § 1033" has stated that "the scope of the provision was intended to be broad").

competitive services they find threatening, to degrade access in a manner that favors their own products, and to gate access behind anticompetitive and prohibitive contractual terms—including charging fees for access. For example, if financial institutions determined crypto investments to be "too risky" (or too much of a competitive threat to their own investment services), those banks could simply deny crypto platforms the ability to access data necessary for individuals to onboard to their chosen platform. Giving institutions this power would threaten the competition that this Administration aims to promote and risk its key priorities around de-banking and digital financial assets access.

A narrow definition of "consumer" and "representative" will limit individual consumer choice, not protect individuals. It should be squarely rejected.

6. Does the requirement in section 1033 for the Bureau to prescribe standards promoting the development and use of standardized formats for information made available under section 1033 illuminate the types of entities that should be considered "consumers" or have any other implications for how "representative" under 12 U.S.C. 5481(4) should be interpreted?

"[M]any consumer-authorized third-party representatives were providing personal financial management use cases well before 2010," meaning the "U.S. consumer data sharing market [already] encompassed consumers' authorized third-party representatives at the time Congress enacted the CFPA in 2010."[46] This historical record and Congress's specific reference to standardized, machine-readable formats in Section 1033 make clear that consumer-authorized data sharing is what Congress had in mind when it enacted Section 1033.

Section 1033(d) requires the Bureau to "prescribe standards" that "promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers."[47] The reference to "machine readable" files (as opposed to "human readable" files) suggests that the files will be used not only by individuals, but also by their agents, trustees, and representatives, including digital financial services providers. If Congress had intended only individual consumers to exercise this right, it would not have been necessary to require interoperability through standardized, machine-to-machine formats. Individuals receive information in human-readable form; by contrast, the statutory direction to enable machine-readable transfer indicates that Congress anticipated consumers would rely on technology-based intermediaries to access and use their data on their behalf.

The reference to "standardized formats" further implies that those "machine readable" files will be compatible with multiple types of software. By directing the Bureau to prescribe standards that accommodate machine-to-machine exchange, Congress recognized that "consumers" accessing data under Section 1033(a) (and thus "representatives" under 12 U.S.C. § 5481(4))

---

[46] PFDR Rule, 89 Fed. Reg. at 90,881; *see* Feb. 2001 OCC Bulletin, *supra* note 44; *see also* Matt Hawkins, *The History and Rise of APIs*, Forbes (June 23, 2020, at 8:20 AM EDT), https://www.forbes.com/councils/forbestechcouncil/2020/06/23/the-history-and-rise-of-apis; Belinda Luscombe, *Intuit Buys Mint.com: The Future of Personal Finance?*, Time (Sept. 15, 2009), https://time.com/archive/6906464/intuit-buys-mint-com-the-future-of-personal-finance.

[47] 12 U.S.C. § 5533(d).

would include technology-enabled entities—fintechs, data aggregators, and other software platforms—authorized by consumers to act on their behalf.

This provision, along with Section 1033(a)'s requirement that information be made available in an "electronic form usable" by individuals and their representatives, thus affirms Section 1033's intent to facilitate a broader ecosystem in which authorized third-party representatives access financial data on behalf of individual consumers.

7. If a "representative" under 12 U.S.C. 5481(4) is interpreted not to be required to have fiduciary duties, what elements are required in establishing that the individual is a "representative" acting on behalf of the consumer?

The PFDR Rule includes authorization, certification, and revocation requirements that ensure that a third-party representative is acting on an individual's behalf. For example, a third party's disclosures must be "be clear, conspicuous, and segregated from other material," and individuals may revoke third parties' authorization through a method "that is as easy to access and operate as the initial authorization."[48] The general requirements, particularly to the extent the CFPB retains them in a non-prescriptive form, will ensure that a third-party representative is acting on an individual's behalf, while providing sufficient flexibility for the format and mechanisms underlying authorization, disclosure, and revocation to evolve with market best practices.

8. Are there any legal precedents or other considerations relevant to the above questions based on the applicability of the same definition of "consumer" to other Dodd-Frank Act provisions?

As discussed above, the term "representative," as used in the definition of "consumer," does not imply a fiduciary relationship or require fiduciary duties. When Congress intends to require such a relationship or duties, or to otherwise limit coverage to a subset of representatives, it does so through specific, restrictive terms. Congress's drafting choices elsewhere in the Dodd-Frank Act, the same legislation containing the CFPA and Section 1033, confirm Congress's convention. For example, a Dodd-Frank provision governing treatment of whistleblowers under the Securities Exchange Act of 1934 expressly refers to a whistleblower and their "*legal* representative," not just their "representative."[49] Similarly, a different Dodd-Frank provision added a definition to the Investment Advisers Act of 1940, defining a "retail customer" as "a natural person, or the *legal* representative of such natural person."[50] The decision to use the term "representative" without qualification in the CFPA's definition of "consumer" thus stands in stark contrast to the more restrictive term "*legal* representative" used elsewhere in Dodd-Frank.

The Supreme Court has long treated such variation in statutory language as intentional. In *Russello v. United States*, the Court explained that "[w]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or

[48] 12 C.F.R. §§ 1033.411(a), 1033.421(h).

[49] Investor Protection and Securities Reform Act of 2010, Pub. L. No. 111-203, tit. IX, § 922(a), 124 Stat. 1822, 1843 (codified at 15 U.S.C. § 78u-6(c)(1)(B)(i)(II)) (Title IX of Dodd-Frank) (emphasis added).

[50] *Id.* § 913(g)(2), 124 Stat. at 1829 (codified at 15 U.S.C. § 80b-11(g)(2)) (emphasis added).

exclusion."[51] This principle applies directly here. If Congress had intended the definition of "consumer" to apply only to fiduciaries or some other subset of representatives, it would have expressly limited the statutory language. But "[t]he short answer is that Congress did not write the statute that way."[52]

* * * * *

Defrayment of Costs in Exercising Rights Under Section 1033

Section 1033 requires covered data providers to make available to a consumer or their authorized third party, "***upon request***, financial information in the control or possession" of the data provider.[53] Congress put no restrictions on an individual consumer's or their authorized third party's right to receive covered financial information when they request it. "Upon request" plainly means just that—*upon receipt of a request*, not after payment of a fee. The CFPB does not have the power to override Congress, which is what it would be doing if it allowed fees or otherwise attempted to establish principles for access fees (e.g., fees to "recover reasonable costs"), let alone sought to impose a specific price for data access.

Had Congress intended to allow fees for data access, it would have explicitly said so, just as it has done in other contexts where consumers may request access to their data. For example, in the Fair Credit Reporting Act ("FCRA"), Congress deemed that "a consumer reporting agency may impose a reasonable charge on a consumer . . . if the consumer has already received a free disclosure [of their credit report] during the 12-month period immediately preceding the request."[54] Likewise, in the healthcare context, Congress provided that when individuals seek access to their own electronic healthcare information, the fee "shall not be greater than the entity's labor costs in responding to the request."[55] The law's silence here speaks volumes: fees are not permitted, and the current PFDR Rule's fee ban is thus in line with Section 1033's statutory requirements and jurisdictional limitations.

Permitting access fees would not only exceed the Bureau's authority, it would also undermine market competition, put small companies out of business, and eliminate individuals' ability to use the innovative, competitive financial services on which they rely. Certain Wall Street banks' insistence that authorized data access occur exclusively through their APIs only heightens this risk. While the industry (including Plaid) is aligned on the benefits of API-based data access, access to most financial institutions' APIs is restricted to only those third parties that enter into bilateral agreements with the institutions that own them. Because these APIs are often the exclusive means by which consumers' authorized third parties can access data under Section 1033, dominant institutions have the power to block, choke, thwart, or degrade that access, including through the imposition of prohibitive contractual terms and fees—thus undermining the very access and competition that Section 1033 was meant to foster.

---

[51] 464 U.S. 16, 23 (1983) (quoting *United States v. Wong Kim Bo*, 472 F.2d 720, 722 (5th Cir. 1972)).

[52] *United States v. Naftalin*, 441 U.S. 768, 773–74 (1979).

[53] 12 U.S.C. § 5533(a) (emphasis added).

[54] 15 U.S.C. § 1681j(f).

[55] 42 U.S.C. § 17935(e)(3).

In response to the pushback against fees, certain incumbent financial institutions have claimed that fees must be permitted in order to allow for cost recovery. Aside from the fact that the CFPB has no authority to permit fees, this argument is yet another smokescreen to distract from these financial institutions' anticompetitive aims. For more than a decade, the authorized data-sharing market has existed and developed without the imposition of fees—underscoring that fees are not some critical allowance without which the market will stagnate. Indeed, consumers already pay their financial institutions through existing account fees, loan interest, service charges, and interchange fees; the fees and charges these financial institutions collect go, in part, toward their data-sharing infrastructure. Allowing fees—even for supposed "cost recovery"—would result in double charges for individuals, while carrying severe consequences for competition and innovation in the consumer-authorized data sharing market.

The PFDR Rule was intended to protect consumers' ability to access their data under Section 1033, while encouraging competition and innovation; allowing fees would place that access right directly at risk, while further entrenching incumbents and sacrificing the development of consumer-friendly technologies, including emerging AI solutions. The CFPB should maintain the PFDR Rule's prohibition on fees.

9. Does the PFDR Rule's prohibition on fees represent the best reading of the statute? Why or why not?

Yes. Consumer access is mandatory under Section 1033 and is not subject to any condition other than the request of the individual or their authorized third-party representative. Congress did not authorize covered data providers to charge a fee for that request or access—even a fee that allows for supposed cost recovery. Nor did Congress authorize the CFPB to impose any fees on consumers or market participants or to establish price controls[56] for consumers' data access.

The CFPB is bound by the authority granted to it by Congress, and that authority is limited by the text of the relevant law—both what it says *and what it does not*. To that end, Section 1033's text makes clear that Congress intended to allow consumers to access their data whenever they request it, and to authorize the CFPB to prescribe rules (1) requiring covered persons to make that data available and (2) creating standards and formats for providing that data.[57] It is equally clear from Section 1033's text that Congress intended to prohibit fees for data access and to therefore *not* allow the CFPB to permit such fees:

[56] Section 1033 does not grant the CFPB any authority to fix a price for data access. In fact, the Dodd-Frank Act goes out of its way to prohibit the CFPB from setting prices in the market. *See* 12 U.S.C. § 5517(o) ("No provision of this title shall be construed as conferring authority on the Bureau to establish a usury limit applicable to an extension of credit offered or made by a covered person to a consumer, unless explicitly authorized by law."). So, as a matter of simple law, the CFPB cannot set a data interchange fee and impose it on consumers and commercial entities. *See also* Memorandum from Mark R. Paoletta, Chief Legal Officer, CFPB, to CFPB Staff 3 (Apr. 16, 2025), https://www.consumerfinanceandfintechblog.com/wp-content/uploads/sites/58/2025/04/CFPB-Memo.pdf ("The Bureau's primary consumer enforcement tools are its disclosure statutes. The Bureau shall not engage in attempts to create price controls.").

[57] *See* 12 U.S.C. § 5533(a), (d).

- Section 1033 is titled "Consumer ***rights*** to access information."[58] A right is a "[l]egal entitlement . . . to have or obtain something."[59] For example, the First Amendment provides that "Congress shall make no law . . . prohibiting the free exercise" of religion;[60] this right is not conditional—it makes clear that the American people can freely practice their religion without condition. The same is true of the data access right in Section 1033. The imposition of access fees would impede a consumer's ability to exercise this right.

- Section 1033 also requires that covered persons "***shall*** make available . . . ***upon request***" (by an individual or authorized third-party representative) certain financial data.[61] The phrase "shall make available" is definitive and unconditional, particularly when paired with "upon request." Notably, Congress did not say "may" or "can," and certainly did ***not*** say "shall, *subject to payment of reasonable costs*, make available." "You shall not pass!" was not conditional on the Balrog paying Gandalf a bridge toll. Congress could have subjected the consumer's data access right to the imposition of fees. It did not.

Given the clear language of Section 1033 and the lack of any authority for the CFPB to permit fees, the PFDR Rule's prohibition on fees must be maintained.

10. Was the PFDR Rule correct to conclude that permitting fees "would obstruct the data access right that Congress contemplated"? Why or why not?

Yes. Allowing entrenched financial institutions to set rates on data access will result in their smaller competitors—community banks, credit unions, and fintechs—paying monopoly rents to the same publicly subsidized, too-big-to-fail financial institutions they are trying to disrupt and in individuals having fewer and more expensive choices in the market.

Consumer harm: Americans, particularly lower-income individuals, are price sensitive when it comes to financial services.[62] The imposition of access fees—which individual consumers will ultimately bear, directly or indirectly[63]—will prevent some individuals from being able to use the innovative, competitive services that they have relied on up to this point. Indeed, such fees would doubly interfere with the goals of Section 1033, as one of the core benefits of the data access

[58] *Id.* § 5533 (emphasis added).

[59] *Right*, *Oxford English Dictionary* (3d ed. 2010) (def. II.8), https://www.oed.com/dictionary/right_n.

[60] U.S. Const. amend. I.

[61] 12 U.S.C. § 5533(a) (emphasis added).

[62] For example, a Federal Deposit Insurance Corporation 2021 national survey found that almost three in ten unbanked households (29.2%) cited "[b]ank account fees are too high" as their primary reason for not having one. FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households* 2 (Oct. 2022), https://www.fdic.gov/analysis/household-survey/2021report.pdf.

[63] *See* Luisa Beltran, *JPMorgan's Plan to Charge for Data Could 'Cripple' Crypto and Fintech Startups, Execs Warn*, Fortune (July 16, 2025), https://finance.yahoo.com/news/jpmorgan-plan-charge-data-could-195633869.html; Jeff Kauflin, *Fintechs Consider Raising Prices Due to JPMorgan's Looming Fees*, Forbes (updated Sept. 10, 2025, at 5:34 PM EDT), https://www.forbes.com/sites/jeffkauflin/2025/08/28/fintechs-consider-raising-prices-due-to-jpmorgans-looming-fees.

right is the ability for consumers to shop around and get a better rate. If a fee is imposed on that shopping, the consumers most impacted will be the ones who struggle the most to make ends meet and who would most benefit from lowering the cost of their financial services.

Business harm: Allowing fees, including for cost recovery, would punish smaller and innovative market participants. Take, for example, a community bank that is trying to attract customers by building a personal financial management feature and which has a free API provided by a core service provider. When the community bank, acting as an authorized third-party representative of the individual, accesses data from a Top 10 bank, which has built its own API, it would incur a fee because the Top 10 bank claims that its already-existing API was expensive to build or is expensive to maintain. The community bank will either be forced to eat the cost, thus harming its margins and ability to survive, or pass the cost along to its customers. In contrast, when that Top 10 bank offers a similar personal financial management tool, it would pay no fee to access data from the community bank, which has no costs to recover for its free API. Why should the community bank pay for the Top 10 bank's technology and vendor choices, and get punished for its own? Substitute the community bank for a fintech company or innovative new market entrant, and you get the same result. Fees are an anticompetitive lever that distort an otherwise competitive market, tilting it toward dominant incumbents while simultaneously requiring challenger companies to subsidize the very incumbents bent on their demise.

Market harm: During President Trump's first term, the OCC found that large banks have the market power to fix the price of financial services. The OCC noted that "[t]he dominant market position of the large bank population is clear when all OCC-regulated institutions with assets of $100 billion or more are considered. Together, these banks account for approximately 55 percent of the total assets and deposits of all U.S. banks and hold approximately 50 percent of the dollar value of outstanding loans and leases in the United States."[64] The OCC warned that "a decision by one or more of these banks not to provide a person with fair access to financial services could have a significant effect on that person, the nation's financial and economic systems, and the global economy," particularly if the service "is not available on reasonable terms elsewhere."[65] ***This—fair access, financial and economic system impact, global economy effects—is exactly what is at risk if access fees are permitted.*** This risk exists because data providers have a 100% monopoly on their customers' data, creating the potential for them to charge monopoly rents that, at minimum, raise significant barriers to entry for would-be competitors and, at worst, make it economically impossible for individuals to access their financial data.[66]

Also troubling is that allowing access fees—or even staying silent on fees and "letting the market set prices"—would create a massive wealth transfer from community banks, credit unions, and challenger companies to the biggest Wall Street banks. That is because financial data is not

[64] Fair Access to Financial Services, 85 Fed. Reg. 75,261, 75,264 (proposed Nov. 25, 2020).

[65] *Id.*

[66] "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. 74,796, 74,814 (proposed Oct. 31, 2023).

equally distributed across the more-than-10,000 entities covered by Section 1033. The vast majority of consumer data is held by a very small number of the largest banks—without access to which no financial data product or service is viable. The ten largest bank data providers control approximately 45% of consumer data access, according to Plaid's data. No challenger—whether a community bank, credit union, fintech company, or new market entrant—can successfully offer a product that requires consumer-authorized data access if they cannot offer it to more than 40% of the market. If the CFPB eliminates the prohibition on fees, the largest data providers will be able to use their dominant market power to demand any rate they want from challenger companies requesting to access data on behalf of an individual. These companies will have no choice but to absorb fees or raise prices simply to survive—rendering those companies less competitive (or worse, defunct), increasing hurdles for consumers to access services of their choice, and thwarting American innovation.

> ***11. What is a reasonable range of estimates regarding the fixed costs to "covered persons" of putting in place the standards required by sub-section D of section 1033 and the operational architecture to intake, document, and process requests made by consumers, including natural persons and persons acting on behalf of a natural person (i.e., an agent, trustee, or representative)? How do these estimates vary by the size of the covered financial institution?***
>
> ***12. What is a reasonable range of estimates regarding the marginal cost to covered financial institutions of responding to requests made under the auspices of section 1033? How do these estimates vary by the size of the covered financial institution?***

Plaid answers Questions 11 and 12 together. While Plaid itself has not incurred the costs associated with building and maintaining a developer interface (or bank API), it has entered into multiple data access agreements with financial institutions to access their developer interfaces. Since 2018, none of those institutions has shared specific information related to their costs in establishing or maintaining their developer interfaces, despite Plaid's repeated requests. While Plaid has not been able to obtain that information, it is notable that—with one recent exception[67]—none of those institutions has imposed ongoing fees for access, having built and maintained developer interfaces for their own commercial reasons and recovering infrastructure costs through account fees, interest payments, and other service charges.

Allowing data providers to charge fees, including to recover costs of data access, would create perverse incentives and absurd outcomes because different financial institutions have wildly different costs.[68] The CFPB estimated that an institution's cost to establish an API ranged from $2 million to $20 million, which was, in fact, wrong: the cost for the majority of institutions that have an API is $0. For example, in November 2020, Plaid and Jack Henry announced an

[67] *See* Justin Bachman, *Fintechs Blast JPMorgan Over Data Fees*, Payments Dive (July 15, 2025), https://www.paymentsdive.com/news/fintechs-blast-jpmorgan-over-data-fees/753021; Alex Rampell, *How Big Bank Fees Could Kill Fintech Competition*, Andreessen Horowitz (July 31, 2025), https://a16z.com/newsletter/big-bank-fees-could-kill-competition.

[68] To the extent they can even calculate them. Throughout the entire PFDR rulemaking process, none of the large banks provided the Bureau with its actual costs for building and running those APIs.

agreement to move over 350 banks to API-based access using Jack Henry's Banno Digital Platform.[69] One of the conditions of that deal, which still holds today, was that "[i]t will also come at no cost to Banno clients."[70] In this environment, what is a "reasonable" cost to one data provider would be outrageously expensive to another.

13. How is the range above affected by the need of the "covered person" to confirm that an agent, trustee, or representative acting on behalf of an individual has actually been authorized by the consumer to act on their behalf?

It is not. First, under the PFDR Rule, "covered persons" are *not* required to confirm that an agent, trustee, or representative has been authorized by the consumer to act on their behalf. The Rule only says that covered persons are "*permitted* to confirm the scope of a third party's authorization."[71] Thus, any expense a covered person incurs in confirming this authorization is purely voluntary and should not be incorporated into any calculation of a cost that should be shared between a covered person and a consumer. Second, Plaid has developed technical integrations, which we provide to covered persons for free, that allow the covered person to obtain a real-time record of the consumer's authorization.[72] Other market participants have or can develop similar technologies, obviating the need for covered persons to incur any cost related to confirmation of authorization.

14. Is there any legal precedent from other Federal statutes, not involving Federal criminal law or provision of services by the U.S. Government, where there is a similar omission of explicit authorization to the agency to set a cost sharing balance in effectuation of a new statutory right and, if so, what principles has the court allowed the agency to use in establishing a proper balance?

We are unaware of any legal precedent in which there is a similar omission of explicit authorization to the agency to set a cost-sharing balance in effectuation of a new statutory right, but where the agency has nonetheless concluded it has the authority to promulgate a cost-sharing regime. Instead, the lack of explicit authorization is a sign that there is no authorization. The Supreme Court's decision in *Loper Bright Enterprises v. Raimondo* dictates that, if the CFPB does wade into cost-allocation, it would not receive deference on that choice.[73]

---

[69] See Reed Bouchelle, Plaid and Jack Henry Partner to Enable Plaid Exchange for Over 350 Banks, Plaid (Nov. 24, 2020), https://plaid.com/blog/plaid-exchange-jack-henry.

[70] *Id.*

[71] 12 C.F.R. § 1033.331(b)(2) (emphasis added). This ability to confirm the scope of a third party's authorization provides opportunities for incumbent financial institutions to introduce anticompetitive messaging or other friction to try to dissuade individuals from pursuing competitive products. The Bureau should remove this opportunity for mischief as part of this rulemaking.

[72] *See All of Your Customer Connections*, Plaid, https://plaid.com/products/permissions-manager (last visited Oct. 19, 2025).

[73] *See* 603 U.S. 369, 381–82 (2024) (emphasizing that questions of an agency's statutory authority when statutes are ambiguous are for Congress or courts to decide, not for agencies to resolve through their own policy discretion).

In contrast, agencies have been permitted to allow fees and cost-sharing only where Congress expressly contemplated as much. For example:

- In the healthcare context, Congress has conferred a statutory "right" to obtain electronic healthcare information, while providing that fees for providing that information "shall not be greater than the entity's labor costs in responding to the request."[74]

- The Telecommunications Act requires carriers to let consumers keep their phone numbers when switching providers and expressly directs the FCC to ensure the costs of implementation are borne "on a competitively neutral basis."[75] Accordingly, the FCC established standards by which state regulators could allocate costs, which the Ninth Circuit upheld.[76]

- The Telecommunications Act's universal service provisions also establish a nationwide right to telecommunications access. In the statute, Congress expressly stated that contribution requirements should be levied on equitable and nondiscriminatory terms.[77] Consistent with that instruction, the FCC adopted contribution mechanisms implementing those principles. The Supreme Court later upheld the statute's "equitable and nondiscriminatory" standard as an intelligible principle against a nondelegation challenge, confirming that Congress, not the agency, supplied the guiding standards for the FCC's contribution formulas.[78]

- Under the Federal Power Act, Congress specifically guaranteed "just and reasonable" and "nondiscriminatory" fee-based access to the transmission grid. FERC therefore permissibly applied a "beneficiaries pay" principle, requiring costs to be roughly commensurate with benefits, and the D.C. Circuit has upheld FERC's action in this area.[79]

Together, these decisions show that, when Congress decides to authorize fees or cost-sharing, it is explicit in its provision of this authority to the applicable federal agency. In contrast, where Congress is silent, the Supreme Court has made clear that agencies do not have authority to permit fees or cost-sharing. Because Section 1033 does not authorize any fees or cost-sharing, the Bureau acted correctly in declining to permit fees in its PFDR Rule and has no authority to now reverse course.

---

[74] 42 U.S.C. § 17935(e)(1), (3).

[75] 47 U.S.C. § 251(e)(2).

[76] *See US W. Commc'ns v. MFS Intelenet, Inc.*, 193 F.3d 1112, 1120–21 (9th Cir. 1999).

[77] 47 U.S.C. § 254(b)(4).

[78] *See FCC v. Consumers' Rsch.*, 145 S. Ct. 2482, 2511 (2025).

[79] *See FirstEnergy Serv. Co. v. FERC*, 758 F.3d 346, 352–56 (D.C. Cir. 2014).

15. Absent any legal precedent from other laws, should covered persons be able to recover a reasonable rate for offsetting the cost of enabling consumers to exercise their rights under section 1033? Why or why not?

No. There *is* legal precedent, as discussed above, which directly supports a prohibition on access fees. In short, the CFPB and covered persons are bound by the text of Section 1033, which does not allow for access fees and instead requires that covered persons make consumers' data available to them *upon request*. However, even if such precedent did not exist, covered persons should still be prohibited from recovering any fees, including supposed reasonable costs; to decide otherwise would result in severe harm to Americans, small businesses, and the market.

The consumer-permissioned data sharing market has successfully operated for years, including transitioning to API-based access, *without fees (including for cost recovery)*. Seventy-five percent of Plaid's data access traffic has moved to APIs without any financial institution imposing ongoing fees for its API;[80] another 7% is committed to move to API, again without any ongoing fees. Even more remarkably, over 1,500 financial institutions that are *not* covered under the PFDR Rule (because they have fewer than $850 million in assets), but are covered by Section 1033, have already been enabled on API-based access. To Plaid's knowledge, none of these financial institutions charges for ongoing API access (and the vast majority of them got their APIs for free from their chosen digital banking platform).[81] Perhaps this is because banks in particular already recover costs relating to their infrastructure through existing account fees, loan interest, service charges, and interchange fees. Permitting fees as part of the PFDR Rule would result in consumers being double-charged.

Tellingly, by far the loudest voices claiming that APIs are expensive and demanding the right to charge for their use are the same ones that advocated for their mandatory use. The Bureau should not reward the rent-seeking of the largest Wall Street banks with a windfall revenue stream.

Finally, access fees would create a permanent incentive against improving current technologies used to access individuals' data, such as developer interfaces. If a Wall Street bank with an expensive API—that it built for its own commercial reasons and to its own specifications—can impose the cost of its outdated or inefficient technology on others, why would it ever aim to bring those costs down? Indeed, a financial institution enjoying the government-permitted welfare of cost recovery might decide to hire more people than it needs, build features that add cost but not value, or bundle in capabilities that do not serve market needs. *Why not? Someone else is paying for it.*

[80] In light of regulatory ambiguity, one bank recently demanded fees for access to data under Section 1033, but that bank's traffic had moved to API many years ago, without demanding fees.

[81] Notably, few if any of these banks are members of the trade association representing the largest Wall Street banks which sued the CFPB demanding the right to charge for data access.

16. If covered persons should be able to recover a reasonable rate for offsetting the costs of enabling consumers to exercise their rights under section 1033, should the Bureau place a cap on the upper bounds of such rates that can be charged? If so, what should the cap be on such rates, and why? If not, why not?

The CFPB should not place a cap because it should not permit fees, including cost recovery, at all. Any such cap would also be arbitrary, capricious, and create competitive distortions and poor incentives in the market. Different financial institutions have wildly different costs in managing their internal and vendor technologies. In the case of data access, these costs could range from $0—the "cost" for several hundred banks using Jack Henry's Banno Digital Banking Platform—to the CFPB's top-end estimate of $20 million. Under these circumstances, any cap intended to account for "cost recovery" would almost certainly be "wrong"—that is, it would be higher than the cost for some institutions and lower than the cost for others. That distortion would disincentivize innovation and cause the entire market to move to the cap. An entity enjoying a regulatory subsidy supporting its inefficient technology—particularly a subsidy that simultaneously obviates that entity's need to compete by effectively pricing out the competition—will have *no* reason to improve that technology.

17. If consumers ought to bear some of the cost in implementing requirements under section 1033, should that be shared by every consumer of a covered person, including those who may not wish to exercise their rights under section 1033?

To the extent the CFPB disagrees with Plaid's analysis above that fees, including for cost recovery, are not permitted, then the answer is, "Yes." The financial services market is replete with forms of basic infrastructure that are paid for, but not used by, every customer of a financial institution. For example, almost every bank has at least one branch, and some have many thousands of branches. These physical branches cost money, and that business expense is spread across the bank's entire customer base regardless of whether the bank's customers ever use even a single one of those branches. Banks similarly have websites and apps, the costs of which are shared by all bank customers, even if some bank customers do not use them. Data access is the financial services infrastructure of the 21st century, and, to the extent cost-recovery is permitted, it should be shared across all the customers of a financial institution the way other infrastructure costs are. Indeed, *it already is* through banks' existing cost recovery mechanisms, discussed above.

* * * * *

Information Security Concerns in the Exercise of Section 1033 Rights

The security of people's financial data is foundational to a well-functioning consumer-authorized data sharing market, and the PFDR Rule takes meaningful steps toward ensuring that responsibility is borne by all market participants. By grounding the Rule's security framework in the existing GLBA Safeguards Rule[82]—a flexible, risk-based standard already used within the

[82] Or the FTC's equivalent rule. *See* 16 C.F.R. pt. 314.

industry—the CFPB avoided imposing a patchwork of new or duplicative requirements. This approach allows digital financial services providers to compete and innovate while maintaining strong consumer protections.

Some large financial institutions nevertheless continue to misuse security "concerns" as a pretext to stifle the consumer-authorized data sharing market. These concerns—targeted at authorized third parties providing competitive digital financial services—are designed to attract regulatory sympathy, but they exaggerate risks that are already mitigated by a myriad of federal and state laws governing data security and liability that apply to those authorized third parties.[83]

The framework for protecting consumer financial data, including in the PFDR Rule, is already comprehensive, well-tested, and effective, and does not need additional requirements. In addition to GLBA Safeguards, other statutes such as the EFTA and the Bureau's Unfair, Deceptive, or Abusive Acts or Practices ("UDAAP") authorities—along with state data breach and privacy laws—establish clear, enforceable obligations that ensure accountability, data security, and protection across the financial ecosystem. These laws define liability for safeguarding consumer information, preventing fraud, and ensuring authorized financial transfers. Further obligations that merely add regulatory complexity and burden, without any commensurate additional consumer protection, are not needed and simply increase barriers to competition.

Separately, while the PFDR Rule appropriately grounds its approach to security in existing law, as currently drafted it does not adequately incentivize the elimination of screen scraping. The Bureau should make several changes to ensure individuals can access all of their financial information while also creating incentives for the market to transition away from screen scraping. Specifically, data providers that include non-covered data elements in their developer interfaces should be permitted to block screen scraping for those elements so long as they otherwise meet the Rule's developer interface performance standards.

18. Does the PFDR Rule provide adequate protections for the security of consumer's data? Why or why not?

Yes. The PFDR Rule provides adequate protections for the security of consumers' data by incorporating the already-existing requirements of the GLBA Safeguards Rule. The Safeguards Rule applies to banks and other financial institutions and has proven effective in protecting consumers and their information. It ensures that all such entities are subject to comparable baseline security obligations, including requirements for risk assessments, safeguards, testing, and oversight of service providers. The Safeguards Rule also offers a flexible, risk-based approach that is tailored to the size and complexity of each entity and the sensitivity of the information at issue. By allowing for this flexibility, the Safeguards Rule enables entities to adopt strong existing practices, while retaining room to innovate and adapt as the market and related threats evolve.

By using the Safeguards Rule framework, the PFDR Rule thus protects consumers' data, while

[83] As noted above, it is well-recognized that "dominant market participants use privacy and security as a justification to disallow interoperability and foreclose competition." Off. of Tech. & Bureau of Competition, *supra* note 7.

avoiding the imposition of conflicting or duplicative requirements and ensuring that consistent regulatory standards apply to that data, regardless of whether it is held by a data provider or authorized third party.

21. In what way does the existence or non-existence of a fiduciary relationship affect the incentives in doing cost-benefit analysis regarding the level of information security established?

The existence or non-existence of a fiduciary relationship does *not* affect the incentives in a cost-benefit analysis regarding information security. In both theory and practice, business, financial, reputational, and regulatory considerations—not fiduciary principles—drive companies to implement strong information security regimes. For many companies, their public reputations and values, as well as their ability to attract and maintain customers, are critically dependent upon their security posture, with many companies going beyond baseline industry standards as a competitive differentiator. For example, companies like Apple have made security and privacy core to their value proposition, but Apple is not a fiduciary of its customers. So too with Plaid itself—we pride ourselves on our robust security posture, which meets or exceeds the standards imposed by the GLBA Safeguards Rule.

Certain large financial institutions, supposedly in the name of greater security, advocate for a narrow reading of Section 1033 that would allow only third-party fiduciaries to access data on an individual's behalf. But that reading is not only wrong, but also borne of pretextual, anticompetitive motives. These same institutions typically do not have fiduciary relationships with their customers, but they nevertheless have strong incentives, as well as legal obligations, to maintain robust information security systems.[84] The same is true of many non-bank financial companies—money transmitters, payment processors, and credit agencies, just to name a few. There is no basis, in law or in practice, for an assertion that more stringent security protections exist where a company has a fiduciary relationship.

25. Covered persons are subject to several legal obligations regarding risk management, such as safety and soundness standards, Bank Secrecy Act (BSA) requirements, and Anti-Money Laundering (AML) regulations. What should covered persons consider under these legal obligations when making information available to consumers? How could the PFDR Rule's interface access provision better allow covered persons to satisfy these legal obligations?

The Bureau should leverage emerging technology by allowing covered persons to enhance their existing customer identification program ("CIP") efforts using information provided by digital financial services providers. These providers often maintain up-to-date device data and other indicators of suspicious activity that can materially strengthen fraud detection and systemic risk monitoring. Permitting covered persons to securely integrate this information would also improve BSA and AML compliance, reduce duplicative verification burdens for consumers, and support the identification of potentially suspicious activities such as money laundering or fraud. Digital financial services providers, like fintechs and aggregators, may also be able to supply

[84] Indeed, full-service financial institutions do not offer higher security standards to, say, their registered investment advisor accounts than they do to ordinary checking accounts.

insights that allow covered persons with fewer resources and less sophisticated compliance and security frameworks to enhance their own processes in a manner otherwise only feasible for larger institutions. To facilitate this, the Bureau could encourage digital financial services providers to share with covered persons fields or metadata designed to support identity checks, AML alerts, or other fraud prevention.[85]

26. What are the costs and benefits of the PFDR Rule's reliance on existing information security standards in the GLBA?

The PFDR Rule's reliance on the GLBA Safeguards Rule and equivalent FTC standards yields substantial benefits for data providers, authorized third parties, and individual consumers. Most entities in the consumer-authorized data sharing market—whether banks or fintechs—are already subject to GLBA Safeguards. Aligning the PFDR Rule's security expectations with the GLBA Safeguards Rule avoids layering new, conflicting, or ambiguous frameworks on top of a standard already used within the industry. This alignment reduces compliance ambiguity, lowers implementation costs, and ensures that all parties managing consumer financial data are held to clear, enforceable, and consistent obligations grounded in existing law.

Importantly, this approach promotes regulatory consistency across an increasingly interconnected financial services landscape. Many financial institutions now operate on both sides of the data-sharing equation—both as data providers and as authorized third parties. If the Bureau were to require different security standards for each functional role, it would introduce unnecessary operational complexity and legal uncertainty for all participants. For example, financial institutions would need to apply one standard when operating as data providers, and another when operating as authorized third parties. Fragmenting security obligations in this way risks weakening protections rather than strengthening them.

27. To what information security standards ought entities adhere when accessing consumer financial data held by a covered person, and who is best positioned to evaluate whether these entities are adhering to such standards?

The GLBA Safeguards Rule remains the most appropriate and effective baseline standard for entities accessing consumer financial data from covered persons. It is widely recognized, adaptable to different business models and risk profiles, and already applies to most authorized third parties and data providers. By applying this same standard within the context of Section 1033, the Bureau can ensure consumers benefit from consistent protections regardless of where their data resides.

With respect to evaluation of adherence, the PFDR Rule currently allows data providers to deny access based on self-determined security "concerns"; this arrangement invites conflicts of

[85] In the context of consumer-authorized data sharing, digital financial services providers are not service providers or vendors to financial institutions. Rather, they are chosen and used by individual consumers independently of those consumers' relationships with their financial institutions. Because there may not be a commercial relationship between the digital financial services provider and financial institution governing the sharing of such information, it is important for the Bureau to encourage the arms-length provision of information that may combat financial crime.

interest and undermines the Bureau's pro-competitive objectives. Many entities accessing consumer financial data are already supervised by federal agencies, including the CFPB. For those that fall outside the scope of direct supervision, the Bureau should adopt an approach that allows compliance with the Rule's security requirements to be demonstrated through third-party certifications or audits conducted against established frameworks such as ISO 27001, SOC 2, or NIST CSF. These assessments should be conducted by qualified, independent assessors to avoid conflicts of interest and promote trust across the ecosystem. These changes to the PFDR Rule's approach would ensure compliance with security requirements, while ensuring that third parties' access is not controlled by the very incumbent data providers with which they compete.

28. What are the costs and benefits of the PFDR Rule's provisions designed to reduce the use of screen scraping? What changes would better protect the security of consumer credentials?

Even before its finalization, the anticipation of a forthcoming PFDR Rule contributed to meaningful progress in expanding secure, API-based data access. In response, many data providers accelerated their move toward modernized, secure access technologies. However, the Rule as currently drafted does not adequately incentivize the complete elimination of screen scraping and, if left unchanged, could put financial data access at risk for millions of consumers. The Bureau should make several changes to ensure that consumers have access to all of their financial information, while also creating better incentives for the market to fully transition away from screen scraping.

First, it is critical to understand the reality of the data access landscape today. Over 150 million consumers have used Plaid to access their financial data.[86] As mentioned above, over 75% of data access on Plaid's network today is through APIs. But that also means that tens of millions of consumers, whose financial institutions either do not have or make available APIs, currently rely on screen scraping to access their data. If the Bureau were to prohibit screen scraping today, those tens of millions of consumers would either lose access to financial services *they currently rely on*, or be forced to change their bank—in almost all cases leaving a community bank or credit union for a large Wall Street bank. 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.[87]

Given that market reality, the current PFDR rule has two key limitations in reducing the use of screen scraping.

- First, banks with under $850 million in assets are exempted from the requirement to build developer interfaces. While Plaid has diligently secured API access for many of these institutions, generally through partnerships with digital bank platforms and at no cost to the data providers, market momentum in API adoption amongst these banks has tapered

[86] Justina Chen & Brenna Ramsey, *Setting the Standard for Safer, Permissioned Data Access*, Plaid (Sept. 11, 2025), https://plaid.com/blog/open-finance-trust-security.

[87] 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, when data providers refuse to make data available absent anticompetitive conditions, or when third parties have not yet been able to negotiate a data access agreement.

off, with hundreds of institutions representing millions of consumers still accessible only through screen scraping. The Rule does nothing to incentivize these data providers to transition access to APIs. Absent regulatory incentives, it is possible some screen scraping will persist in perpetuity because some data providers will choose not to transition to APIs. If there is a blanket ban on screen scraping, customers of those institutions will lose access or the ability to authorize access to their financial data in violation of Section 1033.[88]

- Second, the PFDR Rule does not cover all account or data types regularly accessed by consumers and their representatives today—mortgage, auto, and student loan data being several glaring omissions. These financial accounts and data types are clearly covered by Section 1033, but the Bureau simply chose to limit the scope of the initial PFDR Rule for expediency, clearly stating its intent to expand to other accounts and data types in future rulemakings.[89] Today, some data providers make these accounts and data types available via their APIs. However, if the Rule were to ban screen scraping while only covering a subset of accounts and data types, nothing would prevent data providers from thereafter removing those accounts and data types from their developer interfaces, and data providers currently lacking APIs may decide to comply with the existing Rule by building "bare minimum" APIs that omit these accounts and data types. If developer interfaces do not have all the data types and accounts ***that consumers and their representatives are currently accessing and using for consumers' financial benefit***, then the only way to maintain full data access will be to use both developer interfaces and screen scraping.

The Bureau recognized this problem in the PFDR Rule:

> Nothing in the proposal would have precluded data providers from blocking screen scraping, and nothing in the final rule does so. However, data providers may act improperly if they attempt to block screen scraping across the board without making the requested data available through a more secure alternative. Depending on the facts and circumstances, such interference with the consumer's ability to share their personal financial data may violate the CFPA's prohibition on acts or practices that are unfair, deceptive, or abusive.[90]

The Bureau even suggested a solution to the problem:

---

[88] To be clear, Plaid does not advocate that the Bureau eliminate the exemption for financial institutions with under $850 million in assets. Although many of those institutions have been able to transition to APIs for free, a government mandate should be a last resort, and it would be far better for the Bureau to create a Rule with incentives to speed the market transition to API access, particularly for smaller institutions. Plaid does, however, strongly believe that no consumer should ever lack the means of accessing, or authorizing their representative to access, their financial data. A complete lack of access is a clear violation of Congress' law.

[89] *See* PFDR Rule, 89 Fed. Reg. at 90,856 ("The CFPB intends to implement CFPA section 1033 with respect to other covered persons and consumer financial products or services through future rulemaking.").

[90] *Id.* at 90,895.

> However, if a data provider has established a developer interface that complies with—or in markets not yet covered by this final rule, conforms to—the requirements of this final rule, then blocking screen scraping may further consumer privacy and data security while ensuring that consumers are able to authorize access to their financial data in a manner that is safe, secure, reliable and promoting of competition.[91]

The PFDR Rule stopped short of mandating this solution, or even creating an incentive for market participants to implement it. As a result, the Rule does not go far enough to eliminate screen scraping altogether.

The Bureau has two options for improving the Rule to incentivize the adoption of APIs. First, the Bureau could revise the Rule or promulgate future rules, expanding the scope of data coverage to include *all* data types and accounts covered by Section 1033. When a data provider complies with the Rule's requirements regarding performance and data coverage, screen scraping could be prohibited. While this comprehensive approach should make significant strides toward eliminating screen scraping, it would require a much broader revision of the PFDR Rule than currently contemplated.

An alternative approach would be to prohibit screen scraping when accounts and data types covered by Section 1033, even if not presently covered by the PFDR Rule, are made available to the consumer or their authorized third-party representative—***without a fee***—through a developer interface that meets all other access, scope, and performance standards. This approach would incentivize covered data providers to voluntarily make accounts and data types not presently covered by the PFDR Rule available in their developer interfaces in order to eliminate screen scraping. And it would incentivize third parties to use those developer interfaces because access outside of them—provided the interface meets all the stringent requirements needed for consumers to benefit from access—would be prohibited. As more of the market shifts away from screen scraping, non-covered data providers will also feel the pressure to meet consumer expectations around secure and comprehensive data access.

Under either approach, in order to ensure that consumers maintain access to their data, the Bureau would need to be clear that screen scraping is permitted when a developer interface is down—even temporarily—or throttled, limited only to certain parties, or fails to meet the PFDR Rule's performance requirements. Plaid's proposals above are, of course, contingent on access fees remaining subject to a blanket prohibition; in the face of such fees, many authorized third parties may have no choice other than to begin searching for alternate means of data access in order to avoid their harmful consequences.

> ***29. Does the PFDR Rule provide adequate protections for consumers and covered persons to ensure that the request for a consumer's information is in fact knowingly authorized by the individual consumer and that the information is in fact being made available to the consumer as opposed to a malicious actor?***

Yes. The PFDR Rule includes important safeguards to ensure that data access requests are

[91] *Id.*

knowingly authorized by individual consumers. Its requirements for standardized authorization disclosures—specifying the categories of data requested, the purpose of access, the duration of consent, and the consumer's right to revoke—help ensure that authorization is clear, conspicuous, and informed. By mandating these disclosures, the Rule builds a strong foundation for protecting consumers against unauthorized access. The Rule's reliance on GLBA Safeguards also provides appropriate protections to ensure that information is being appropriately made available to the consumer and not a malicious actor. For example, the Safeguards Rule requires institutions to "[p]protect against unauthorized access to or use of [customer] information that could result in substantial harm or inconvenience to any customer."[92]

Any revised version of the Rule should preserve these core protections while allowing for evolving authentication and fraud prevention tools to be incorporated. As threats from impersonation and account takeover evolve, so too must the security measures used to guard against them. New technologies—such as passkeys and digital identification—offer promising ways to verify that access requests originate from the actual consumer, rather than from a malicious actor. The Rule should remain technology-neutral to accommodate such innovations as they become more widely adopted and validated.

* * * * *

Privacy Concerns in the Exercise of Section 1033 Rights

At its heart, Section 1033 is about the fundamental right of Americans to access their financial data—both directly and through authorized third-party representatives. This right unlocks for consumers the ability to use their chosen digital financial services providers, which rely on that data to provide their services. It also highlights the need to ensure that a representative is indeed authorized to act on behalf of an individual in accessing their data. As Treasury explained in its 2018 Report, consumer financial "products and services . . . require ***consumer authorization as the legal basis for accessing*** the financial account and transaction data."[93] Within the context of Section 1033, critical consumer protections thus take the form of the steps necessary to ensure that a third party is authorized to act as a representative on behalf of the individual. The provisions of the PFDR Rule relating to authorization, certification, and revocation accomplish this, ensuring that consumers retain control over their data. Plaid thus respectfully recommends that the CFPB retain in the PFDR Rule a non-prescriptive requirement that third parties provide to individual consumers transparent, comprehensible, and readily accessible disclosures regarding data access, as well as a requirement that third parties provide a revocation mechanism so consumers can revoke their prior authorizations.[94]

The PFDR Rule, however, went further than regulating access and authorization and instead purported to enact, without proper authority, a prescriptive and novel federal privacy regime. More specifically, the PFDR Rule limited data use to ***only*** that which is "reasonably necessary"

[92] 16 C.F.R. § 314.3(b)(3).

[93] 2018 Treasury Report, *supra* note 18, at 32 (emphasis added).

[94] The disclosures should continue to broadly ensure that the consumer has information regarding (i) to whom the consumer is granting access, (ii) what data is being accessed and shared, and (iii) for what purposes, so that they can make an informed decision whether to grant access to their data.

for the authorized third party to provide the original product or service the consumer requested.[95] This could be construed as prohibiting authorized third parties from using covered data for beneficial purposes, including developing new and innovative products and providing additional services to a company's own customers—*regardless of whether the consumer authorized those uses*. By rigidly constricting individual consumers' right to control how their financial data can be used, the CFPB not only substituted its moral and political judgments for those of individual consumers, stripping them of the control and access inherent to Section 1033 itself, it also untethered the PFDR Rule from its source.

Consider a consumer who uses a budgeting app to manage their finances. That consumer can explicitly authorize the app to access their checking account or credit card data for the budgeting use case, and they can revoke that access at any time. But if the same consumer wants the budgeting app to use that data to help them identify other useful tools or products in the marketplace (for example, a lower fee deposit account or a more competitive rate on a loan), under the PFDR Rule, they cannot simply consent or opt-in to that use because the Rule categorically deems "[c]ross-selling of other products or services" not "reasonably necessary" to provide the budgeting app and therefore not permitted.[96] To comply with the PFDR Rule, the budgeting app arguably must set up this use as a standalone service that the consumer can seek in the market and require the consumer to redo the entire authorization process simply to grant the same app access to the same data to offer this additional use. With these cumbersome and redundant requirements, the CFPB overstepped its mandate and hindered innovative companies from designing the best financial services and user experiences for consumers.

The CFPB not only went beyond its own jurisdictional authority in promulgating such extensive restrictions, but also beyond major domestic[97] and international[98] privacy laws, placing American competition and innovation at risk. Congress most assuredly did not intend for an American consumer to have less control over and fewer rights with respect to their data than a consumer in France. If the data use restrictions within the PFDR Rule are retained (and Plaid notes that they can be easily excised without altering the Rule's other critical protections), they risk impeding the development of innovative new financial products ranging from cash flow underwriting to crypto investments to payments enablement, which would run afoul of this Administration's position that "[r]egulations that reduce competition, entrepreneurship, and innovation—as well as the benefits they create for American consumers—should be eliminated."[99]

---

[95] 12 C.F.R. § 1033.421(a)(1).

[96] *Id.* § 1033.421(a)(2)(ii).

[97] Under the California Privacy Rights Act, a California resident can, with proper notice, opt out if they dislike a particular use, or opt in if they find it valuable; the law centers the decision with the consumer, *not* with the uninvolved regulator. *See* Cal. Civ. Code § 1798.120(a)(1). Virginia and Colorado also allow additional uses of data subject to consumer choice. *See* Va. Code Ann. § 59.1-577(A)(5) (2023); Colo. Rev. Stat. § 6-1-1306(1)(a)(IV)(B).

[98] Under GDPR, in contrast to the PFDR Rule, data may be used for additional purposes so long as the entity using the data has a lawful basis, often consent. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, arts. 6(1)(a), 7(3), 2016 O.J. (L 119) 1, 36–37.

[99] Reducing Anti-Competitive Regulatory Barriers, Exec. Order No. 14,267, § 1, 90 Fed. Reg. 15,629, 15,629 (Apr. 9, 2025); *see id.* (noting that "some regulations operate to exclude new market entrants" and

Retaining the PFDR Rule's data use restrictions would also risk further entrenching incumbent data providers. These restrictions apply only to authorized third parties and not to data providers, meaning a third party may be unable to use their own consumers' data for new product development—regardless of what their consumers authorize—but an incumbent data provider could use that same data to develop its own new products. These uneven and extra-jurisdictional use restrictions risk leaving emerging technology companies far behind the regulatorily-advantaged, entrenched incumbents. It is critical that the privacy protections in any updated PFDR Rule foster not only consumer protection, but also the choice, competition, and innovation underpinning the purpose of Section 1033 and the CFPA itself. Plaid thus respectfully recommends that the CFPB strike all references and provisions relating to the use of data, primarily found in the PFDR Rule at 12 C.F.R. § 1033.421(a)–(c).

To be very clear, this is not to say that privacy controls related to data use are not important; ***they absolutely are***. But they already exist. The Section 1033 access right exists within a broader framework of federal and state laws and regulations that prescribe how data can be used, both by data providers and authorized third parties. GLBA is just one example, among many, of such laws.[100] Moreover, if the Administration believes current laws are inadequate, then it could consider supporting efforts to modernize the GLBA or working with Congress on a new, broadly applicable privacy statute, an effort Plaid encourages. Plaid supports clear, consistent, and modern privacy regulation across financial and consumer services. Such an approach would minimize consumer confusion without sacrificing consumer choice, competition, and innovation, as the PFDR Rule does.

30. Does the PFDR Rule provide adequate protection of consumer privacy? Why or why not?

The authorization provisions of the PFDR Rule provide adequate protection of consumer privacy by requiring explicit, revocable consumer authorization, thus ensuring that third parties accessing an individual's financial data are doing so on that person's behalf. Rightfully, the CFPB expressed concern in its ANPR commentary that "there is certain information that few individuals may not want revealed to everyone and anyone, sometimes even those closest to them."[101] This is exactly why the authorization provisions within the PFDR Rule are critical; through such provisions, the Rule ensures that only representatives acting on behalf of an individual (i.e., authorized third parties)—not "everyone and anyone"—are accessing the consumer's data. With these controls in place, as the CFPB notes, "the consumer is able to better calibrate the level of privacy they maintain."[102] Plaid's recommendations regarding authorization are summarized here:

"[f]ederal regulations should not predetermine economic winners and losers").

[100] *See, e.g.*, 15 U.S.C. § 1681b(a) (FCRA strictly limits conditions under which consumer reporting agencies can furnish consumer reports); *id.* § 6502(a) (Children's Online Privacy Protection Act); Tex. Bus. & Com. Code Ann. § 541.101(a)–(b) (Texas Data Privacy and Security Act).

[101] Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40,986, 40,988 (Aug. 22, 2025) (advance notice of proposed rulemaking).

[102] *Id.* at 40,989.

- The CFPB should retain a non-prescriptive requirement that third-party representatives provide transparent, comprehensible, and readily accessible disclosures regarding data access to consumers. The disclosures should broadly ensure that the individual has information regarding (i) to whom they are granting access, (ii) what data is being accessed and shared, and (iii) for what purposes.

- The CFPB should similarly retain a requirement that third parties provide a revocation mechanism so consumers can revoke their prior authorizations.

- While the PFDR Rule appropriately requires third parties to obtain authorization to access consumer data, it improperly moves beyond Section 1033's jurisdictional scope by imposing an impermissibly strict "reasonably necessary" privacy standard and implied categorical prohibitions on data use. Accordingly, the CFPB should strike all references and provisions relating to the use of data, primarily found within 12 C.F.R. § 1033.421(a)–(c).

> ***31. How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions, where customers either have the right to opt into or opt out of having their data licensed or sold? What is the approximate balance between such regimes where the customer is given a choice?***
>
> ***32. How prevalent is the licensure or sale of consumer financial data by bank and non-bank financial institutions where consent to license or sale is part of a standard user agreement or privacy notice?***

Plaid answers Questions 31 and 32 together. In its ANPR, the CFPB notes that "[f]inancial institutions collect, use, and disclose data in many ways that impact consumer privacy. One major privacy threat is when customers are unaware of ongoing licensure or sale of their data."[103] While Plaid is not positioned to offer an in-depth assessment of financial institutions' data practices, we agree with the CFPB's concern about consumers being unaware of the licensure or sale of their data. Plaid also observes that the current PFDR Rule does not impose (or purport to impose) any restrictions on data provider financial institutions' use, licensing, selling, or sharing of consumer data. To the extent the CFPB remains concerned that financial institutions are engaged in licensure or sale of data without consumers' knowledge, no provision within the present Rule will address such concern.

> ***33. What is the prevalence of licensure or sale of consumer data by companies with a fiduciary duty to their clients?***

Fiduciary duties apply in narrow circumstances and generally address "best-interest" advice and conflicts of interest, not data licensure and sale. The more relevant safeguard is consumer disclosure and authorization. Explicit authorization, clear disclosures, and strong revocation rights supply practical protections regardless of whether a company is a fiduciary. That is the model Section 1033 establishes, and it is the one that best aligns with consumer expectations.

[103] *Id.*

* * * * *

In closing, we thank you again for allowing us the opportunity to comment on the ANPR as the CFPB considers rules to protect the right of American consumers to access and share their data with the authorized third parties they rely on. We appreciate the consideration given to our comments, and look forward to further opportunities to participate in this process.

Respectfully Submitted,

/s/ Danielle Aviles Krueger

Danielle Aviles Krueger
Head of Policy, Plaid