October 21, 2025

Via email to 2025-ANPR-PersonalFinancialDataRights@cfpb.gov

Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, D.C. 20552

Re: Stripe, Inc. comments on the Advance Notice of Proposed Rulemaking under section 1033 of the Dodd-Frank Act (Docket No. CFPB– 2025–0037)

To Whom It May Concern:

Stripe, Inc. appreciates the opportunity to comment on the Advance Notice of Proposed Rulemaking (ANPR) that the Consumer Financial Protection Bureau (CFPB) published as part of its efforts to revise rules implementing Section 1033 of the Dodd-Frank Act (Section 1033). As we enter into a new rulemaking process, Stripe is optimistic about this opportunity to resolve longstanding debates about how to structure the open banking ecosystem, and looks forward to collaborating on a framework that promotes innovation and strengthens American competitiveness.[1]

In submitting these comments, Stripe recognizes that the CFPB is in the unenviable position of deciding how to revise a final rule amidst strong disagreements about its key provisions, such as who may serve as a representative on behalf of consumers requesting data; assessment of fees for data access requests pursuant to the rule; and data security and data privacy concerns associated with such data access requests. Each of these topics is critical to the continued development of data access infrastructure, with far-reaching impacts on American consumers and innovation. And each of these topics has been hotly contested for many years. However, we now must recognize that many of the arguments asserted in these policy debates are in fact poison pills meant to undermine the objectives of consumer-permissioned data access:

[1] On August 29, 2025, Stripe submitted comments to raise urgent concerns regarding burdensome fees that banks are planning to charge for consumers' access to their own data through data aggregators. Stripe, Inc., Comment Letter on Advance Notice of Proposed Rulemaking under section 1033 of the Dodd Frank Act, 90 Fed. Reg. 40986 (Aug. 29, 2025), https://www.regulations.gov/comment/CFPB-2025-0037-0012. Today we are submitting a second comment letter to provide additional information and views to assist the CFPB in its revisions to the Section 1033 rule.

competition and innovation for the benefit of consumers.

In recent months, large banks have pressured the CFPB to change their positions on complex issues in the final rule that had been the subject of debate and public comment for a decade. After banks sued the CFPB in an attempt to set aside the final rule,[2] they demanded (or signaled their intent to demand) anti-competitive fees that will alter the competitive landscape and restrict consumers' ability to direct their data in today's data-driven environment. If banks are permitted to appoint themselves as consumer data gatekeepers—a contradiction to Section 1033's intent to empower consumers to control access to their own data—the United States (U.S.) data access ecosystem and its potential for innovations will inevitably fall behind our global counterparts.

For more than two decades, American consumer financial innovation has been pushed forward by nonbank financial technology companies, or fintechs, reliant on the consumer's ability to link their accounts to access financial account data at no cost. Today roughly 8 in 10 Americans use at least one fintech app or service to manage their money.[3] Many of these services are now ubiquitous and essential to modern financial services, including family budgeting, peer-to-peer payments, pay-by-bank, automated utility bill payments, automated savings, earned wage access, buy-now-pay-later, crypto wallets, and many more. These advancements are nothing short of a financial services revolution that empowered consumers through innovative online tools; however, none of these technological innovations would have materialized if banks had levied protectionist fees that limited consumers' ability to direct their own data to third-party services.

Now we are at another inflection point in the innovation of financial technology services.[4] In

---

[2] *See* Press Release, BPI, Banks Challenge CFPB Rule Jeopardizing Security and Privacy of Consumer Financial Data (Oct. 22, 2024), https://bpi.com/document-type/press/ (search press releases by date).

[3] *See* Press Release, Financial Technology Association, Four Takeaways on the State of Fintech from The Harris Poll (Feb. 10, 2023), https://www.ftassociation.org/four-takeaways-on-the-state-of-fintech-from-the-harris-poll/#:~:text=%231%20Fintech%20is%20the%20new,apps%20per%20used%20rose%20overall.

[4] In August 2025, the Financial Technology Association (FTA) released a public letter from over 80 business leaders calling on the Administration to oppose data access fees that would prevent consumers from connecting their bank accounts to better financial products of their choice. Notably, business leaders urged the Administration to prevent such fees from stifling America's ability to lead in the responsible development of digital assets, artificial intelligence (AI), and payments. These are national priorities for innovation and global competition—and valued products among American consumers. Press Release, FTA, Over 80 CEOs Urge President Trump to Oppose Exorbitant Consumer Data Access Fees (Aug. 14, 2025), https://www.ftassociation.org/news-resources/press-releases/ (search press releases by date).

recent months, AI companies have begun to launch "agentic commerce" services, creating new online storefronts where consumers use AI chat functions to receive product recommendations and make purchases through the AI platform. This emerging approach to online shopping will eventually enable AI agents to search for and purchase products on a consumer's behalf. Yet, widespread availability and adoption of agentic commerce features hinges on AI agents being able to access account data to facilitate transactions as consumer representatives. If consumers are unable to appoint representatives to act on their behalf, or we lack a coherent regulatory framework for determining how consumers can authorize such agents, we will fail to realize the consumer benefits that AI and agentic commerce can bring.

Similarly, the CFPB's approach to consumer data access rights will have profound impacts on whether stablecoins can fulfill their promise for reducing frictions in the payment system. Stripe is among the many industry stakeholders that believe stablecoins will enable faster, easier, and cheaper borderless money transfers. U.S.-based companies will be able to pay global vendors in stablecoins, and the funds arrive almost instantly—without wire fees or the need for currency conversion. Small businesses will transact digitally in stable-value currency without needing point-of-sale (POS) infrastructure. But none of these revolutionary benefits of technological innovation will materialize if banks are permitted to levy fees that warp the economics of innovation, preventing consumers from easily moving their funds from a bank account to a stablecoin-based wallet offered by a competing fintech provider.

These are significant shifts in the payments ecosystem that will drive further innovation in financial services, unless they are asphyxiated by fees and other anti-competitive restrictions imposed by incumbents. Specifically, data access fees will increase the cost of data transfers and pay-by-bank to make them less viable without any countervailing benefit to consumers. As it is, banks already make significant profits from credit and debit card payments; additional fees would further inflate bank profits without providing any corresponding benefit to consumers.[5] Moreover, as discussed below, restrictions on the use of certain account information in the name of fraud prevention actually increases fraud risk while creating significant friction for competing payments service providers.

Banks assert these fees are justified for cost recovery. However, as a developer of Application

[5] Interchange fees are transaction fees charged between banks for processing credit and debit card payments. When a customer makes a purchase using a card, the business's acquiring bank pays the interchange fee to the cardholder's issuing bank. Card networks set interchange fees, which are typically a percentage of the transaction amount plus a fixed fee.

Programming Interfaces (APIs), Stripe understands that the total fees will significantly exceed the actual costs associated with infrastructure maintenance. Banks established data access via APIs for their own strategic and business reasons, and they undoubtedly recovered those costs through account fees and other charges. As described in further detail below, banks have no basis for charging additional fees for data access today—such transactions do not require any material increase in their infrastructure costs—and banks should not be permitted to recoup those purported costs in perpetuity. The final rule should prohibit data access fees to prevent anti-competitive profiteering at the expense of consumers, competition, and innovation.

In that context, Stripe urges the CFPB to revise the final rule to preserve a data access infrastructure that benefits consumers through innovation and competition. Following a brief overview of open banking in the U.S. (Part A), this comment encourages the CFPB to consider the following key issues:

- Section 1033 clearly authorizes representatives to obtain data on behalf of consumers, and there is no basis for imposing vague and onerous fiduciary requirements. Simply put, the statute clearly provides that authorized third parties may access account information on behalf of consumers, and neither the statute nor the final rule mandates a fiduciary relationship for representatives to access account data at a consumer's direction. If Congress had intended to require fiduciary duties, it would have done so expressly. Any claims that such a requirement exists are a clear attempt to disrupt the established data access framework. (Part B)

- The CFPB should prohibit data providers from unlawfully charging data access fees, even while it finalizes its revisions to the rule. Stripe urges the CFPB to prohibit data access fees, as these would inherently obstruct consumers' right to access their data "upon request" under Section 1033. Banks, by seeking to impose such fees, would leverage their significant market power to disrupt established practices for consumer data access that have evolved naturally over decades. Had Congress intended a cost-sharing framework for consumer data access under Section 1033, it would have explicitly granted such authority in the law. Furthermore, as a leading developer of APIs, Stripe recognizes that banks and other data providers have little justification for charging any data access fees beyond the one-time costs of establishing data access infrastructure, which many already developed for their own strategic business purposes, independently of this rule. While some fintechs announced they entered into DAAs to maintain their access to consumer

data in a bank's possession, these DAAs do not signify "the market is figuring this out on its own"; rather, they are only short-term lifelines accepted out of necessity. (Part C)

- Third party data recipients and data aggregators should be held to data privacy and data security standards in the Gramm-Leach-Bliley Act (GLBA). Stripe firmly believes that Section 1033 data access should be safer and more secure than riskier data access practices, like screen scraping. Accordingly, all participants in the data access chain, including authorized third parties, data aggregators, and banks, should adhere to the requirements in the Gramm-Leach-Bliley Act (GLBA). DAAs typically require GLBA compliance. These are important data controls that Stripe already implements within its product flows and supporting infrastructure, and other data aggregators should do the same. Moreover, a final rule should require deletion and reauthorization processes to ensure that data is only retained for as long as necessary and only for the service the consumer selected. With those protections, data use should be permitted for certain secondary purposes with a consumer's informed consent. (Part D)

- The CFPB should not endorse tokenization or other practices that mask account data for account and routing numbers. Stripe has significant concerns about the potential negative impacts that the use of Tokenized Account Numbers (TANs) instead of Primary Account Numbers (PANs) could have on consumer choice, fraud prevention, and competition. Stripe's internal analysis of ACH outcomes demonstrates that TANs lead to transaction failures associated with invalid data from the bank at three times the rate for institutions using TANs than PANs offered by the same institutions, and more than twenty-five times the rate of PANs from non-TAN institutions. In addition to their unreliability, TANs also fail to achieve their stated goal of reducing fraud. Based on Stripe's internal ACH processing data, ACH failures that could be associated with fraud occur at more than two times the rate for TANs as compared to PANs from other institutions that do not issue TANs. Without stable account numbers to identify bad actors over time TANs will make it more difficult for payment service providers to detect fraud and mitigate risk in the ecosystem. (Part E)

- The CFPB should maintain the final rule's compliance timelines. Stripe urges the CFPB to uphold current compliance deadlines to prevent the largest banks (holding at least $250 billion in total assets) from charging data access fees that would undermine consumer data access rights under Section 1033. The largest banks have long known that

the requirements were coming and, in most instances, are already compliant through their existing API direct connections. Therefore, the largest banks will not benefit from extensions to the compliance timelines. Conversely, small businesses that depend on data access will suffer great hardship if they are forced to pay data access fees to maintain their operations. Rather than allowing fees to take hold, Stripe urges the CFPB to uphold the existing compliance deadlines for the largest banks, thereby prohibiting data access fees. (Part F)

These are key issues that require measures to ensure the continued development of modern payments and financial management infrastructure. American consumers must retain the freedom to direct their data under the rights granted by Section 1033.

A. Access to consumer account data has been a driving force behind innovation in financial services for decades.

Since the 1990s, modern payments and other online financial services have empowered consumers through innovation driven by access to account data.[6] These industries developed over a period of years—starting more than a decade before Congress adopted Section 1033—and continue to develop today. In particular, fintech companies consistently launched innovative new software applications to make consumers' lives more convenient and to empower them to command their financial decisions. These applications are made possible through the transfer of account data, at the direction of consumers, from their financial institutions to third-party service providers.

As the industry first emerged, third party service providers powered their applications with data obtained from consumer account data through "screen scraping."[7] While screen scraping is effective, it is undesirable because the bank providing data is unable to determine whether the party logging into the account is the accountholder, an accountholder representative, or a fraudster. Moreover, screen scraping can be slow and inefficient, which results in the

[6] *See* Julian Alcazar & Fumiko Hayashi, *Data Aggregators: The Connective Tissue for Open Banking*, Payments System, Fed. Rrv.. Bank of Kansas City (Aug. 24, 2022), https://www.kansascityfed.org/documents/9012/PaymentsSystemResearchBriefing22AlcazarHayashi0824.pdf.

[7] *Id.* at 1. Screen scraping is where a consumer authorizes a third party services provider to log into their bank account on their behalf to obtain data, often using data aggregators to collect and share the data with the third party services provider. *Id.*

deployment of obsolete data.[8] In light of these risks, screen scraping has been replaced over time with programmatic interfaces made between data aggregators and data providers through data access agreements (DAAs) that govern the process, means, and security for such data transfers.

Although terms are often imbalanced toward data providers' interests, the DAAs have been a step in the right direction for innovation in a safer and more intentional way. Specifically, banks and other data providers agreed to provide no-cost, direct access via APIs for secure and efficient exchange of data based on a defined set of standards.[9] The APIs allow consumers to direct banks to share their account data with third party services without also sharing their account credentials, and permit them to control the types, amounts, and frequency of data collected from their consumers' accounts.[10] API standards have been developed over years by industry-led technical standards bodies (*e.g.* Financial Data Exchange, or FDX) to establish a common, interoperable technical standard for the secure and convenient access of permissioned consumer and business financial data. Standardized APIs have fueled the growth of data-based services that are, in part, enabled by data aggregators that serve as a single point of connection between thousands of third party services and thousands of banks and other financial institutions.

API data access has grown exponentially in recent years. Today, more than 114 million consumers connect their accounts via APIs that align with the FDX standard.[11] Indeed, API connections have delivered an incredible number of high-value services for consumers. These services include sophisticated personal financial management tools for budgeting, tailoring financial advice for reducing debts, and long-term financial planning for investments and

---

[8] *Id.*

[9] APIs are a set of rules and protocols for building and interacting with software applications. APIs define the methods and data formats that software components use to communicate with each other. They serve as a type of contract between different software components, stipulating how those components interact. Not only do APIs allow different software systems to communicate with each other, but programmers can use them to access the functionality of other software components. For more information, visit https://stripe.com/resources/more/payment-application-program-interfaces-apis.

[10] Alcazar & Hayashi, *supra* note 8, at 1.

[11] Press Release, Financial Data Exchange, 114 Million Reasons to Keep Moving Forward on Industry-Led Standard for Secure Data Sharing (Apr. 25, 2025), https://www.financialdataexchange.org/FDX/FDX/News/FDX-News.aspx?hkey=018fdd8f-d23e-407c-8732-810ca910f57c (search press releases by date). *See also* J.P. Morgan & WIRED Consulting, *Where Open Banking Goes Next*,Payments Unbound (2025), https://www.jpmorgan.com/payments/payments-unbound/magazine/articles/open-banking-internet-of-money ("One forecast predicts that, by 2029, there will be 645 million total open banking users, up from 183 million in 2025.")

retirement. APIs give access to account data that enhances consumers' application process and potentially improves their access to credit; both bank and nonbank lenders can access consumer data via APIs to make the application process more convenient, efficient, and accurate.[12] Moreover, through data obtained by API access, consumers can more easily utilize ACH payment methods that benefit merchants (especially small businesses and emerging fintechs) because ACH payments are less expensive to accept than credit and debt card payments; those lower rates mean that merchants are not forced to pass those costs on to consumers and in many cases have offered discounts directly to consumers if they pay using their bank account rather than by credit or debit card.

Banks and other data providers entered into DAAs for data access through their APIs to satisfy consumer demand for innovative services. But some banks, apparently concerned about rising competition from the fintech sector, including stablecoin and pay-by-bank, are now attempting to insulate their legacy products from competition.[13] These competitive tensions originate from the threat that lower-costs payment methods pose to bank-issued credit cards (which carry an interchange rate that banks charge merchants, and which they must pass on to consumers). These competitive tensions are natural, given the rapid advancements in technology and services. But the purpose of Section 1033 was precisely to prevent incumbents from using control over access to consumer data to keep consumers locked in their own ecosystem by making it harder to use competing products and services.

Indeed, banks hold tremendous leverage in their DAA negotiations with data aggregators that third parties utilize to access data as directed by consumers. Most notably, banks leverage their possession of consumers' data to insert imbalanced terms in the contract, for example, banks retain the ability to implement and increase fees at their discretion. DAA terms even permit banks to arbitrarily degrade API performance leaving third parties without any viable alternatives for data access.

As a consequence, without clear guardrails in a revised Section 1033 rule, incumbent financial institutions will continue leveraging their positions in negotiations, putting their own competitive interests ahead of consumer preference and undermining merit-based competition.

---

[12] Alcazar & Hayashi, *supra* note 8, at 3-4.

[13] *See* Hugh Son, *Jamie Dimon Says JPMorgan Chase Should Absolutely Be "Scared S---less" About Fintech Threat*, CNBC (Jan. 15, 2021), https://www.cnbc.com/2021/01/15/jamie-dimon-says-jpmorgan-chase-should-absolutely-be-scared-s-less-about-fintech-threat.html.

In addition, banks can prioritize their own products and data connections without any fear of repercussions, for example, by providing stale or incomplete data in response to a data call, responding slowly to data calls in comparison to their own consumer interfaces, limiting the volume of data calls permitted, and, of course, charging fees (and increasing those fees over time) to undermine fintech innovators who would compete with them.

A CFPB rule is essential to protect our data access infrastructure from such anti-competitive incentives. Section 1033 clearly reflects Congress's intent to empower consumers by giving them control over their financial data so they can exercise choice when shopping for financial products rather than being trapped in a single bank's ecosystem. These data, which are a byproduct of bank services, and not the property of banks, enable consumers to seek out better, cheaper, and more innovative financial services that may not be available at their bank. Therefore, a final rule is crucial to protect the data access infrastructure from anti-competitive efforts that would hamper innovation, instead of harnessing its full potential as intended.

B. Section 1033 clearly authorizes representatives to obtain data on behalf of consumers, and there is no basis for imposing vague and onerous fiduciary requirements.

Section 1033 clearly allows consumers to share their data with authorized representatives, and does not contain any indication that those representatives should be subject to onerous fiduciary obligations that go beyond the consumer protections reflected in the current rule. Representatives must be properly authorized by the consumer, and must implement data privacy and security measures as required under existing law for those who come into possession of consumer financial account information. The current rule's requirements ensure that authorized third-party representatives will act on behalf of consumers. However, neither the statute nor the current rule mandates a fiduciary relationship for representatives to access account data at a consumer's direction.

Section 1033's requirements for data sharing only make sense if the data will be obtained and used by a third-party, and not merely for providing consumers visibility into the account data in the bank's file. Specifically, the statute says that the CFPB "shall 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 consumers under this section."[14]

[14] 12 U.S.C. § 5533(d) (emphasis added).

Congress chose the terms "standardized formats" and "machine readable files" over other potential terms (such as "electronic format" or "human readable") to enable data ingestion by third-party software providers.

Moreover, Congress adopted Section 1033 with full knowledge of the data access infrastructure developing around it. As noted earlier in this comment (Part A), the fintech marketplace has relied on consumers' ability to use third parties to connect their bank account to applications and services since the 1990s. Therefore, arguments that the law merely intends to ensure that consumers can receive a spreadsheet with their account data simply do not match the statutory language and clear intent. As a practical matter, Section 1033 must be interpreted to guarantee consumer-directed data sharing with representatives, or else the statute would become meaningless.

There is also no basis for imputing a general requirement that third-party representatives be fiduciaries, subject to vague obligations not clearly stated in the statute or the final rule. If Congress had intended to require fiduciary duties, it would have done so expressly. In fact, we need look no further than the Dodd-Frank Act to see how Congress might have qualified the term "representative" to assign a fiduciary duty of care. The Act uses the phrase "legal representative" to mean fiduciary-type relationships.[15] Congress's choice to use "representative" (and not "legal representative" or some other qualifying term) can only mean that we should apply its common meaning, which is a "person who stands for or acts on behalf of another."[16] In addition, Congress could have removed the guesswork by specifying that authorized third parties (and data aggregators acting at the direction of consumers) must be either "agents" or "trustees," thereby rendering the term "representative" irrelevant. Nevertheless, Congress chose not to make that distinction, and therefore the term "representative" in Section 1033 should be

[15] *See, e.g.*, 15 U.S.C. § 80b-11(g)(2) (defining "retail customer" to include a "natural person, or the legal representative of such natural person").

[16] *See, e.g.*, *Representative*, Black's Law Dictionary (11th ed. 2019); *Representative*, Oxford Advanced Learner's Dictionary, https://www.oxfordlearnersdictionaries.com/definition/english/representative (last visited Oct. 21, 2025) ("a person who has been chosen to speak or vote for somebody else or for a group of people"); *Representative*, Merriam-Webster's Collegiate Dictionary (11th ed. 2022) ("one that represents another or others"); *Representative*, The American Heritage Dictionary of the English Language (5th ed. 2022) ("[o]ne that serves as a delegate or agent for another"); *Representative*, Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/representative (last visited Oct. 21, 2025) ("someone who speaks or does something officially for another person or group of people"); *Representative*, Collins English Dictionary, https://www.collinsdictionary.com/us/dictionary/english/representative (last visited Oct. 21, 2025) ("a person who has been chosen to act or make decisions on behalf of another person or a group of people").

read in accordance with its ordinary meaning, without importing additional fiduciary requirements.

The meaning of the term "representative" is simpler than banks would have you believe. Section 1033 plainly mandates that banks "shall make available to a consumer, upon request, information in the control or possession" of the bank. 12 U.S.C. § 5533(a). The Dodd-Frank Act defines a "consumer" as "an individual or an agent, trustee, *or representative* acting on behalf of individuals." 12 U.S.C. § 5481(4) (emphasis added). Banks argue that a representative must be a fiduciary of the consumer; however, that condition does not exist in the statute—or anywhere else in Federal law. On the contrary, Federal law even recognizes that "agent" (which could be read to imply a higher level of duty than a "representative") does not inherently carry a fiduciary relationship. 26 C.F.R. § 301.7701-6(b)(2) (There may be a fiduciary relationship between an agent and a principal, but the word agent does not denote a fiduciary.).

Large banks did not argue during the initial rulemaking period that the law requires representatives to be fiduciaries. This argument became central to their opposition to Section 1033 only when the Bank Policy Institute (BPI) sued the CFPB to block the recently-finalized rule. In that context, it seems that large banks do not genuinely view a fiduciary duty as critical to open banking relationships, which explains the absence of fiduciary requirements (to Stripe's knowledge) in the data access agreements negotiated between banks and data aggregators over the past decade. The argument that representatives must adhere to fiduciary duties beyond common industry practice (and what had been settled in the final rule) is a manufactured litigation tactic designed to undermine the rule in spite of the law's clear language and decades of industry practice.

Interpreting Section 1033 to mean that representatives must meet a vague fiduciary duty of care, in addition to the clear obligations already contained in the final rule, would impose impractical and unnecessary burdens on the marketplace. While we oppose a heightened duty of care for representatives, Stripe agrees that proper authorization measures are crucial for access to a consumer's data. As written, the final rule permits consumer data access by authorized third parties but only if they "[o]btain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing." 12 C.F.R § 1033.401. Section 1033.411 details the authorization disclosure and its content, requiring third parties to provide an authorization disclosure to consumers that includes: information about the authorized third party, the identity

of the bank that controls or processes the covered data, a description of the product or service that the consumer has requested from the authorized third party, a list of the categories of data that will be accessed and the duration of the data collection with a limit of one year after the consumer's most recent authorization, and a description of the process for revocation of such authorization.

Stripe's data aggregation product, called Financial Connections, goes to great lengths to ensure proper authorization of bank account connections. We work directly with financial institutions as well as via partner aggregators to ensure that consumers and businesses who want to connect their bank account are able to do so securely. All merchants and businesses who look to use Financial Connections data go through a rigorous onboarding process. Every time a consumer connects a new bank account, we collect their consent, clearly describe what data will be shared and with which parties, and how the user can disconnect their data. Stripe also has robust controls for disconnecting linked accounts. Consumers can follow a simple disconnection process that allows them to instantly disconnect their bank account, or submit a manual request to revoke a third party's access to their connected bank account data. We provide granular controls for the consumer to disconnect specific accounts or specific businesses, if desired.

In short, consumers retain control over Stripe's access to data, and the terms of authorization and requirements of the current rule ensure that third parties like Stripe act in the interest of consumers when accessing, using, or retaining their data. Notably, the final rule already requires that "third parties accessing covered data pursuant to the final rule's framework to adhere to the authorization procedures and third party obligations in subpart D … [which] ensure that third parties accessing a consumer's covered data are *acting on the consumer's behalf*.[17]

Looking forward, consumers will rely on digital agents to manage large portions of their financial lives by engaging in commerce on their behalf, making automated payments, and enabling other capabilities that we have not yet conceived. A generalized fiduciary duty of care goes beyond what the law authorizes and would disrupt the current approach to data access that has been formed by decades of market practice and anticipation of a CFPB rule informed by principles articulated by the CFPB that would ensure representatives act on behalf of consumers.

[17] Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838, 90921 (Nov. 18, 2024) (emphasis added).

Instead, Stripe encourages the CFPB to consider an alternate future, where fintechs engage with banks in partnerships and free market competition to build "best in class" financial products, rather than trapping consumers within their primary bank's ecosystem. For inspiration, we need look no further than J.P. Morgan Chase, which recently published the following:

> This kind of data sharing can enable valued-adding services. Account aggregation services, for instance, allow consumers to view and manage multiple financial accounts from different institutions in a single interface. "Open banking is about giving people control over their financial data," says Helen Child, CEO of Open Banking Excellence. "It democratizes banking information, and ultimately helps you manage your money better."[18]

This version of the future is only achievable if we continue to build on today's approach to enabling consumer-directed account data access. Account connectivity is the only way to enable the delivery of diverse and innovative products from competing providers to consumers.

C. <u>The CFPB should prohibit data providers from unlawfully charging access fees, even while it finalizes its revisions to the rule.</u>

As detailed in our comment letter dated August 29, 2025,[19] Stripe encourages the CFPB to safeguard existing data access infrastructure from fees that inherently interfere with consumers' ability to access their data "upon request," a right guaranteed under Section 1033. Section 1033 reinforces existing data access practices by establishing that consumers, not financial institutions, own and control access to their financial data. By imposing fees, banks are seeking to exploit their outsized market influence to disrupt settled market-driven practices around consumer data access that developed organically over decades. In order to protect the market from such anti-competitive efforts, Stripe recommends that the CFPB take immediate measures to prevent data providers from imposing access fees.

The CFPB has clear authority to prevent data providers from imposing data access fees. Section 1033, entitled "Consumer rights to access information," requires covered persons to "make available to a consumer, *upon request*, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person[.]" 12 U.S.C. § 5533(a) (emphasis added). Under the existing final rule, data

[18] J.P. Morgan & WIRED Consulting, *supra* note 12.
[19] *See supra* note 1, at 1, 3.

providers are barred from imposing any fees or charges on a consumer or their authorized third party for accessing data through its data interface. *See* 12 C.F.R. §§ 1033.301(c); 1033.301(c)(1)–(2). The law necessitates a prohibition on such fees to ensure that consumers can freely exercise the ability to access their own data *upon request*. If banks are permitted to charge fees for such access, then data access would only be available *upon payment*. Further, the CFPB has the statutory authority to promulgate rules to "prevent evasions" of consumer finance protection laws like Section 1033's right of access to information. 12 U.S.C. § 5512(b)(1). And a prohibition on fees is necessary to ensure that data providers do not evade a consumer's right to access their own information by imposing onerous and unlawful fees.

Contextually, Section 1033 already includes provisions meant to reduce compliance burdens on banks, without any mention of cost recovery. Section 1033 states that banks need not make available "any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information." *Id.* § 5533(b)(4). Furthermore, the Act does not "impose any duty on a covered person to maintain or keep any information about a consumer." *Id.* § 5533(c). The consumer's right to access is thus restricted to information that the data provider should have readily available, and the statute does not impose any obligation on the provider to maintain that information beyond its ordinary business uses, minimizing any financial burden on the provider and mitigating any need to recoup fees for the costs of locating, producing, or storing that information.

Courts have also recognized an interpretive principle that consumer protection statutes should be broadly construed in favor of consumers.[20] The Dodd-Frank Act, and the right to access provision in particular, is indisputably a consumer protection statute. *Hong v. SEC*, 41 F.4th 83, 88 (2d Cir. 2022) ("Through the Dodd-Frank Wall Street Reform and Consumer Protection Act,

[20] *See, e.g.*, *Avila v. Riexinger & Assocs., LLC*, 817 F.3d 72, 75 (2d Cir. 2016) ("[B]ecause the [Fair Debt Collection Practices Act (FDCPA)] is 'primarily a consumer protection statute,' we must construe its terms 'in liberal fashion [to achieve] the underlying Congressional purpose.'") (citation omitted); *Begala v. PNC Bank, Ohio, Nat. Ass'n*, 163 F.3d 948, 950 (6th Cir. 1998) ("We have repeatedly stated that [the Truth in Lending Act] is a remedial statute and, therefore, should be given a broad, liberal construction in favor of the consumer."); *Segrist v. Bank of New York Mellon*, 744 F. App'x 932, 935 (6th Cir. 2018) (same); *Moran v. Screening Pros, LLC*, 943 F.3d 1175, 1186 (9th Cir. 2019) ("'[The statute's] consumer oriented objectives support a liberal construction of the [Fair Credit Reporting Act].'" (first alteration in original)); *Johnson v. Riddle*, 305 F.3d 1107, 1117 (10th Cir. 2002) ("Because the FDCPA, like the Truth in Lending Act (TILA), is a remedial statute, it should be construed liberally in favor of the consumer."); *Carmichael v. Nissan Motor Acceptance Corp.*, 291 F.3d 1278, 1280 (11th Cir. 2002) ("Like the TILA, the [Consumer Leasing Act (CLA)] is a consumer protection statute which 'is remedial in nature and therefore must be construed liberally in order to best serve Congress' intent.'"); *Essique v. Walnut Woods Condo. Ass'n*, 2016 WL 7337246, at *2 (E.D. Mich. Dec. 19, 2016) ("And, as with any consumer protection statute, courts interpret the FDCPA liberally to benefit the consumer.").

Congress adopted a range of new whistleblower incentives and protections as well as many other measures aimed at stemming abuses in the financial arena."). Therefore, under this interpretive principle, the CFPB should interpret Section 1033's right of access to personal account information broadly in favor of consumers so as not to impose additional fees on consumers to receive that information.

It is also widely recognized that consumer protection rights must not be conditioned on payment unless specifically authorized by Congress, or else those statutory rights would be available only to those who are able to pay. This would be a truly perverse result, which is why Federal agencies have upheld this principle for decades. For example, in its implementation of the Gramm-Leach-Bliley Act (GLBA), the CFPB noted that financial institutions do not charge customers for delivery of an annual privacy notice by mail because the notice is required by statute and regulation.[21] Regulation E prohibits financial institutions from charging consumers for its error resolution obligations.[22] Regulation Z prohibits financial institutions from imposing a charge related to any aspect of the dispute resolution process, including any costs for documentation or investigation of the consumer's claim.[23] Each of these regulations prohibits fees because their authorizing statutes do not explicitly permit financial institutions to charge consumers for exercising their rights. In contrast, the Fair Credit Reporting Act (FCRA) explicitly permits a consumer reporting agency to "impose a reasonable charge on a consumer" to share certain information with a consumer. 15 U.S.C. § 1681j(f)(1)(A)(i). Accordingly, if Congress had intended to impose a cost-sharing framework for consumer data access under Section 1033, it would have provided that authority in the law.

Given that statutory language and parallel regulations strongly counsel against charging fees for customers to receive their personal account information, the CFPB should not depart from its current position that fees should not be imposed. 12 C.F.R. § 1033.301(c). "When an agency departs from its prior position, the change creates unique 'aspect[s] of the problem' that it must confront." *Kentucky v. EPA*, 123 F.4th 447, 468 (6th Cir. 2024). An agency changing its position from a prior final rule "must at least 'display awareness that it is changing position' and 'show

---

[21] Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach Bliley Act] (Regulation P), 79 Fed.Reg. 64,057, 64,073 (Oct. 28, 2014), https://www.govinfo.gov/content/pkg/FR-2014-10-28/pdf/2014-25299.pdf.
[22] 12 C.F.R. § 1005.11(d)(2)(ii) ("The financial institution may not impose fees for items it is required to honor under § 1005.11.").

[23] *See* 12 C.F.R. § 1026.13(d)(1).

that there are good reasons for the new policy.'" *Encino Motorcars, LLC v. Navarro*, 579 U.S. 211, 221 (2016). "It follows that an '[u]nexplained inconsistency' in agency policy is 'a reason for holding an interpretation to be an arbitrary and capricious change from agency practice.'" *Id.* at 222; *Motor Vehicle Mfrs. Ass'n v. State Farm*, 463 U.S. 29, 42 (1983) ("Accordingly, an agency changing its course by rescinding a rule is obligated to supply a reasoned analysis for the change beyond that which may be required when an agency does not act in the first instance.").

One data aggregator announced it had agreed to pay access fees under its DAA with a large bank, and more fintechs and aggregators may follow. These DAAs could be interpreted as signifying that market participants are figuring this out on their own. However, nothing could be further from the truth. Without a rule to uphold consumer rights under Section 1033, DAAs will merely reflect the inherent power imbalance resulting from incumbent financial institutions gatekeeping consumer data. For example, DAAs with banks typically provide banks with the option to implement fees at any time. These provisions enshrine the incumbents' overwhelming market leverage derived from treating consumer account data as their own proprietary assets that they are seeking to monetize, even though they already charge for the underlying account services. Moreover, if data access fees were to become standard practice across the many thousands of financial institutions in the U.S., consumer data access would grind to a halt.

If data providers are permitted to charge fees, they will surely seek to impose fee structures that do not reflect the actual costs of providing data access. According to one public report, a bank would charge $1.50 for each customer authorization token when consumers initially consent to third-party services.[24] The same bank would implement per-request fees ranging from $0.05 for basic account information, balance checks, and transaction lookups, up to $0.20 for payment-related services like ACH or direct debit initiation, with fees decreasing at higher call volumes.[25] This approach would penalize financial service providers who offer payment-related services, even when such payments are a small part of their offering (such as budgeting or investment tools with limited payment capabilities). Meanwhile, API calls classified as "payments-related" do not inherently cost more to process, whether received from a fintech company or directly from an individual customer. The costs of collecting balance and ownership information are the same regardless of the use case, and balances and ownership information

[24] Jas Shah, *A Taxing Time for Fintech: JPMorgan, Data Tolls, and the Open Banking Value Chain*, Fintech: Under the Hood (Aug. 1, 2025), https://jasshah.substack.com/p/a-taxing-time-for-fintech-jpmorgan (last visited Oct. 21, 2025).

[25] *Id.*

help prevent fraud and failed payments–which will *reduce* the cost to data providers. Attempts to charge more for payments-related data collection therefore appear designed primarily to prevent competition in incumbent banks' core markets.

As a market-leading developer of APIs,[26] Stripe knows there is little basis for banks to charge any fees for data access. First, APIs that satisfy the final rule do not require banks to store or process any additional data beyond what they already require for maintenance of the underlying consumer account. For example, even APIs that return a large amount of data, such as transaction histories, only access a subset of the data (*i.e.* the transactions) that banks already maintain to serve their customers' accounts. Second, banks already have the infrastructure in place to programmatically return the data since that function already exists to power their own websites and mobile applications. In truth, banks incur trivial setup and maintenance costs that can be attributed specifically to providing access to data recipients; any setup costs were incurred while establishing infrastructure. These costs were recovered long ago through account fees, interest charges, and service fees.[27] Finally, costs of maintaining an API are miniscule at economies of scale, and would constitute only a tiny portion of the fees banks would charge for data access. Large providers average $3 per account annually and costs decrease significantly with scale—dropping as low as $0.25 per account per year for the largest institutions.[28] Therefore, imposing additional charges for data access is simply an anticompetitive tax that harms innovation, raises costs for consumers, and contradicts both the text and purpose of Section 1033.[29]

This is consistent with Stripe's experiences with the cost for maintaining APIs. In fact, while Stripe offers its own APIs, it has no plans to charge any fees for recovery of API maintenance costs because those costs are an inconsequential cost that is already factored into the product

[26] Stripe, Stripe Named Leader by Independent Research Firm (May 19, 2022), https://stripe.com/newsroom/news/stripe-wave-2022.

[27] Claims that API maintenance is expensive are speculative at best. According to comments submitted in response to the final rule, "several data providers stated that it was difficult to disaggregate the costs of developer interfaces from their consumer interfaces and other information technology systems." *See* Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838, 90961 (Nov. 18, 2024)."

[28] *Id.*

[29] The Administration has already targeted companies that "impose egregious fees while providing minimal value" to consumers in other contexts. Exec. Order No. 14254, Combating Unfair Practices in the Live Entertainment Market, 90 Fed. Reg. 14699 (Mar. 31, 2025). It has also cracked down on "debanking" in the financial services industry. Exec. Order No. 14331, Guaranteeing Fair Banking for All Americans, 90 Fed. Reg. 38925 (Aug. 7, 2025). The CFPB should craft its rule to block banks from engaging in similar abusive practices here.

costs. Simply put, the projected bank-imposed fees for direct data access via API are out of step with the minimal costs that Stripe incurs to maintain its own APIs.

While the law mandates access to consumer-permissioned data at no cost, the ANPR suggests the CFPB is considering whether banks could charge "reasonable" fees for bank maintenance of the data access framework. An approach that requires any fact-based analysis for each bank's fee demands will inevitably lead to disputes between banks and third parties, and disputes between the CFPB and banks. The fixed costs of maintaining API access will vary across financial institutions. Moreover, some costs stem from their own product decisions; for instance, a bank's implementation of Tokenized Account Numbers (TANs) would generate additional costs for creating and maintaining a new account number while ensuring it is transactable via ACH/RTP. Consequently, permitting institutions to levy fees will incentivise them to develop functionalities that are not essential for the data access right guaranteed by Section 1033. The only clear path forward is to honor the plain language of Section 1033 by requiring that banks give consumers access to their data upon request, without any barriers to access. Nevertheless, if the CFPB chooses to pursue a standard allowing reasonable fees, it should be limited to actual costs that can be clearly demonstrated by the financial institution.

D. Third party data recipients and data aggregators should be held to data privacy and data security standards in the Gramm-Leach-Bliley Act (GLBA).

The ANPR seeks information about the requisite strength of data security measures and the associated costs. In response to that request, Stripe firmly believes that Section 1033 data access should be safer and more secure than riskier data access practices, like screen scraping. Accordingly, all participants in the data access chain, including authorized third parties, data aggregators, and data providers, should adhere to the requirements in the Gramm-Leach-Bliley Act (GLBA). DAAs typically require GLBA compliance. These standards are important because consumers should have confidence that the data they entrust to banks and third parties are fully protected, and that they fully understand how the data will be used. These are important data controls that Stripe already implements within its product flows and supporting infrastructure.

In addition to GLBA compliance, banks and authorized third parties (and their data aggregators) should protect consumer data privacy by limiting data uses to the specific purposes authorized by the consumer and ensuring that consumers can revoke access at any time with immediate effect. Moreover, a final rule should require deletion and reauthorization processes

to ensure that data is only retained for as long as necessary and only for the service the consumer selected.

With those protections, authorized third parties should be permitted to use data for certain secondary purposes with a consumer's informed consent. Any limitation on secondary data use would contradict consumer preference and substantially limit data use for the benefit of consumers. This could essentially freeze market innovation by preventing market participants from using such data to enhance products, keep pace with marketplace innovations, and develop convenient new product features that consumers would enjoy.

In order to strike the right balance, the final rule should clarify that authorized third parties are permitted to collect and use data for other purposes if they obtain the consumer's informed consent to do so, which is consistent with existing privacy standards. Otherwise, limiting data use would place third parties that receive data under Section 1033 at a competitive disadvantage relative to entities receiving data pursuant to the GLBA guardrails, without any justification.

In addition, Stripe believes that aggregated and de-identified data is appropriate for use, especially in the context of model development when the consumer is informed and provides consent. Use of aggregated and de-identified data should be permitted because there are many important pro-consumer use cases, ranging from better fraud prevention to improved financial advice or product offerings, that are made possible by the use of such data.

E. The CFPB should not endorse tokenization or other practices that mask account data for account and routing numbers.

Another important privacy and security issue is whether banks should be permitted to provide authorized third parties with tokenized account numbers (TANs) in lieu of primary account and routing numbers (PANs). PANs are the primary identifier used to facilitate the movement of trillions in bank payment volume each year. While Stripe strongly supports measures to protect consumers' sensitive information, it also has significant concerns about the potential negative impacts that the use of TANs, instead of PANs, have on consumers, fraud prevention, and competition.

Stripe's internal analysis of ACH outcomes demonstrates that TANs are counterproductive. Our data, derived from processing ACH payments and payouts to millions of businesses, indicates that TANs degrade the reliability of ACH payments and correlate with higher rates of fraudulent

or unauthorized transactions. Therefore, TANs fail to achieve their stated goal of reducing unauthorized transactions, and in fact introduce new risk vectors. Specifically:

- TANs lead to transaction failures in the ACH ecosystem when the originating bank returns an ACH network failure code, R04, which represents an "invalid account number." In those instances, the TAN issuer fails to recognize the TAN due to the institution's own technical failure, or due to having inactivated the TAN due to expiry or revocation. Stripe observes these R04 errors at **three times** the rate for institutions issuing TANs than PANs issued from the same institutions, and **more than twenty-five times** the rate of PANs from non-TAN institutions.
- ACH payments on TANs are *not* associated with lower rates of unauthorized transactions. In fact, Stripe data show the opposite: ACH returns that could be associated with fraud occur at **two times** the rate for TANs as compared to PANs from other institutions that do not issue TANs.[30]

Stripe recognizes that TANs offer consumers theoretical security benefits, like the ability to revoke a temporary credential if they later believe a data recipient is compromised. But the incremental fraud vectors that TANs open up and their inherent unreliability are too substantial a trade off. To understand why we observe higher fraud rates with TANs than PANs, it is important to understand how TANs make it more difficult for payment service providers to detect fraud. TANs may be issued on a per "application" basis, which means Stripe may receive a unique TAN whenever a consumer links their bank account in a new context. As a consequence, a bank's production of TANs in lieu of PANs makes it difficult for payment service providers to identify unique accounts used to perpetrate fraud across merchants.[31] Similarly, Stripe relies on PANs to detect suspicious activities indicative of financial crimes. As part of its transaction monitoring, Stripe's Financial Crimes and Anti-Money Laundering teams rely on the payment methods we have on record to associate accounts with specific consumers; using that information, Stripe can trace the payment method usage across different transactions. However, when PANs are tokenized (and therefore unable to be linked to a specific consumer across transactions), Stripe loses an important tool used to support anti-financial crimes

[30] Stripe's internal data reflect the elevated rates of ACH network failure codes—specifically, R05 ("unauthorized debit"), R07 ("customer revoked authorization"), R08 ("payment stopped"), and R10 ("originator not known or authorized").

[31] When a single fraudster makes many transactions across many merchants, Stripe would no longer be able to trace the fraudulent transactions to an individual because the TAN would be different each time.

investigations. To avoid these negative outcomes, Stripe suggests that the final rule should prohibit the use of TANs before conducting a separate inquiry to consider the risk that it would introduce to the payment system.

TANs add a significant new fraud vector in the bank-based payments ecosystem, reducing the safety of the system and increasing costs for merchants, processors, and ultimately consumers for transactions on ACH rails. Stripe has observed how using TANs can create an exploitable path for fraudsters. Fraudsters attach and use a new account (to Stripe it appears new because the TAN is new) to make purchases, and then revoke the TAN before the ACH transaction can settle, which causes the payment to fail. As a consequence, the fraudster will receive the purchased goods (which were shipped after the merchant payment is authorized but before settlement), and the business for whom Stripe processed the payment suffers the financial loss (which ultimately results in higher prices for consumers and/or lower competition because merchants will be dissuaded from offering bank-based payments).

Finally, permitting banks to mask the account and routing numbers that consumers direct them to share in favor of sharing only TANs will create an anti-competitive market environment. Permitting banks to issue only TANs gives them broad control over when to deactivate an account number, even if that is not the consumer's intention. Moreover, merchants are less inclined to accept bank payments in light of the increased fraud and risk implications for their business, further driving business to card products that ultimately result in higher costs passed on to the consumer. Without clear guidelines and limitations on the use of TANs, each bank may implement its own proprietary tokenization technology. In that scenario, third parties would only be able to partner with the network provider of the bank's choosing, as only that provider would have the capability to revoke a consumer's TAN. By permitting use of TANs in this manner, Section 1033 could have the unintended consequence of centralizing power in the hands of a few banks.

F. The CFPB should maintain the final rule's compliance timelines.

Stripe urges the CFPB to uphold current compliance deadlines to prevent the largest banks (holding at least $250 billion in total assets) from charging data access fees that would undermine consumer data access rights under Section 1033. The largest banks have long known that the requirements were coming and, in most instances, are already compliant or close to compliant through their existing API direct connections. Therefore, the largest banks will not

benefit from extensions to the compliance timelines. Conversely, small businesses that depend on data access will suffer great hardship if they are forced to pay data access fees to maintain their operations. (Relatedly, if the CFPB proposes to allow data providers to charge access fees, it is clear that small businesses would suffer harm. Accordingly, the CFPB would be required to convene a panel of representatives from impacted small businesses under the Small Business Regulatory Enforcement Fairness Act prior to proposing a new or amended 1033 rule.)

Rather than allowing fees to take hold, Stripe urges the CFPB to uphold the existing compliance deadlines for the largest banks, thereby prohibiting data access fees. Alternatively, if the CFPB is inclined to extend compliance deadlines for certain, other provisions of the rule, it should maintain the compliance date with respect to the prohibition against data access fees as a stand-alone requirement.

Conclusion

Stripe urges the CFPB to revise the final rule to safeguard a data access infrastructure that fosters innovation and competition for the benefit of consumers. American consumers are entitled by law to access and direct their account data for innovative third-party services. While the nation's largest banks would have the CFPB change its positions on complex issues following a decade of debate and public comment, American financial innovation must be protected from anti-competitive measures through basic guardrails that ensure fair competition within the free market.

We appreciate your consideration of our comments and would be happy to provide you with additional information. Please do not hesitate to contact us with any questions.

Respectfully submitted,

Jonah Crane

Head of Global Regulatory &
Policy Development