IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE,

Plaintiffs,

v. Case No. 5:24-cv-00304-DCR

CONSUMER FINANCIAL PROTECTION BUREAU and RUSSELL VOUGHT, in his official capacity,

Defendants.

RENEWED MOTION TO INTERVENE OF THE FINANCIAL TECHNOLOGY ASSOCIATION

Pursuant to Federal Rule of Civil Procedure 24, the Financial Technology Association ("FTA") respectfully renews its motion to intervene as a Defendant in this case. FTA satisfies the standards for intervention as of right under Federal Rule of Civil Procedure 24(a) and, in the alternative, permissive intervention under Federal Rule of Civil Procedure 24(b)(1). As set forth in the attached declaration, FTA's members and American consumers and businesses using their products benefit from the rule and have an interest in defending it. That interest is impaired if the rule is enjoined or otherwise suspended—even temporarily. The recent steps taken by the Consumer Financial Protection Bureau ("CFPB"), including agreeing to toll the compliance deadlines of the rule for 30 days and requesting an additional tolling period of 60 days, make clear that the CFPB cannot adequately represent FTA's interests.

This Court should hear from FTA before ordering any additional tolling or delay in the rule's compliance deadlines. The parties cannot, consistent with the Administrative Procedure Act ("APA"), agree amongst themselves to what is effectively a stay of the existing rule without this Court making certain findings, including that Plaintiffs are likely to succeed on the merits and are suffering irreparable harm in the absence of such relief. *See infra* Part III. In these circumstances, FTA should be permitted to intervene as of right or permissively to defend the rule so that the Court can receive briefing as to whether to issue such a stay.

BACKGROUND

1. FTA champions the transformative role of financial technology for American consumers, businesses, and the economy. *See* Declaration of Penny Lee ¶ 2 ("Lee Decl."). As part of that mission, FTA supports regulation that empowers consumers to access and share their financial data with the applications ("apps") and services they want to use, thus fostering innovation and competition in the financial services market. *Id.* FTA's members are innovators seeking to provide more seamless services, lower-cost products, and greater consumer choice in the financial services market. *Id.* These members leverage internet and mobile technologies to offer consumers access to credit, new payment (including pay by bank) options, and financial advisory services that can significantly reduce costs, accelerate access to funds, and improve transparency and convenience. *Id.*

The provision of these essential services, along with continued digitally native financial technology ("fintech") innovation, relies on consumers' ability to access, unlock, and share their financial data with new and often competitive financial service providers. The ability to control and share financial data empowers consumers with more efficient and convenient ways to manage their finances, and allows consumers to explore tailored, cost-effective financial products and

providers. Additionally, data sharing fosters competition by enabling new entrants to enter the marketplace. This data sharing also aligns with frameworks in other jurisdictions across the globe, such as the UK, Australia, Brazil, and more, that have established a consumer data right and require financial institutions to allow consumers to securely share their data with third parties.

2. In 2010, Congress enacted the Consumer Financial Protection Act (the "Act"). Section 1033 of the Act requires banks to "make available to a consumer, upon request, information in the control or possession of the [bank] concerning the consumer financial product or service that the consumer obtained" from the bank. 12 U.S.C. § 5533(a). The Act further defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." *Id.* § 5481(4). In addition, the Act provides that the Consumer Financial Protection Bureau ("CFPB") "by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information ... to be made available to consumers under this section." *Id.* § 5533(d). The Act also authorizes the CFPB to ensure that "all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive." *Id.* § 5511(a). Finally, the CFPB is generally authorized to prescribe rules "as may be necessary or appropriate to enable [it] to administer and carry out the purposes and objectives of the Federal consumer financial laws, and to prevent evasions thereof." *Id.* § 5512(b)(1).

3. Pursuant to these and other authorities, on October 31, 2023, the CFPB issued a proposed rule to enable consumers to more easily share their personal financial data, subject to certain safeguards. *See* Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Oct. 31, 2023). The CFPB began by explaining that "[d]igitization and decentralization in consumer finance create new possibilities for more seamless consumer switching and greater

competitive intensity." *Id.* at 74,796. The CFPB therefore proposed regulations to specify the "scope of data that third parties can access on a consumer's behalf, the terms on which data are made available, and the mechanics of data access," all while "ensur[ing] that third parties act on consumers' behalf when collecting, using or retaining data." *Id.* at 74,799. As relevant here, the CFPB proposed to require banks to share consumer data with consumers and with third parties through a "developer interface," and proposed regulations to determine whether the performance of such developer interfaces was "commercially reasonable"; authorized standard setting organizations to develop measures of compliance with various provisions of the rules; prohibited banks from collecting access fees from third parties in exchange for providing these services; and proposed compliance deadlines. *See generally id.* at 74,806-43.

FTA submitted a comment in response to the Bureau's proposed rule that "applaud[ed] the Bureau's Proposal" for its support of a robust personal financial data right. *See* Lee Decl., Ex. A ("FTA Comments"), at 1. FTA further stated it "support[ed] the Bureau's proposed incorporation of, and reliance on, a recognized standards setting organization (SSO) that will issue qualified industry standards," because "prescriptive technical requirements issued by the regulator will fail to keep pace with technological change and the development of related best practices." *Id.* at 10. Though FTA urged the CFPB to take additional steps to make data available to third parties and to clarify other aspects of the proposed rule, FTA broadly noted its "support [for] the thoughtful and consumer-centric final implementation of the rule." *Id.* at 1.

Similarly, certain FTA members also participated in the rulemaking and expressed support for the CFPB's aim to provide for greater choice and competition in the marketplace for financial services. Lee Decl. ¶ 7. For example:

- FTA member Plaid Inc. ("Plaid") commented that the CFPB's "rulemaking is critical to consumers fully realizing the consumer empowerment goal that underpins § 1033, and to

achieving a fair, transparent, and competitive financial services marketplace." Lee Decl., Ex. B ("Plaid Comments"), at 2. Plaid further commented that the proposed rule's "emphasis on fair and free consumer and third party access to data providers' developer interfaces, effective and transparent authorization managed by third parties, and the role [SSOs] can play in implementing data access at a technical level will, if finalized, dramatically improve data portability, competition, and consumer outcomes." *Id*.

- FTA member Ribbit Capital commented that it "commend[s] the [CFPB] on its work to date and support[s] this effort to develop a pro-consumer open banking system in the United States." Lee Decl., Ex. C ("Ribbit Capital Comments"), at 1. Ribbit Capital further commented that it "agree[s] with the [CFPB] on the importance and value of consumer financial data and believe[s] it should be used to deliver value back to the consumer by improving financial access, choice and opportunity." *Id.* at 11.

- FTA member Stripe, Inc. ("Stripe") commented that the CFPB's "Section 1033 rule will be an important catalyst for competition by empowering consumers to choose products and services that best meet their financial needs," and "strongly support[ed] the CFPB's swift finalization of the rule." Lee Decl., Ex. D ("Stripe Comments") at 1, 2.

- FTA member Wise commented that "[a]s a supporter of consumer-centric financial services regulation, Wise warmly welcomes the [CFPB's] continuation of the Section 1033 rulemaking process," and "commend[ed] the [CFPB] on its efforts to consider the impact of consumer access to financial records." Lee Decl., Ex. E ("Wise Comments"), at 1, 4. Wise further commented that it "support[ed] the CFPB's proposal to recognize a [SSO] to issue industry standards." *Id.* at 2.

4. On October 22, 2024, the CFPB finalized its rule largely in line with its proposal.[1] *See* Final Rule for the Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90838 (Nov. 18, 2024) ("Final Rule"). The Final Rule sets forth specific compliance deadlines for its provisions to take effect, ranging from April 1, 2026 to April 1, 2030. *See* 89 Fed. Reg. at 90,860, 90,956; 12 C.F.R. § 1033.121(b).

That same day, Plaintiffs filed their complaint challenging the Final Rule, which they subsequently amended on November 18, 2024. The amended complaint alleges that the CFPB exceeded its statutory authority under § 1033 and acted arbitrarily and capriciously with respect to certain portions of the Final Rule, including by adopting an unlawful interpretation of the term

[1] The CFPB finalized a portion of the proposed rule regarding standard setters on June 11, 2024.

"consumer" in Section 1033, unlawfully requiring disclosure of payment initiation information, unlawfully delegating authority to private SSOs, and unlawfully and unreasonably prohibiting banks from charging access fees. *See* ECF No. 22 ("Am. Compl."), ¶¶ 99-172. On December 27, 2024, the CFPB filed its answer to the amended complaint. ECF No. 29.

On January 8, 2025, the CFPB issued an order recognizing Financial Data Exchange, Inc. ("FDX") as a standard setter under the Final Rule. See Decision and Order, *In re Financial Data Exchange, Inc.*, No. 2024-CFPB-PFDR-0001 (CFPB Jan. 8, 2025), available at https://files.consumerfinance.gov/f/documents/cfpb_standard-setter-decision-and-order-of-recognition-fdx_2025-01.pdf. The CFPB's order notes that FDX's member organizations include "depository and non-depository commercial entities." *Id.* at 1. FDX's website notes that its members include numerous BPI members, such as Bank of America, JPMorgan Chase, and Wells Fargo.[2]

5. On January 28, 2025, the Court adopted a briefing schedule for cross-motions for summary judgment. ECF No. 34. Thereafter, a series of developments at CFPB occurred that created uncertainty as to whether the CFPB intends to continue defending this case. On February 1, 2025, Director Rohit Chopra announced his departure from the CFPB. On February 7, 2025, Russell Vought was designated as acting Director of the CFPB. On February 8, 2025, Vought directed CFPB staff to stop working on proposed rules; suspend the effective dates of any finalized rules that are not effective; cease all investigative work, supervision, and examination activity; and refrain from making or approving filings or appearances in any litigation except to ask for a pause

[2] Financial Data Exchange – Members, https://www.financialdataexchange.org/FDX/FDX/The-Consortium/Members.aspx

in proceedings.[3] Consistent with that directive, the CFPB then sought stays in other pending litigation challenging CFPB rules. *See, e.g.*, *Texas Bankers' Ass'n v. CFPB*, No. 24-40705 (5th Cir.); *Cornerstone Credit Union League v. CFPB*, No. 25-00016 (E.D. Tex. Feb. 6, 2025).

6. On February 12, 2025, FTA moved to intervene in this matter to defend the Final Rule. On February 25, 2025, Plaintiffs and the CFPB filed a joint motion to stay proceedings for 30 days because the "CFPB's new leadership needs time to review and consider the CFPB's position on various pending agency actions and recently finalized rules, including the rule Plaintiffs challenge here." ECF No. 40, at 2. The joint motion further stated that the "CFPB also consents to a corresponding tolling of the compliance deadlines prescribed by the Rule." *Id.* The joint motion said nothing about FTA's pending motion to intervene.

7. That same day, this Court granted a "30-day stay of these proceedings and a corresponding 30-day tolling of the obligations prescribed by the rule the plaintiffs are challenging." ECF No. 41, at 2. The Court amended and modified the summary judgment briefing schedule accordingly. *Id.* However, the Court then *sua sponte* denied FTA's motion to intervene without prejudice, stating that "[u]nless the matter is resolved by the parties on or before March 31, 2025, the FTA may renew its Motion to Intervene at that time." *Id.*

8. On March 26, 2025, the parties requested a further stay of the litigation and an additional tolling of the Rule's compliance deadlines for 60 days, noting that the parties "continue to be interested in exploring whether the CFPB may take some action on the Rule that will substantially affect the need for this litigation." ECF No. 42, at 2.

[3] *See, e.g.*, Landon Mion, *Russ Vought, Tapped as CFPB's Acting Director, Directs Bureau to Issue No New Rules, Stop New Investigations*, Fox News, https://foxnews.com/politics/russ-vought-tapped-cfpbs-acting-director-directs-bureau-issue-no-new-rules-stop-new-investigations (Feb. 9, 2025).

ARGUMENT

FTA renews its motion to intervene. FTA has associational standing and should be permitted to intervene as of right or permissively given its timely motion, the interest of FTA and its members (as well as the consumers and small businesses they serve) in preserving the Final Rule—an interest that will be impaired if the Rule is vacated or its compliance deadlines are delayed—and the CFPB's inability to represent FTA's interests.

Finally, as set forth below, this Court cannot accept the parties' joint stipulation to tolling of the Rule's compliance deadlines simply because the Plaintiffs and the CFPB agree to such tolling. The compliance deadlines are set forth in the Rule itself, which the CFPB issued via notice and comment after hearing from thousands of stakeholders. *See* 12 C.F.R. § 1033.121(b). The mere possibility that the CFPB "may take some action on the Rule," ECF No. 42, at 2, does not justify delaying the existing deadlines. The rule, including its deadlines, can only be suspended via a rescission—which itself requires notice and comment—or via a stay or injunction entered by this Court after affirmative findings that Plaintiffs are likely to succeed on the merits and suffer irreparable harm. FTA must be permitted to intervene to argue why such a stay or injunction is unwarranted.

I. FTA Has Associational Standing.

Because FTA seeks to preserve the Final Rule via a judgment in favor of Defendants, it does not have an independent obligation to demonstrate an Article III stake in this case. *See Little Sisters of the Poor Saints Peter & Paul Home v. Pennsylvania*, 591 U.S. 657, 674 n.6 (2020); *Town of Chester v. Laroe Estates, Inc.*, 581 U.S. 433, 439-40 (2017). Nevertheless, even if FTA were required to establish associational standing, it could make that showing. To establish associational standing, FTA "must show that (1) its members would otherwise have standing to sue in their own

right; (2) the interests that the suit seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Universal Life Church Monastery Storehouse v. Nabors*, 35 F.4th 1021, 1036 (6th Cir. 2022) (internal quotation marks omitted); *see generally Friends of the Earth, inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); *Hunt v. Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977).

Each requirement is satisfied here. First, FTA is composed of members who would be directly and adversely affected by a judgment vacating the rule. These members, which are authorized third parties and data aggregators under the Rule, operate business models premised on consumers being able to access and securely share their financial data. Lee Decl. ¶ 4. For example:

- FTA member Plaid has explained that "as a data aggregator and third party," Plaid "allow[s] consumers to safely and securely share their own financial data from the institutions with which they bank (data providers) with their chosen digital finance apps and services (third parties)," thereby "accelerat[ing] greater choice and competition in the financial services marketplace" and "further[ing] the CFPB's aims of opening and decentralizing this market." Plaid Comments at 1.
- FTA member Ribbit Capital "is a global investment firm focused on the intersection of financial services and technology," and its "mission is to change the world of finance by providing capital and guidance to visionary financial services entrepreneurs around the world." Ribbit Capital Comments at 1. Ribbit Capital's portfolio "consists of more than 130 private and public company investments across six continents and a multitude of sectors within financial services, including payments, personal finance, investments and wealth, lending, insurance, cryptoassets, financial infrastructure, and financial software." *Id.* These investments include fintechs, which have "emerged to compete with traditional banks and to help eliminate consumer practices," and "are now positioned for the next wave of financial services development." *Id.*
- FTA member Stripe "is a technology company that builds economic infrastructure for businesses to transact on the Internet," and has "developed its Financial Connections product to streamline consumers' interactions with financial services by enabling consumers to elect seamless and secure bank payments online without being required to navigate burdensome (and unnecessary) manual verification processes." Stripe Comments at 1-2. As Stripe further explained, "consumers' ability to share their financial data with third parties of their choice will accelerate the market's ability to further leverage bank payments" and "can be used to develop and provide a diverse range of financial tools to consumers." *Id.* at 2.

- FTA member Wise is a "global payments company" that "believe[s] consumers have a fundamental right to access and control their financial data," and that "when this data is shared securely at the direction of consumers, it can help them better manage their finances, while receiving improved and innovative products and services." Wise Comments at 1.

As these examples illustrate, FTA members have a clear interest in defending the Final Rule.

Second, the interests FTA seeks to protect are germane to its organizational purpose. FTA is a trade association that represents the legal and economic interests of its member businesses. Lee Decl. ¶ 4. Its members have interests in ensuring "properly implemented, open banking in the United States," FTA Comments at 19, including ensuring that compliance with the Rule is required in a stable and predictable manner. Hence, acting to defend the CFPB's rule here, which furthers those interests, is germane to FTA's mission.

Finally, individual member participation is unnecessary in this case because the "suit raises a pure question of law" and the claims and relief sought do not require the Court to consider the "individual circumstances" of each member. *Int'l Union, United Auto., Aerospace & Agr. Implement Workers of Am. v. Brock*, 477 U.S. 274, 287 (1986); *Cf.* Am. Compl. ¶ 31 (agreeing that individual member participation is not needed in this suit).

II. FTA Should Be Permitted to Intervene as of Right or Permissively under Rule 24.

A. FTA Is Entitled to Intervene as a Matter of Right.

Under Federal Rule of Civil Procedure 24(a), the "court must permit anyone to intervene who: ... claims an interest relating to the property or transaction that is the subject of the action, and is so situated that disposing of the action may as a practical matter impair or impede the movant's ability to protect its interest, unless existing parties adequately represent that interest." Fed. R. Civ. P. 24(a)(2). To satisfy this standard, a proposed intervenor must show that (1) the motion to intervene is timely; (2) the proposed intervenor has a substantial legal interest in the subject matter of the case; (3) the proposed intervenor's ability to protect that interest may be

impaired absent intervention; and (4) the existing parties may not adequately represent the applicant's interest. *See, e.g.*, *Wineries of the Old Mission Peninsula Ass'n v. Twp. of Peninsula*, 41 F.4th 767, 771 (6th Cir. 2022). Each of these elements is "broadly construed in favor of potential intervenors." *Coal. to Defend Affirmative Action v. Granholm*, 501 F.3d 775, 779 (6th Cir. 2007) (quotation marks omitted); *see also Purnell v. City of Akron*, 925 F.2d 941, 950 (6th Cir. 1991).

FTA satisfies all four requirements. First, the motion is timely. In considering whether a motion to intervene is timely, the Court considers "all relevant circumstances," especially "(1) the point to which the suit has progressed; (2) the purpose for which intervention is sought; (3) the length of time preceding the application during which the proposed intervenors knew or should have known of their interest in the case; (4) the prejudice to the original parties due to the proposed intervenors' failure to promptly intervene after they knew or reasonably should have known of their interest in the case; and (5) the existence of unusual circumstances militating against or in favor of intervention." *Stupak-Thrall v. Glickman*, 226 F.3d 467, 472-73 (6th Cir. 2000) (quotation marks omitted).

Under the "relevant circumstances" of this case, *id.*, FTA's motion is timely. As to the first factor, this litigation has not progressed past its initial stages. *Cf. In re Auto. Parts Antitrust Litig., End-Payor Actions*, 33 F.4th 894, 901 (6th Cir. 2022) (explaining that, in the context of the first timeliness factor, "[l]itigation is in its final stages when the district court has already ruled on dispositive motions, closed discovery, certified classes, or held fairness hearings that lead to settlement approval" (citations omitted)). FTA initially moved to intervene less than three months after Plaintiffs amended their complaint and just over six weeks after Defendants filed their answer to the amended complaint; no discovery had taken place; and the parties had only recently had

their Rule 26 conference. *See, e.g.*, *Truesdell v. Meier*, No. 3:19-cv-66, 2020 WL 1991402, at *2 (E.D. Ky. Apr. 27, 2020) (timeliness factor satisfied when motion to intervene was filed "nearly 5 months after th[e] suit was filed" because "where little time has elapsed since the suit was filed, and little discovery has taken place, there is little prejudice to the existing parties on the basis of timeliness"); *cf. Stupak-Thrall*, 226 F.3d at 475 (motion untimely when "the court's previously identified 'finish line' ... was fast approaching"); *Suter v. Appalachian Reg. Healthcare, Inc.*, No. 14-cv-43, 2015 WL 12990211, at *1 (E.D. Ky. Mar. 6, 2015) (motion untimely when "trial ... will begin in less than four weeks"). Moreover, FTA filed its initial motion to intervene just days after the CFPB's acting Director ordered CFPB staff to cease many, if not all, of their functions, including ceasing all litigation activities beyond requesting a pause in litigation—thereby raising questions as to the CFPB's intention to continue litigating this case. And following this Court's denial without prejudice of FTA's initial motion to intervene, FTA has immediately renewed its motion to intervene after the parties sought additional tolling of the Rule's compliance deadlines.

With respect to the second factor, as discussed below, FTA has a valid purpose to intervene—namely to protect the economic interests of itself and its members, which are narrower than, and may diverge from, the CFPB's broader public interest in defending the Final Rule. *See In re Automotive Parts*, 33 F.4th at 902 (noting this Circuit is "more inclined to grant intervention when the purpose of intervention is limited in scope" and does not create a "likelihood of delay").

With respect to the third factor, as noted above, FTA initially moved to intervene early in this litigation, and very soon after the prior CFPB Director was fired and the acting Director reportedly ordered CFPB staff to refrain from taking any litigation activities beyond requesting a pause in litigation. *See Cameron v. EMW Women's Surgical Ctr.*, 595 U.S. 267, 279-80 (2022) (holding that the "most important circumstance relating to timeliness" is that the prospective

intervenor "sought to intervene as soon as it became clear that [its] interests would no longer be protected by the parties in the case" (internal quotation marks omitted)). And FTA has immediately renewed its motion to intervene following the parties' latest joint filing, which has now made clear that the CFPB is not aligned with FTA's interest in ensuring that the Rule is timely implemented in accordance with its stated compliance deadlines.

With respect to the fourth factor, the parties will suffer no prejudice because FTA intends to take no discovery and will adhere to the deadlines the Court adopts for additional briefing in this case. *See* ECF No. 41; *see also, e.g.*, *Ctr. for Bio. Div. v. Rural Utils. Serv.*, No. 5:08-cv-292, 2008 WL 4186891, at *2 (E.D. Ky. Sept. 10, 2008) (finding no prejudice where the proposed intervenor "is prepared to promptly join these proceedings and be bound by any substantive or procedural order issued prior to an order granting intervention").

Finally, with respect to the fifth factor, FTA's motion to intervene is timely given the unusual circumstances in which the recent and ongoing developments described above show that the governmental defendant is not fully defending the Final Rule.

Second, FTA has "an interest relating to the property or transaction that is the subject of the action." Fed. R. Civ. P. 24(a)(2). This Circuit has adopted a "rather expansive notion of the interest sufficient to invoke intervention as of right." *Mich. State AFL-CIO v. Miller*, 103 F.3d 1240, 1245 (6th Cir. 1997). Courts have long recognized that trade associations comprised of members affected by a regulatory rule possess an interest sufficient to intervene in a case challenging that rule. *See, e.g.*, *First City Bank v. Nat'l Credit Union Admin. Bd.*, 111 F.3d 433, 436 (6th Cir. 1997); *see also, e.g.*, *Zillow, Inc. v. Miller*, 126 F.4th 445, 451 (6th Cir. 2025) (noting that judge in Eastern District of Kentucky allowed Kentucky Press Association to intervene post-judgment to appeal ruling striking down portion of state open records law that benefited its

members); *Alaska Wilderness League v. Jewell*, 99 F. Supp. 3d 112, 122 (D.D.C. 2015) (concluding that a trade association had a sufficient interest in intervening to defend a U.S. Fish and Wildlife Service regulation that benefited its member companies).

As a trade association, FTA has a substantial interest in intervening to defend a rule that benefits its members. As FTA's and various of its members' comments to the CFPB make clear, the Final Rule will have a substantial impact on FTA's members. Lee Decl. ¶¶ 4-7. FTA explained that "[f]intech innovators are leveraging internet and mobile technologies to offer consumers access to credit, new payment options, and financial advisory services that can significantly reduce costs, accelerate access to funds, improve transparency and convenience, and enhance financial inclusion." FTA Comments at 1. "Much of this innovation is the result of consumers being increasingly able to expand their access to tailored financial products by unlocking and sharing their financial data with new providers." *Id.* at 2. Accordingly, FTA submitted comments "in support of the thoughtful and consumer-centric final implementation of the rule" (while noting certain areas of the proposed rule that it advocated to change). *Id.* at 1. FTA further stated it "support[ed] the Bureau's proposed incorporation of, and reliance on, a recognized standards setting organization (SSO) that will issue qualified industry standards," because "prescriptive technical requirements issued by the regulator will fail to keep pace with technological change and the development of related best practices." *Id.* at 10. FTA's comments also discuss particular aspects of the proposed rule in granular detail, further substantiating its members' interest in the Final Rule. *Id.* at 2-19. Because FTA's members benefit from the Final Rule, FTA has a significant, protectable interest in ensuring that the Final Rule withstands challenge. Lee Decl. ¶ 4. FTA's members also submitted comments underscoring the importance of this case to fintech businesses. *See supra at* 4-5; Lee Decl., Exs. B-E.

Third, the disposition of this action may impair or impede FTA's ability to protect its interest. A potential intervenor "must show only that impairment of its substantial legal interest is possible if intervention is denied." *Wineries*, 41 F.4th at 774 (quotation marks omitted). This burden is "minimal," *id.*, requiring only that "disposition of the present action would put the movant at a practical disadvantage in protecting its interest." *Id.* (quotation marks omitted). Thus, the proposed intervenor need only show that impairment is "possible," not a certainty. *Mich. State AFL-CIO*, 103 F.3d at 1247. That possibility is apparent here: Plaintiffs seek to vacate the Final Rule. If Plaintiffs prevail, the Court's judgment would impose harm on FTA's members, as well as millions of American consumers who use FTA members' products and services and the digital finance ecosystem in which FTAs members operate.

Finally, the CFPB does not adequately represent FTA's interests. When FTA initially filed its motion to intervene, there was already uncertainty as to whether the CFPB would continue to defend the Rule. The parties' prior joint motion, in which the CFPB "consent[ed] to a corresponding tolling of the compliance deadline prescribed by the Rule," ECF No. 40, at 2, reinforced that the CFPB cannot adequately represent FTA's interests, given FTA's interest in ensuring compliance with the Rule on the schedule set forth in the Rule itself. *See* 12 C.F.R. § 1033.121(b). And the inadequacy of CFPB's representation of FTA's interests is now apparent given the parties' latest joint motion, which seeks an additional tolling of the Rule's compliance deadlines for 60 days and creates continued uncertainty for businesses and consumers across that country that support the implementation of a consumer data right in the United States.

In any case, as the Supreme Court has made clear, this requirement presents "proposed intervenors with only a minimal challenge." *Berger v. N.C. State Conf. of the NAACP*, 597 U.S. 179, 195 (2022). That "minimal challenge" is easily met when a private entity seeks to intervene

on the side of the government. For example, in *Trbovich v. United Mine Workers of Am.*, 404 U.S. 528 (1972), the Supreme Court held that a union member was entitled to intervene in a lawsuit brought by the Secretary of Labor, when the union member had filed the administrative complaint that triggered the lawsuit. "At a high level of abstraction, the union member's interest and the Secretary's might have seemed closely aligned." *Berger*, 597 U.S. at 196 (citing *Trbovich*, 404 U.S at 529–30). But although the "Secretary's and union member's interests were 'related,'" "the interests were not 'identical'—the union member sought relief against his union, full stop; meanwhile, the Secretary also had to bear in mind broader public-policy implications." *Id.* (quoting *Trbovich*, 404 U.S. at 538–39). "Rather than endorse a presumption of adequacy, the Court held that a movant's burden in circumstances like these 'should be treated as minimal.'" *Id.* (quoting *Trbovich*, 404 U.S. at 538 n.10).

In keeping with those principles, the Sixth Circuit has recognized that governmental entities do not adequately represent the interests of private parties for purposes of Rule 24(a)(2). *See Wineries*, 41 F.4th at 775 (finding private interests diverged from the local government's interest and recognizing the "[n]umerous cases from other circuits dealing with the interest of governmental entities" in relation to the interest of private entities). Other courts of appeals have taken the same view. *See Wal-Mart Stores, Inc. v. Tex. Alcoholic Beverage Comm'n*, 834 F.3d 562, 569 & n.9 (5th Cir. 2016) (finding that state agency did not adequately represent trade association's interests and collecting numerous cases); *Kane Cnty. v. United States*, 928 F.3d 877, 894 (10th Cir. 2019) (governmental interests "involve a much broader range of interests, including competing policy, economic, political, legal, and environmental factors" (quotation marks omitted)); *Fund for Animals, Inc. v. Norton*, 322 F.3d 728, 736–37 (D.C. Cir. 2003) (noting that "we have often concluded that governmental entities do not adequately represent the interests of

aspiring intervenors," such as when the private intervenor "is seeking to protect a more narrow and 'parochial' financial interest not shared" more broadly).

Thus, even in an ordinary case, the CFPB—a government regulator—could not adequately represent the interests of FTA, a private trade association. As a governmental entity, the CFPB's stated goal is to advance its sovereign interests, while FTA's goal is to advance the business interests of its members. And, as discussed, this is far from the ordinary case in which a private trade association seeks to intervene on the same side as a governmental entity, given the agency's agreement to toll the compliance deadlines set forth in the Rule.

Moreover, although FTA here seeks to defend the consumer data rights set forth in the Final Rule, FTA disagrees with the CFPB's exercises of power in other contexts. And FTA does not even agree with the Final Rule in all respects: FTA urged the CFPB during the rulemaking to take additional steps to facilitate additional secure sharing of consumer data, a point made by numerous other stakeholders from across industry and academia. For example, FTA's comments explained how the CFPB should permit the "[b]roader use of data, including for secondary use and when data is de-identified" to continue to evolve technology that will help fight fraud, expand responsible credit access, and offer additional consumer benefits. FTA Comments at 4. FTA would participate in any future rulemaking to advance these arguments and others to further strengthen the existing Rule. Because FTA's interests and arguments therefore differ from the CFPB's, the CFPB does not adequately represent FTA's interests for purposes of Rule 24(a).

B. Alternatively, this Court Should Allow FTA to Permissively Intervene Under Rule 24(b)(1).

In the alternative, FTA requests that the Court grant permissive intervention under the less-demanding standard in Rule 24(b)(1). That standard provides that "[o]n timely motion, the court may permit anyone to intervene who ... has a claim or defense that shares with the main action a

common question of law or fact." Fed. R. Civ. P. 24(b)(1). In deciding whether a party should be permitted to intervene, the "court must consider whether the intervention will unduly delay or prejudice the adjudication of the original parties' rights." Fed. R. Civ. P. 24(b)(3); *see generally Buck v. Gordon*, 959 F.3d 219, 223-25 (6th Cir. 2020); *League of Women Voters of Mich. v. Johnson*, 902 F.3d 572, 576-80 (6th Cir. 2018).

As explained above, FTA's motion to intervene is timely. And for the same reasons that FTA shares a substantial legal interest in the subject matter of this appeal, FTA has a claim that shares in the legal and factual questions likely to be raised in this case. Moreover, as explained, FTA's intervention will not unduly delay the action or prejudice the existing parties because FTA does not intend to seek any discovery and will follow the same briefing schedule the Court has established as to the rest of the parties. *See* ECF No. 41. Therefore, the Court should grant FTA's motion to intervene under Rule 24(b)(1).

III. This Court Should Not Further Toll the Compliance Period Without Hearing from FTA.

In their latest filing, the parties have again requested that this Court toll the compliance deadlines for the Rule. While tolling the deadlines may suit the parties' interests, this Court cannot simply agree to toll deadlines set forth in the Final Rule without at least hearing from FTA and making certain findings mandated by the APA. The parties' proposed 60-day "tolling period" would result in a substantive alteration to the compliance deadlines in the current Rule—the type of alteration that requires notice-and-comment rulemaking. To avoid notice-and-comment rulemaking, the parties are asking the Court to issue what is, in reality, 60-day stay of the Final Rule, over and above the 30-day tolling period that this Court has already granted. But under the APA, the Court cannot grant such a stay unless it makes the threshold determination that Plaintiffs are likely to succeed on the merits and a stay is needed to prevent irreparable harm. FTA should

be permitted to intervene so that the Court can receive briefing on whether that legal standard is satisfied.

It is a bedrock principle of administrative law that an agency cannot unilaterally—or in conjunction with plaintiffs—amend (much less repeal) their legislative rules without undertaking notice-and-comment rulemaking. Rather, the APA "mandate[s] that agencies use the same procedures when they amend or repeal a rule as they used to issue the rule in the first instance." *Perez v. Mortgage Bankers Ass'n*, 575 U.S. 92, 101 (2015); *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009); *see generally* 5 U.S.C. §§ 553(b)-(c); 551(5). That process requires the agency to "issue a '[g]eneral notice of proposed rulemaking,'" "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments," and "consider and respond to significant comments received during the period for public comment." *Perez*, 575 U.S. at 96 (quoting 5 U.S.C. § 553(c)). These procedures ensure that the numerous stakeholders who have an interest in the existing rule can be heard before the rule is modified or rescinded.

Here, the Final Rule was promulgated via an extensive rulemaking process. The agency provided notice of the proposed rule and received and considered more than 11,000 comments. Am. Compl. ¶¶ 11, 82. That process culminated in the Final Rule. Any modification of the Final Rule, in the absence of judicial involvement, therefore requires a new round of notice-of-comment rulemaking. That is so even with respect to the Rule's specific compliance deadlines, ranging from April 1, 2026 to April 1, 2030, which are set forth in the regulatory text. *See* 12 C.F.R. § 1033.121. The CFPB reasonably explained how it chose those specific deadlines. 89 Fed. Reg. at 90,860, 90,956. Under the APA, Plaintiffs and the CFPB cannot undo this elaborate rulemaking process by agreeing amongst themselves to delay the Rule's deadlines.

To avoid notice-and-comment rulemaking, the parties ask this Court to enter an order "tolling" the Final Rule's compliance deadlines for an additional 60-day period. Effectively, they seek a 60-day stay of the Final Rule—the practical effect of which would be to alter the deadlines currently appearing in 12 C.F.R. § 1033.121. But the APA specifies what must be shown for this court to grant such a stay—and mere agreement between the parties does not suffice. Rather, under the APA, a "reviewing court ... may issue all necessary and appropriate process to postpone the effective date of an agency action," but only "to the extent necessary to prevent irreparable injury." 5 U.S.C. § 705. Moreover, the Sixth Circuit has recognized that a stay pursuant to 5 U.S.C. § 705 requires consideration of the traditional stay factors, including not only irreparable harm but also the "likelihood that the party seeking the stay will prevail on the merits of the appeal," the "prospect that others will be harmed if the court grants the stay," and the "public interest in granting the stay." *State of Ohio ex rel. Celebrezze v. Nuclear Regul. Comm'n*, 812 F.2d 288, 290 (6th Cir. 1987). This makes sense: agency rules, including the Final Rule, affect numerous stakeholders, not just the parties participating in the litigation. Here, however, the parties have not made any showing that Plaintiffs are likely to succeed on the merits or that they will suffer irreparable harm if a stay is not granted. And this Court has not evaluated whether third parties or the public interest will be harmed if the compliance deadlines for the Rule are delayed. Granting FTA's intervention and receiving briefing on these questions is therefore essential to aid this Court's review.

Finally, to the extent Plaintiffs and the CFPB both seek for the CFPB to "take some action" to resolve this case, ECF No. 42, at 2, they cannot accomplish that result via a standard settlement agreement, in which the parties privately decide on an appropriate resolution and then dismiss the case with prejudice. Rather, this Court would need to grant an injunction, but only after finding that the factors bearing on such relief have been satisfied, including likelihood of success on the

merits and irreparable harm. *See, e.g.*, *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008); *Ohio v. Becerra*, 87 F.4th 759, 768 (6th Cir. 2023). Even if both Plaintiffs and the CFPB consent to an injunction, a "consent decree is a judicial act because it places the power and prestige of the court behind the compromise struck by the parties." *Evoqua Water Techs., LLC v. M.W. Watermark, LLC*, 940 F.3d 222, 229 (6th Cir. 2019). The Court must decide for itself whether that "judicial act" has any legal basis. Allowing the parties to stipulate to an injunction in these circumstances would allow the CFPB to "circumvent the usual and important requirement, under the Administrative Procedure Act, that a regulation originally promulgated using notice and comment … may only be repealed through notice and comment." *Arizona v. City and County of San Francisco*, 596 U.S. 763, 765 (Roberts, C.J., concurring). The Court should not permit this "tactic of 'rulemaking-by-collective-acquiescence.'" *Id.*

In short, this Court has made no findings as to whether a stay or injunction is warranted. Nor has it received briefing on that issue. And because the CFPB is no longer defending the deadlines set forth in the Final Rule, it is unlikely to receive any such briefing absent FTA's intervention. The Court should therefore grant FTA's motion to intervene and set a briefing schedule to determine whether any further delay in the Final Rule's effective dates is justified.[4]

CONCLUSION

The renewed motion to intervene should be granted.

[4] FTA has no objection to the parties agreeing to stay this *litigation* pending further developments at the CFPB, as long as the Rule's compliance deadlines are not further tolled.

Dated: March 26, 2025

Respectfully submitted,

/s/ Michael P. Abate

Michael P. Abate
KAPLAN JOHNSON ABATE & BIRD
710 West Main Street, 4th Floor
Louisville, KY 40202
(502) 540-8280 (Telephone)
mabate@kaplanjohnsonlaw.com

Counsel for the Financial Technology Association

CERTIFICATE OF SERVICE

I hereby certify that on March 26, 2025, the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

Dated: March 26, 2025 */s/ Michael P. Abate*

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE,

Plaintiffs,

v. Case No. 5:24-cv-00304-DCR

CONSUMER FINANCIAL PROTECTION BUREAU and RUSSELL VOUGHT, in his official capacity,

Defendants.

DECLARATION OF PENNY LEE IN SUPPORT OF THE FINANCIAL TECHNOLOGY ASSOCIATION'S MOTION TO INTERVENE

I, Penny Lee, declare:

1. My name is Penny Lee. I am over 18 years of age, of sound mind, and capable of making this declaration. I have personal knowledge of the matters set forth in this affidavit. I am the President and CEO of the Financial Technology Association ("FTA"). Before joining FTA, I led the public affairs group at Invariant, a government relations and strategic communications firm. I previously served as Chief Strategy Officer at 1776, a technology incubator and accelerator. I also co-founded and chaired K Street Capital, an angel investment group, which has invested in over 70 companies and has $65 million in assets under management. I graduated from Baylor University with degrees in political science and journalism.

2. FTA is a Washington, DC-based trade association representing digitally-native financial technology (fintech) industry leaders. FTA champions the transformative role of technology for American consumers, businesses, and the economy. As part of that mission, FTA supports regulation that empowers consumers to access and share their financial data with the applications ("apps") and services they want to use, thus fostering innovation and competition among the financial services market. FTA's members are innovators seeking to provide more seamless services, lower-cost products, and greater consumer choice in the financial services market. These members leverage internet and mobile technologies to offer consumers access to credit, new payment (including pay by bank) options, and financial advisory services that can significantly reduce costs, accelerate access to funds, and improve transparency and convenience.

3. FTA has long advocated for personal financial data rights and open banking rules of the road to promote competition, choice, and access. Consumers' ability to securely control and share their personal financial data rights enables millions of Americans to access lower-cost, transparent, and tailored financial services.

4. FTA has an interest in defending the Consumer Financial Protection Bureau's Final Rule for the Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838 (Nov. 18, 2024) ("Final Rule"). The Final Rule increases competition, improves consumers' choices, and drives momentum for future innovations that benefit consumers—like cash flow underwriting, stronger fraud tools, pay-by-bank, and personalized financial services—while fostering greater trust in the financial ecosystem. Many of FTA's members operate on business models premised on consumers being able to easily access and share their financial data from their bank accounts. FTA has an interest in advancing the legal and economic interests of its members, who benefit

from the CFPB's Final Rule. Because FTA's members benefit from the CFPB's Final Rule, they would be harmed by a judgment invalidating the Final Rule.

5. FTA submitted comments in the rulemaking process that "applaud[ed] the [CFPB's] Proposal" and expressed "support [for] the thoughtful and consumer-centric final implementation of the rule." FTA Comments, Notice of Proposed Rulemaking – Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, at 1 (Dec. 21, 2023) (Ex. A). FTA's comments explained that "Fintech innovators are leveraging internet and mobile technologies to offer consumers access to credit, new payment options, and financial advisory services that can significantly reduce costs, accelerate access to funds, improve transparency and convenience, and enhance financial inclusion." *Id.* "Much of this innovation is the result of consumers being increasingly able to expand their access to tailored financial products by unlocking and sharing their financial data with new providers." *Id.* at 2.

6. FTA's comments also noted the benefits of the rule for consumers: "The ability to control and share financial data allows consumers more convenient and efficient ways to view and manage their money and shop for new, more tailored, and lower-cost financial services products and providers. This facilitates competition by allowing new entrants in the marketplace and ensuring information is no longer trapped with incumbent providers; consumers are empowered to use their data for their own benefit." *Id.* "When presented with clear information on data collection, use, and practices, consumers are best positioned to authorize the sharing and use of their financial data. A broad right to such authorization ensures that consumers can benefit from increased financial services competition and improved product offerings." *Id.* at 4-5.

7. FTA members also participated in the rulemaking and expressed support for the CFPB's aim to provide for greater choice and competition in the marketplace for financial services.

Those members would be harmed by a judgment invalidating the Final Rule. *See* Plaid Comments, Notice of Proposed Rulemaking – Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, at 1 (Dec. 29, 2023) (Ex. B); Ribbit Capital Comments, Notice of Proposed Rulemaking – Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, at 1 (Dec. 29, 2023) (Ex. C); Stripe Comments, Notice of Proposed Rulemaking – Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, at 1-2 (Dec. 27, 2023) (Ex. D); Wise Comments, Notice of Proposed Rulemaking – Required Rulemaking on Personal Financial Data Rights, Docket No. CFPB-2023-0052, at 1 (Dec. 29, 2023) (Ex. E).

I declare under penalty of perjury that the foregoing is true and correct.

Executed: February 12, 2025
Washington, D.C.

Penny Lee

EXHIBIT A

Submitted electronically

December 21, 2023

Comment Intake—FINANCIAL DATA RIGHTS
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights
(Docket No. CFPB-2023-0052; RIN 3170-AA78)

The Financial Technology Association (FTA) appreciates the opportunity to provide feedback on the CFPB's "Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights," which will implement Section 1033 of the Dodd-Frank Act (the "Proposal"). FTA believes that a robust personal financial data right can empower consumers, drive greater financial health and opportunity, and advance consumer-centric financial services competition.[1] We accordingly applaud the Bureau's Proposal and offer this comment letter in support of the thoughtful and consumer-centric final implementation of the rule.

FTA champions the transformative role of financial technology for American consumers, businesses, and the economy. A core pillar of FTA's effort to advance consumer-centric financial services development in the U.S. is ensuring modern regulatory frameworks that recognize and foster the benefits of financial technology-driven innovation, including with respect to new models that rely on responsible use of financial data. Fintech innovators are leveraging internet and mobile technologies to offer consumers access to credit, new payment options, and financial advisory services that can significantly reduce costs, accelerate access to funds, improve transparency and convenience, and enhance financial inclusion.

[1] We agree with the Bureau that "[d]igitization and decentralization in consumer finance create new possibilities for more seamless consumer switching and greater competitive intensity." *See* Consumer Financial Protection Bureau, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf. Examples of open banking include when consumers seamlessly connect their bank account to a payment app, use personalized financial dashboards to better understand their financial health, provide access to non-traditional financial data in order to receive credit, and aggregate investments with robo-advisors. Open banking further provides opportunities to stimulate payments innovation by permitting direct integrations with banks and offering consumers faster and lower-cost payments services.

Much of this innovation is the result of consumers being increasingly able to expand their access to tailored financial products by unlocking and sharing their financial data with new providers. The ability to control and share financial data allows consumers more convenient and efficient ways to view and manage their money and shop for new, more tailored, and lower-cost financial services products and providers. This facilitates competition by allowing new entrants in the marketplace and ensuring information is no longer trapped with incumbent providers; consumers are empowered to use their data for their own benefit.

Notably, today, open banking technology allows access to important tools for unbanked and underbanked consumers, including increased access to credit through identity verification, increased data sources, such as rental, utility, or tax payment history, and no-fee salary advances. This technology further helps to safeguard the financial system, including through enhanced fraud mitigation tools facilitated by robust identity verification capabilities.[2]

I. The Bureau Should Anchor to Core Guiding Principles and Make Important Amendments to the Proposal in Finalizing Section 1033 Implementation.

FTA welcomed the earlier opportunity to comment on the CFPB's "Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights." In that letter, we noted the importance of the Bureau anchoring the ultimate implementation of the 1033 rulemaking to three core principles, which remain equally relevant here. More specifically, we urged then and reiterate now that in finalizing the rule, the Bureau should:

1. *Focus on consumer-centric implementation*: The touchstone of the final rule should be fostering competition and responsible innovation in financial services that permits more informed comparison shopping and product selection, better holistic understanding of financial health and wellness, and ultimately greater financial choice and opportunity. As discussed in greater detail below, this means allowing for consumer-centric secondary use of such data, subject to clear disclosure, as well as robust privacy and security safeguards.

2. *Avoid anti-competitive behavior*: Traditional financial institutions (FIs) have commonly held a consumer's financial data captive in order to prevent the consumer from switching to a different service provider or shopping for alternative products and services.[3] Consistent

[2] *See, e.g.*, MX, *What Is Instant Account Verification? What to Know and Key Benefits*, available at https://www.mx.com/blog/what-is-instant-account-verification/; Plaid, *Plaid Identity Verification* (last visited Dec. 14, 2023), available at https://plaid.com/products/identity-verification/.

[3] *See* Dan Murphy and Jennifer Tescher, *Policymakers must enable consumer data rights and protections in financial services*, Brookings (Oct. 20, 2021) ("Already there are reports of some financial institutions restricting access to consumer data. Such restrictions can serve to entrench incumbent institutions and limit competition to the detriment of consumers. These restrictions also are out of step with consumer preferences."), available at

with the U.S. Treasury Department's recent white paper on competition in financial services, the Bureau should monitor and prevent industry attempts to craft, interpret, and apply certain Section 1033 requirements in a manner that would block the sharing of financial data, restrict data parity, and advance anti-competitive objectives.

3. *Leverage Existing Legal Frameworks, Technologies, and Standards Setting Organizations (SSOs)*: Given the potential complexity of implementing Section 1033, FTA supports the Bureau's proposed reliance on existing legal and regulatory frameworks, and available technologies, to avoid creating new, untested requirements that may delay implementation, increase uncertainty, or complicate compliance. FTA further supports reliance on SSOs, but encourages the Bureau to work promptly to provide more specificity around the proper development and approval of an SSO given its centrality to the successful implementation of open banking in the United States.

With these core principles underpinning our feedback, FTA will detail below the following recommendations and suggested amendments to final implementation of the open banking rule:

A. Broader use of data, including for secondary use and when data is de-identified, benefits consumers and should be permitted, subject to appropriate disclosures and additional safeguards.
B. Given the importance of SSOs and related standards and certifications, the final rule should provide greater clarity regarding the composition, operations, and role of SSOs, as well as more time to ensure an SSO is properly developed.
C. Given the time, cost, and complexity of operationalizing Section 1033 requirements, the final rule should create a more realistic timeframe for implementation—a failure to do so could result in confusion, undermine security and trust, and lead to service interruptions that harm consumers.
D. The concept of digital wallets is vague and undefined—the final rule should provide greater clarity regarding definitions and responsibilities, as well as provide for an extended implementation timeframe.
E. The Bureau should further ensure that the final rule:
    i. Clarifies the interplay of Section 1033 with the proposed FCRA rulemaking and confirms that data aggregators are not de facto credit bureaus.

https://www.brookings.edu/research/policymakers-must-enable-consumer-data-rights-and-protections-in-financial-services/; *see also* Director Rohit Chopra, *Prepared Remarks of CFPB Director Rohit Chopra on the Overdraft Press Call* (Dec. 1, 2021) ("If America can shift to an open banking infrastructure, it will be harder for banks to trap customers into an account for the purpose of fee harvesting."), available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-rohit-chopra-overdraft-press-call/.

ii. Avoids overly prescriptive disclosure requirements and ensures such disclosures are not used by data providers to dissuade or discourage a consumer from seeking a personal data transfer.

iii. Establishes clear standards around the use of Tokenized Account Numbers to avoid anticompetitive behavior, undermining fraud models, and chilling further innovation in business models.

II. Broader use of data, including for secondary use and when data is de-identified, benefits consumers and should be permitted, subject to appropriate disclosures and additional safeguards.

As a threshold matter, FTA understands and agrees with the Bureau on the importance of safeguarding how consumer data is collected and used by intermediaries and financial services providers. FTA members are among the world's leading financial technology firms focused on improving consumer financial services, outcomes, and opportunities. Financial data is often at the center of financial services innovation, and its fair, transparent, and permissioned use is critical to building consumer trust and driving consumer-centric competition and product development.[4] To this end, FTA members take seriously their responsibilities and obligations to customers, and view such commitments as essential to building this long-term trust.

As part of these commitments, FTA has published data privacy principles that reflect FTA's values of promoting consumer trust and transparency, along with financial inclusion and robust competition to lower costs and improve financial services.[5] These principles for engaging with consumers include: (i) full transparency regarding how data is collected and used, (ii) consumer control of personal data, (iii) provider use of data for stated and transparent purposes, (iv) plain language disclosures, and (v) non-discrimination.

We note these principles as consistent with the overarching goals and intent of Section 1033 and consistent with unlocking the full value of open banking for consumers. When presented with clear information on data collection, use, and practices, consumers are best positioned to authorize the

[4] It is important to emphasize that this rulemaking should mark only the beginning of a broader push in the U.S. to an "open finance" system, whereby all individuals and entities have the ability to share their permissioned financial data with chosen third-parties. To this end, broader categories of data should be incorporated into an open finance system and no data providers should be allowed to engage in anti-competitive behaviors in order to block or dissuade the sharing of such data. FTA welcomes the Proposal's requirements regarding the obligations of data providers for categories of data not explicitly covered by the final rule and the push for wider adoption of APIs that will underpin an expanded open finance system in this country.

[5] Financial Technology Association, *FTA Privacy Principles for the Future of Finance* (last visited Dec. 14, 2023), available at https://www.ftassociation.org/fta-privacy-principles-for-the-future-of-finance/.

sharing and use of their financial data. A broad right to such authorization ensures that consumers can benefit from increased financial services competition and improved product offerings.

On the other hand—and of particular concern given the Proposal's current approach to data collection and use—unnecessarily prescriptive regulatory limitations and restrictions on data collection, retention, and use will undermine consumer interests by reducing the ability of third parties to develop new products and services and offer consumers additional products that compete with their legacy providers. An approach that seeks to preclude providers from collecting and using data for consumer-centric product innovation will have negative consequences on competition, innovation, and the health of financial services in the United States. As detailed below, this approach is also not necessary to satisfy legitimate consumer and regulatory privacy concerns. To this end, reasonable safeguards can empower consumers to understand and authorize how their data is used, while preventing harms referenced by the Bureau in its Proposal.

A. Consumers should have the right to permission their data that is "reasonably related" to the products or services being offered by a third party.

The Bureau's Proposal limits a provider's access only to a consumer's data that is "reasonably necessary" to provide the product or service requested by the consumer. This standard creates the opportunity for misinterpretation that is unnecessarily restrictive, could impede consumer-centric product offerings, and places third-parties receiving data through Section 1033 at an unfair disadvantage relative to those receiving data under well-established regimes, including the Gramm-Leach-Bliley Act (GLBA).

More specifically, in offering a particular product or service—and further improving or tailoring such product or service—a provider may reasonably collect a range of data and data elements. Each such data element alone may not be explicitly "necessary" for the provision of a particular product or service, but taken together such elements become necessary to offering the product or service. Additionally, certain data elements may be important to improving aspects of the product or service, including the associated customer experience and overall product performance, rather than being critical in offering the original product or service. Allowing space for improving products is critical to avoid locking in the status quo. The improvement of products may require access to various data elements, some of which will prove to be essential to that new product or offering.

For this reason, the Bureau should allow an authorized third-party to collect data that is "reasonably related" to the product or service, especially because the data is already subject to appropriate

safeguards.[6] To this end, the Bureau should consider how the requirement of clear disclosure regarding data use and informed consent can help to minimize regulatory concerns.

Additionally, GLBA allows financial institutions to collect data that goes beyond a "reasonable necessity" standard, subject to disclosure and consent safeguards. Consistent with our north star principle of leveraging existing regulatory frameworks to help ensure consistency and certainty, GLBA should inform Section 1033 implementation to be sure that all providers are on a level playing field when it comes to collection, use, and retention of permissioned consumer financial data. And, indeed, the Bureau does appropriately rely on GLBA in the Proposal as the framework for data security, which it should similarly do in the context of data use and privacy.[7]

If the Bureau maintains a reasonable necessity standard, however, it should clarify that in determining whether data is reasonably necessary for a particular product or service, it will look holistically at the data being collected and used rather than assess necessity at the individual data element level. The Bureau should further make clear that data elements used to improve, develop, personalize, or innovate from an initial product or service offering are properly considered to be reasonably necessary.

As noted above, an overly restrictive view will serve to lock in the status quo and prevent product improvements that benefit consumers, including with respect to consumer underwriting that has long been constrained by singular reliance on credit scores. Importantly, data is also essential to other business operational improvements, including fraud detection and prevention, as well as enhanced user engagement and experience. Given these business and design realities, absent such clarification in the final rule, including through the provision of examples, the term "reasonably necessary" will create uncertainty amongst providers and limit their confidence in using data to offer or improve a product offering or business operation.

B. Secondary use of consumer data is in the consumer's best interest and should be broadly permitted.

The Bureau's Proposal currently prohibits "secondary use" of financial data, except in limited cases, such as countering fraud. While the Bureau properly notes concerns with certain practices, including opaque sales of consumer data to other entities and providers, it takes an overbroad approach to mitigating such concerns rather than a tailored solution that avoids unintended

[6] Adopting the "reasonably related" standard is supported by the fact that this standard is understood and used for various purposes in state data privacy laws. *See, e.g.*, California Consumer Privacy Act of 2018 (CCPA).
[7] *See* Consumer Financial Protection Bureau Proposal, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf.

consequences. The Bureau should consider the many consumer benefits of secondary data use and whether other tailored safeguards can better satisfy important regulatory objectives, including prohibitions of specific business activities known to cause consumer harm, clear disclosure, and informed consent.

With respect to consumer benefits, secondary uses of financial data may include holistic consideration of the consumer's financial health and tailored recommendations for more appropriate products and services that better meet the consumer's financial goals and which may not be within the scope of services initially requested or may not be known to the consumer to exist as an alternative. Some of these tailored offerings may be part of cross-selling efforts, which are commonly desired by consumers.

Indeed, a recent survey of consumers found that 77% would value having their financial institution offer them personalized financial advice based on open banking financial data; and 94% would want their financial institution to use financial data to advise them about a better deal on a product.[8] Both of these scenarios may be considered a "secondary use" of data. Restricting these types of secondary uses would be inconsistent with the overarching principle that Section 1033 implementation should be in the consumer's best interest. It would also be counter to the inclusion of existing regulatory frameworks that permit secondary use of data, including GLBA and state data privacy regimes. A failure to ensure parity in treatment of secondary use under Section 1033 with other data privacy frameworks will arbitrarily place third-parties in this regime at an unfair competitive disadvantage relative to most other firms in the broader economy.

It is further a bedrock of the American rule of law that consumers should be permitted to make their own informed decisions when provided with proper information.[9] For this reason, it is appropriate for the Bureau to focus on the quality and clarity of disclosures, including when a third-party seeks to use data for secondary purposes. A consumer provided with appropriate disclosures that he or she can reasonably understand should accordingly be able to provide informed consent to secondary use. This approach would be the most consumer-centric and foster consumer choice and agency.

To the extent that there are potential secondary uses objectively deemed so harmful to consumers that it should override informed consent, only those specific uses the Bureau so identifies after careful review and sufficient public comment should be precluded. For example, FTA believes

[8] MX, *The Ultimate Guide to Open Banking*, available at https://www.mx.com/assets/resources/ult-guides/ultimate-guide-to-open-banking.pdf.

[9] Jacqueline M. Nolan-Haley, *Informed Consent in Mediation: A Guiding Principle for Truly Educated Decisionmaking*, 74 Notre Dame L. Rev. 775, 827 (1999) ("Informed consent is an ethical, moral, and legal concept that is deeply ingrained in American culture.").

that consumer financial data should not be secondarily used by providers to enhance collections efforts. There may be other such uses that objectively are not in the consumer's best interest. Beyond these scenarios, however, proper disclosures, informed consent, and data privacy and security practices are the appropriate way to address other risks highlighted by the Bureau in the Proposal, including with respect to the protection of sensitive data.

C. In line with the SBREFA panel recommendation, de-identified data should be allowed for a broad range of research & development, model development, and product innovation purposes—a failure to so permit will impede financial services and technology development in the U.S.

The Bureau's Proposal currently includes a blanket prohibition on secondary data use, including when data is de-identified. As the Bureau notes, however, the SBREFA small business panel recommended that the Bureau "consider options that would permit uses of data (including de-identified or anonymized data . . .)." The Bureau goes on to note the existence of a straightforward standard for defining de-identified data that should mitigate outstanding privacy concerns.[10] Given the importance of permitting use of de-identified data and the ready availability of standards to mitigate risks, it would be against the consumer's interest to preclude such use, especially when the use does not harm the consumer. Moreover, a failure to allow for use of de-identified data would cause substantial harm to industry and overall U.S. competitiveness, which require access to high-quality data.[11]

First, smaller financial services providers would find themselves facing an insurmountable competitive disadvantage relative to larger organizations, including banks. Larger FIs collect vast amounts of data on consumers, including under GLBA. These FIs are permitted to pursue research & development, product innovation, and development of new business models, including those leveraging AI technology, using such data. Smaller entities or startups, on the other hand, lack access to large pools of quality data. Section 1033 was intended to help promote consumer choice and market competition, but as proposed by the Bureau, the rule will in effect undermine these objectives if entities receiving data under the rule are not able to use the data, even in a de-identified format, to innovate and compete.

Second, a blanket prohibition on use of de-identified data will impede and undermine U.S. global competitiveness in developing responsible AI/ML technologies, which hold promise across the

[10] *See* Consumer Financial Protection Bureau Proposal, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), n. 144, available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf.

[11] It is important to underscore that once data is properly de-identified it would no longer be subject to the third-party obligations contained within Section 1033.421(h)(3)(ii).

financial services landscape from improving the fairness of consumer underwriting to enhancing compliance and fraud detection. The FSOC recently published its 2023 Annual Report where it noted that "AI offers potential benefits, such as reducing costs and improving efficiencies, identifying more complex relationships, and improving performance and accuracy."[12] FSOC further noted potential risks, including around access to and use of quality data that is subject to appropriate data controls.[13] To this end, Section 1033 holds promise in creating a transparent and regulated pipeline of high-quality data, subject to appropriate safeguards, that can advance responsible model development. The Proposal, however, would undermine such development by limiting access to quality data—likely resulting in less innovation and model development that relies on lower quality data more likely to include inaccuracies, bias, and other harms.

Finally, as noted above—and in contravention of the principle that the Bureau should incorporate existing regulatory requirements and expectations, where appropriate—the current Proposal would place entities receiving data via Section 1033 on an unlevel playing field relative to those receiving data under GLBA or other regulatory frameworks and contractual relationships. Many entities collect and have access to broad pools of de-identified consumer data and rarely have limitations on secondary use. Especially when Section 1033 includes many additional consumer safeguards, it is not necessary to treat these data recipients punitively relative to other data recipients. This approach will also drive nonsensical scenarios where a small bank that receives data directly from customers can use such data, including when it is de-identified, for secondary purposes, while it cannot do the same with respect to data received under Section 1033.

For the reasons noted here, we strongly encourage the Bureau to adhere to the SBREFA small business panel recommendation of allowing use of de-identified data. We further encourage the Bureau to adopt the standard it flagged in the Proposal with respect to defining what "de-identified" data means. More specifically, the Proposal noted that "one standard suggested by SBREFA commenters, articulated in a 2012 FTC privacy report, and codified in several State laws describes de-identified information as data for which a business has (1) taken reasonable measures to ensure that the information cannot be linked to an individual; (2) publicly committed not to attempt to re-identify the information; and (3) contractually obligated any recipients not to attempt to re-identify the information."[14] This standard is a reasonable way to safeguard consumers, while

[12] U.S. Financial Stability Oversight Council, *2023 Annual Report* (December 2023), available at https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf?ftag=YHFa5b931b.
[13] *Id.* FTA and its members believe in the importance of responsibly developing AI technologies, including through collaboration with governmental and regulatory stakeholders. To this end, we look forward to working with the Bureau and the broader government to address risks and ensure responsible AI development in the U.S.
[14] The Proposal (*citing* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at 20-21 (2012), available at https://www.ftc.gov/reports/protecting-consumer-privacy-erarapid-change-recommendations-businesses-policymakers; Cal. Civ. Code section 1798.140(m); Colo. Rev. Stat. section 6-1-1303(11); Va. Code sections 59.1-575, 59.1-581; Utah Code Ann. 13-61-101(14)).

allowing for critical, consumer-centric research and development, competition, and product innovation.

III. Given the importance of SSOs and related qualified industry standards and certifications, the final rule should provide greater clarity regarding the composition, operations, and role of SSOs, as well as more time to ensure an SSO is properly developed.

FTA supports the Bureau's proposed incorporation of, and reliance on, a recognized standards setting organization (SSO) that will issue qualified industry standards. As the Bureau notes, prescriptive technical requirements issued by the regulator will fail to keep pace with technological change and the development of related best practices. Beyond such standards, FTA further believes that an empowered SSO is necessary to ensure the sound and efficient operation of an open banking regime in the U.S.

Given the centrality of the SSO to the Bureau's Proposal, as well as the need to further clarify, define, and potentially expand its role, we believe more work needs to be done by the Bureau in its final rulemaking and subsequently by a future SSO before Section 1033 can be safely effectuated. The following recommendations are aimed at increasing clarity and certainty regarding an SSO—which is a lynchpin of the open banking framework—and allowing proper time for SSO development and operationalization.

A. Clarify the process for official SSO "recognition" and ensure diverse representation and governance.

The Proposal suggests that the Bureau will provide further communications regarding the process for official recognition of an SSO and related requirements. Given the centrality of an SSO to the proposed open banking framework, however, we believe that clarity needs to be provided as soon as possible and in advance of the final rulemaking in order to avoid subsequent delays. As a threshold matter, the CFPB should develop a clear application process and timeline to recognize a standard-setting body. Decisions regarding such applications should be made public and explain why an application was approved or denied.

Additional critical areas for clarification include detailed discussion of the criteria the Bureau will use to assess an SSO, as well as confirmation that the Bureau expects that only one such SSO is necessary to accomplish the rulemaking's objectives. While the Bureau notes that diverse stakeholder participation in the governance of the SSO will be necessary, we also believe the Bureau should be more specific in its expectations. For example, the Bureau should require that the SSO leadership include a number of both small and large non-bank financial technology

companies and providers—offering products across the financial services landscape—to avoid the organization being controlled by a few traditional "dominant firms." The Bureau should also express that diversity in SSO representation should also include representative trade organizations, such as FTA, to help expand the range of viewpoints in establishing qualified industry standards.

Beyond membership and governance, the Bureau should also establish which key categories of standards should be largely finalized in order for the SSO to receive official recognition. Put differently, an SSO should not be eligible for formal recognition unless and until it has promulgated standards central to the safe and efficient implementation of the open banking framework, including around security, authorization, disclosures, and risk management. The lack of such standards would severely undermine the framework and risk security and other operational disruptions.

We recognize that there is a bit of a "chicken and egg" dynamic to how the Bureau will be able to review and recognize an SSO and the pace of its work in promulgating standards. More specifically, it is likely an SSO will need to know it is "on the right track" to receiving recognition before it can garner broader stakeholder buy-in and finalize this important work. For this reason, we believe the Bureau should implement a phased approach to full SSO recognition, whereby it meets periodically with an SSO to review its governance and standards-setting efforts and offers feedback on steps to final recognition. To this end, the Bureau might consider providing an SSO with an earlier "conditional approval" predicated on successful completion of key categories of standards that are central to the open banking framework.

B. Provide appropriate time for SSO development and link industry implementation timelines to such development.

As recognized by the Bureau, the key operational, technological, and security details of the U.S. open banking system should appropriately be placed with an SSO. Given the effective delegation of central aspects of the rulemaking to an SSO, it is imperative that the Bureau provide an appropriate and realistic timeframe for SSO development and formal recognition. As further discussed below, the Bureau should also link the commencement of broader industry implementation timelines to the formal recognition of an SSO both to ensure the safe, smooth, and consumer-centric implementation of the open banking framework, as well as to incentivize all stakeholders to complete the work and authorization of an SSO expeditiously.

With respect to an appropriate timeframe for SSO development, as noted above, the Bureau needs to communicate clear guidance and expectations well in advance of a final rulemaking. The Bureau should also engage in ongoing communication with a potential SSO organization, including through use of a "conditional approval" designation process, to allow SSO development to occur

pending a final rule. In order to ensure that all stakeholders are incentivized to form an SSO, promulgate critical standards, and receive formal Bureau recognition, FTA recommends that the Bureau grant an SSO a conditional approval by the time the final rule is issued and make explicit in a final rule that, barring unexpected challenges, an SSO will be fully approved no later than 6 months following the issuance of a final rule. This approach assumes the Bureau works with the industry in the time leading up to a final rule to ensure such a deadline can be satisfied and that a conditional approval is granted by the time the final rule is issued.

Alternatively, if the Bureau is unable to provide additional clarity around SSO requirements and the formal recognition process in advance of the final rulemaking, then the 6 month timeframe may need to be extended. It is advisable that the Bureau not rush implementation without formal qualified standards being in place in order to avoid uneven implementation of the open banking framework. Without accepted standards in place, there are significant risks of operational failures, all of which will undermine consumer trust in open banking—this would be the worst of all outcomes, even relative to the status quo.

Finally, given the centrality and importance of security, authorization, disclosures, and risk management standards, as discussed in greater detail below, we encourage the Bureau to commence broader industry implementation timelines only once an SSO has been recognized by the Bureau, along with its promulgation of key qualified industry standards. A final rule that requires the final approval of an SSO within 6 months of rule publication can prevent unnecessary delay, and render it appropriate to anchor broader implementation deadlines to such approval.

C. Clarify and expand SSO capabilities and responsibilities in order to ensure safe, reliable and consumer-centric operation of the open banking regime in the U.S.

As noted above, it is critical that the Bureau specify core standards that must be promulgated by an SSO prior to formal recognition. These standards should, at a baseline, cover security,[15] authorizations, disclosures, and risk management. A failure to develop qualified industry standards within these categories will result in uneven and potentially defective implementation of the open banking framework. It will further undermine consumer trust and adoption.

Beyond these central categories requiring standards, FTA further encourages the Bureau to specify and expand an SSO's functions in order to foster an orderly, efficient, and trusted open banking system in the U.S. An SSO could be delegated certain regulatory authorities as a Bureau

[15] It is important to note that we do not believe an SSO should promulgate a new data security standard, but rather should adopt existing standards in order to avoid further standards fragmentation.

recognized self-regulatory organization (SRO)[16] or could replicate the organizational features of entities like Nacha. Consistent with our comments above, the development of a robust SSO will require appropriate time but can also ensure safe and seamless implementation of the open banking system.

To this end, we encourage the Bureau to specify and delegate additional key functions to an SSO, including:

- Development of risk management standards that permit objective review and potential denial of access to a third party;
- The collection and maintenance of lists of third parties that are rejected by data providers based on risk management considerations;
- Identification of existing certifications, audits and other processes that confirm compliance with industry standards and/or requirements in the Bureau's final rule; and
- Maintenance of a white list of entities that meet security and other relevant standards based on appropriate certifications.

Notwithstanding the above, FTA recognizes the possibility that an SSO may not be formally recognized within the 6 month timeframe we recommended above due to unexpected circumstances. This scenario would undoubtedly generate ambiguity regarding Section 1033 implementation and operationalization, as well as create security and user-experience risks. The Bureau should accordingly take all steps to facilitate the development and recognition of an SSO, including through further guidance and regular engagement with potential SSO candidates. The Bureau may further have to consider subsequent extensions of implementation timeframes if unforeseen delays arise given the importance of an SSO to the safe and trusted launch of a formal open banking system in the U.S.

IV. Given the time, cost, and complexity of operationalizing 1033 requirements, the final rule should create a more realistic timeframe for implementation—a failure to do so could result in confusion, undermine security and trust, and lead to service interruptions that harm consumers.

As detailed in the Bureau Proposal, data providers are expected to take numerous steps to implement Section 1033 requirements, including technological integrations, the development of internal policies and procedures, the creation of consumer disclosures and engagement interfaces, and ramp-up of operational capabilities. Notably, these implementation steps can increase in

[16] Well known and established SROs with delegated regulatory authority include FINRA from the SEC and NFA from the CFTC.

complexity for larger companies that in some cases will serve as data providers and in others will be data recipients. Under both scenarios, companies will be required to dedicate substantial resources to implementation and to cover all related financial costs. Proper implementation is, of course, critical given the importance of safeguarding consumer data and ensuring a positive consumer experience necessary for building ecosystem trust.

Against this backdrop, FTA remains a steadfast champion of open banking but also recognizes the importance of avoiding hasty and unsuccessful implementation. The long-term success of open banking will begin through a successful launch—a process that will require care, compliance and operational excellence.

FTA accordingly urges the Bureau to ensure realistic implementation timeframes that focus on getting open banking "right" rather than simply out the door. To this end, we believe it is prudent to add an additional 6 months of time to each category of the Proposal's suggested implementation timeframe. As noted above, we further suggest that the Bureau begin these implementation schedules (which will now be 12 months for the largest data providers) at the time the Bureau formally recognizes an SSO, which should be no later than 6 months after the final rule is issued. Under this construct, the latest that Section 1033 implementation will begin in the marketplace is 18 months after the final rule (and potentially earlier if an SSO is recognized prior to the 6 month post-rule deadline).

We believe that the above formula best balances expediency with care and prudence. It would further incentivize the Bureau and market participants to promulgate SSO standards and recognize an SSO sooner than the 6-month post-rule deadline in order to expedite the implementation timeframes. In the event that an SSO is not recognized by the 6-month deadline, the Bureau and market participants will be negatively impacted by the potential for ambiguity and uneven implementation—a powerful incentive to get the SSO authorized and operational. This construct also aligns the Bureau and market participants in monitoring SSO development and further helps them react if there are unexpected implementation developments.

V. The concept of digital wallets is vague and undefined—the final rule should provide greater clarity regarding definitions and responsibilities, as well as provide for an extended implementation timeframe.

The Bureau's proposed coverage of "digital wallet providers" is incongruous with the Proposal's approach to facilitating the sharing of covered Reg E and Reg Z accounts and may create confusion and data integrity problems for data providers, data users, and consumers alike. The Proposed Rule enables consumers to wield their own data in a way that empowers them to obtain new or better consumer financial products or services. As discussed below, however, capturing consumer data

held by a digital wallet provider may create inefficiencies and inaccuracies that conflict with a consumer's ability to achieve these goals.

First, the Proposal covers certain Reg E and Reg Z accounts and the issuers of those accounts. This approach ensures that consumer account data is available to be shared with third parties for any variety of purposes. The Proposal goes on, however, to include "other payment facilitation providers" based on the preliminary determination "that the marginal burden of including other payment facilitation products and services would be minimal given how these providers would generally already be covered as Regulation E financial institutions."[17] The Proposal further suggests that such an approach will avoid loopholes.

We respectfully submit, however, that this analysis does not consider the confusion, unnecessary duplication, and data accuracy challenges that inclusion of other payment facilitators will introduce when such entities interact with Reg E and Reg Z accounts. In these situations, digital wallet providers do not "control or possess" Reg E or Reg Z account data; but rather, they "control or possess" limited account data only for those transactions that were conducted through the digital wallet. Pulling in digital wallet transactions is not consistent with the Proposed Rule's goal of enabling the sharing of consumer account data because digital wallet providers do not have account data to share. Put differently, except for stored value, pass-through digital wallets are merely a record of the underlying data provider's account, and that record is not related to the product being provided to the consumer. The CFPB should be laser-focused on enabling the sharing of account data and not creating multiple, potentially conflicting sources of truth in the consumer's data ecosystem. Accordingly, we suggest excluding pass-through digital wallet features from the scope of the final rule.

Second, including digital wallet providers has the potential to create confusion for consumers and data integrity challenges for users. The data in the control or possession of digital wallet providers is generally only a portion of the data associated with any covered Reg E or Reg Z account and thus the sharing of that data is necessarily incomplete, potentially misleading to any user of that data, and potentially inaccurate due to latency. A consumer who chooses to share data from a digital wallet provider as opposed to the issuer of the covered Reg E or Reg Z account may end up sharing incomplete data, which may not assist the consumer in obtaining the products or services sought. Moreover, having the same data available in multiple places presents the risk of inaccuracies due to latency. For example, a digital wallet provider may have data showing an ACH debit transaction from a covered Reg E account that has not yet processed the received ACH debit instruction.

[17] Proposal at 31.

There are accordingly a few potential definitional changes that may address the challenges described above:

- Exclude "[f]acilitation of payments from a Regulation E account or Regulation Z credit card" from the definition of covered consumer financial product or service.
    - Entities that facilitate payments have consumer data, but as discussed *infra*, the data is incomplete, confusing, and potentially inconsistent with the data that exists with the provider of the covered Reg E or Reg Z accounts and
    - Pulling in digital wallet providers does not add to the universe of data available to users and consumers-–it is all inherently redundant of data that exists elsewhere, and it will add confusion to the data ecosystem.
- Clarify that a digital wallet provider "controls or possesses" the data only when the data relates to the product that the digital wallet provider or neobank offers to the consumer. Pass-through wallets are merely a record of the underlying data provider's account, and that record is not related to the product being provided to the consumer.

Beyond these definitional clarifications, the Bureau should further consider extending the implementation timeframe for digital wallet providers to ensure final definitions for open banking purposes align with other rulemakings involving this category of providers, including through the payments company larger participant rule and FCRA amendments. Similar to our suggestions above, while FTA champions the benefits of open banking in the U.S., we think it is most important that we collectively get this "right," including by ensuring clear and consistent coverage, definitions, and regulatory expectations. Given the ill-defined and fast-evolving concept of digital wallet in financial services, we believe that definitional clarity is paramount.

VI. The Bureau should implement a number of additional amendments and clarifications to the final rule to ensure successful and consumer-centric implementation of open banking in the U.S.

A. Clarify the interplay of Section 1033 with the Bureau's proposed FCRA rulemaking and confirm that data aggregators are not de facto credit bureaus.

The Proposal raises whether certain FCRA requirements might be applicable in the context of Section 1033 implementation. The Bureau should firmly establish that consumer-permissioned data is not subject to the FCRA for two primary reasons. First, the fact that a consumer owns the data and is controlling its movement distinguishes it from the FCRA context and the risks the FCRA seeks to mitigate. The FCRA was enacted to provide greater visibility and protection to consumers when it came to information being shared about them. But consumer-permissioned

data, particularly given many of the additional protections in the proposed rule, puts the consumer in charge. Second, unlike the FCRA context, under Section 1033, it is the consumer who is permissioning the transfer of his or her information. In this way, it is more akin to a customer providing a bank statement as part of an application for a home mortgage.

Additionally, in ensuring cohesion and consistency between the Section 1033 rulemaking and the FCRA rulemaking, the Bureau should expressly state that sharing of consumer information between entities—potentially through a data aggregator—is generally outside the scope of a consumer reporting agency. Merely summarizing, or reiterating data about a consumer, even in a different format but without adding any insight or additional information, should not be considered "assembling" or "evaluating" under FCRA, particularly when it is customer-authorized. Inappropriately capturing mere transmission activity would have significant impacts for the industry and impose substantial operational costs on covered firms, particularly those who only pass information on.[18] It is accordingly imperative that the Bureau consider and clarify the interplay between its ongoing rulemakings to ensure consistency and avoid unnecessary burden.

B. Avoid overly prescriptive disclosure requirements and ensure such disclosures are not used by data providers to dissuade or discourage a consumer from seeking a personal data transfer.

FTA supports the Proposal's avoidance of prescriptive disclosure requirements in favor of principles that can help ensure consumers have access to clear information needed to make informed decisions. FTA believes that consumers should be provided with clear, plain language disclosures, including with respect to the collection, sharing and use of their personal financial information. These disclosures should not be over-engineered, overly-prescriptive, or needlessly impede the user's experience. FTA notes that existing UDAAP and related disclosure rules provide a sufficient framework within which providers can offer consumers clear disclosures.

FTA opposes the required use of model forms for some or all of the content in authorization disclosures—we accordingly support the Bureau's current principles-based approach in the Proposal. The over-engineering of disclosures can have the unintended effect of reducing the likelihood that consumers will review such disclosures or appreciate potential distinctions in disclosure language.

While overly formalistic and prescriptive disclosure requirements should be avoided, the Bureau should encourage an SSO to promulgate disclosure standards and guidelines that can ensure that

[18] *See* Financial Technology Association, *FTA Comment on the CFPB's Outline of Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights* (Jan. 25, 2023), available at https://www.ftassociation.org/wp-content/uploads/2023/01/FTA-1033-SBREFA-Comment-Letter-vF.pdf.

certain baseline information is provided to consumers. These guidelines can help all stakeholders craft appropriate disclosures tailored to their particular business model, product or service, and information sharing arrangements. SSO guidelines should further discourage data providers from using disclosures to needlessly create friction for consumers and barriers to them sharing their personal financial information. In no way should disclosures be used for anti-competitive purposes, including dissuading or discouraging a consumer from authorizing the sharing of their data.

C. Establish clear standards around the use of Tokenized Account Numbers to avoid anticompetitive behavior, the undermining of fraud models, and barriers to further innovation in business models.

The Bureau's Proposal currently allows a data provider to transmit tokenized account numbers (TANs) in lieu of non-tokenized account and routing numbers, ostensibly to reduce fraud risks. The Proposal offers no discussion of the use of TANs, but does ask for public comment, including with respect to the impact on consumers and potential need for standards.

FTA urges the Bureau to proceed with caution in allowing the use of TANs absent standards issued by a recognized SSO. While TANs may be used by some providers to mitigate certain fraud risks, they also may serve as a barrier to consumers accessing basic account information and to other providers working to counter fraud and other forms of financial crime. Account and routing information are critical forms of identifying information, and their obfuscation accordingly undermines many common anti-fraud practices. Security of information is better protected through sound API-security standards rather than through standardless tokenization.

Indeed, blanket Bureau permission to use TANs hands excessive power to data providers to restrict applications in anticompetitive ways. It further can chill consumer-centric innovation, including novel payments use-cases, such as account-to-account payment methods.

Rather than the current approach in the Proposal, FTA urges the Bureau to delegate discussion and standards regarding TANs to a recognized SSO, where market participants can ensure an optimal balance between security and maximizing the value of the open banking framework. Consumers should not be blocked from basic identifying account information and third-parties should be able to use such information to help counter fraud and innovate with pro-consumer product offerings.

* * *

FTA appreciates the Bureau's consideration of its comments. We believe that properly implemented, open banking in the United States can drive exciting pro-consumer innovation and competition in financial services. While we are all eager to see this new reality, we equally believe in getting this right in order to build consumer trust and maximize the potential of Section 1033. Our feedback is intended to focus on the consumer and the safeguarding of consumer interests. To this end, we would be happy to discuss the issues raised in this letter further. Please contact the undersigned at penny@ftassociation.org for additional information.

Sincerely,

Penny Lee
President and Chief Executive Officer
Financial Technology Association

EXHIBIT B

PLAID

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

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

Re: Required Rulemaking on Personal Financial Data Rights

Director Chopra and Bureau Staff,

Plaid appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (the "Bureau's") Notice of Proposed Rulemaking ("NPRM" or "proposal" or "proposed rule") for the Required Rulemaking on Personal Financial Data Rights.

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

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

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

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

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

Consumer demand, technological innovation, and industry dynamics (both competition and collaboration) have led to significant advances in the United States open finance ecosystem, with hundreds of millions of consumers able to access and share their own financial information so that they can easily use their chosen services. The rulemaking is critical to consumers fully realizing the consumer empowerment goal that underpins § 1033, and to achieving a fair, transparent, and competitive financial services marketplace. It will propel the financial services industry to better serve consumers by bolstering the *consumer right* to access and share their own financial data, and mitigate privacy, security, and anticompetitive risks. In particular, the NPRM's emphasis on fair and free consumer and third party access to data providers' developer interfaces, effective and transparent authorization managed by third parties, and the role Standard Setting Organizations ("SSO") can play in implementing data access at a technical level will, if finalized, dramatically improve data portability, competition, and consumer outcomes.

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

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

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

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

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

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

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

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

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

PLAID

Table Of Contents

I. Plaid's Role In The Open Finance Ecosystem

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

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

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

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

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

II. Definitions (§ 1033.131)

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

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

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

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

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

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

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

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

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

[4] 12 U.S.C. § 5481(4).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

D. Recommendations Regarding Specific Data Types

Identity Data

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

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

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

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

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

Social Security And Driver's License Numbers

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

Tokenized Account Number

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Credit Card Payment Information

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

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

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

Account Terms And Conditions

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

Proprietary Algorithms

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

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

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

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

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

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

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

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

---

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

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

[29] *Id.* at 74820.

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Specifically, Plaid proposes the following changes:

§ 1033.351 Policies and procedures.

* * * * *

(b) Policies and procedures for making covered data available. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:

* * * * *

(2) *Denials of developer interface access*. When a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider:

(i) Creates a record explaining the basis for denial; and

(ii) Communicates to the third party, electronically or in writing, **its general policies and procedures governing the denial of interface access,** the **known, specific security risk(s) or other** reason(s) **relied on as a basis** for the denial**, and information sufficient to satisfy the data provider's burden of demonstrating the reasonableness of its denial, including that such denial is based on a known security risk management concern that is likely to cause substantial injury to consumers. The communication must disclose whether requests from other third parties have included the same specific risks and whether those requests were granted or denied.** ~~and that the~~ **The** communication **must** occur as quickly as is practicable.

(3) *Denials of information requests*. When a data provider denies a request for information pursuant to § 1033.331, the data provider:

(i) Creates a record explaining the basis for the denial; and

(ii) Communicates to the consumer or third party, electronically or in writing, the type(s) of information denied ~~and~~**, its general policies and procedures governing the denial of information requests,** the **specific** reason(s) for the denial, **a description of the specific risk(s) involved or the specific information that the consumer or third party failed to provide, and an explanation of why the denial was justified. The communication must also disclose whether**

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

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

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

* * * * *

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

* * * * *

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

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

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

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

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

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

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

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

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

C. The Bureau Should Prescribe Additional Limits On Access Caps

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PLAID

To address these limitations, we recommend the final rule:

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

VI. Responding To Requests For Information (§ 1033.331)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

VII. Authorized Third Parties (Subpart D)

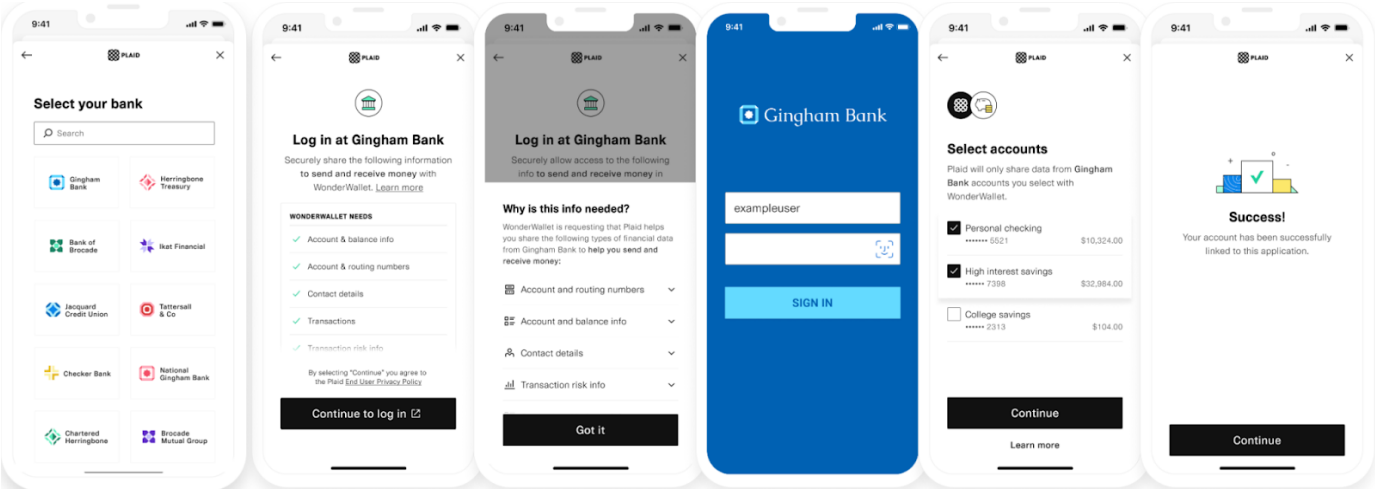
The authorization procedures proposed in the NPRM will help ensure that consumers understand and meaningfully consent when authorizing third parties to access financial data on their behalf. They are sufficiently specific for industry participants to understand their obligations, and the Bureau's principle-based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

PLAID

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

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

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



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

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

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

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

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

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

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

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

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

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

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

[58] Cal. Civ. Code § 1798.140(h).

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

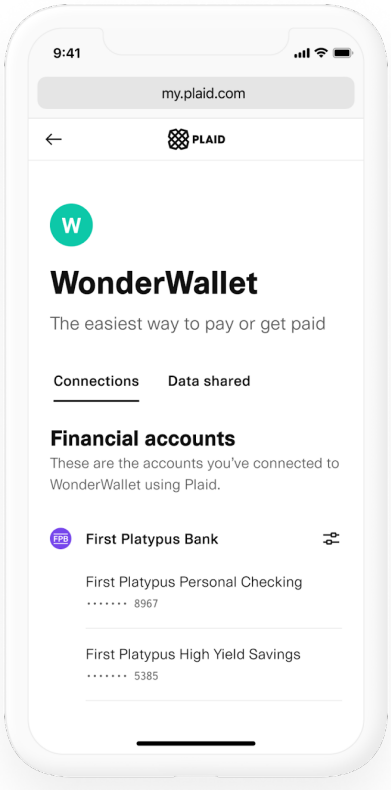
[60] For certain use cases, such as payments on a merchant's website, the covered data is used to enable payment for the product or service purchased from the merchant, rather than for the product or service itself. In such circumstances, it is unclear whether the NPRM requires the merchant to describe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

PLAID

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

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

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

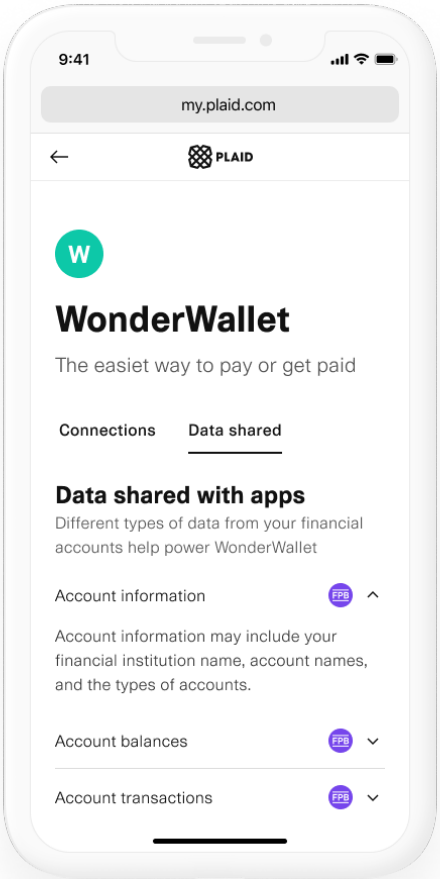


[61] Available at my.plaid.com.

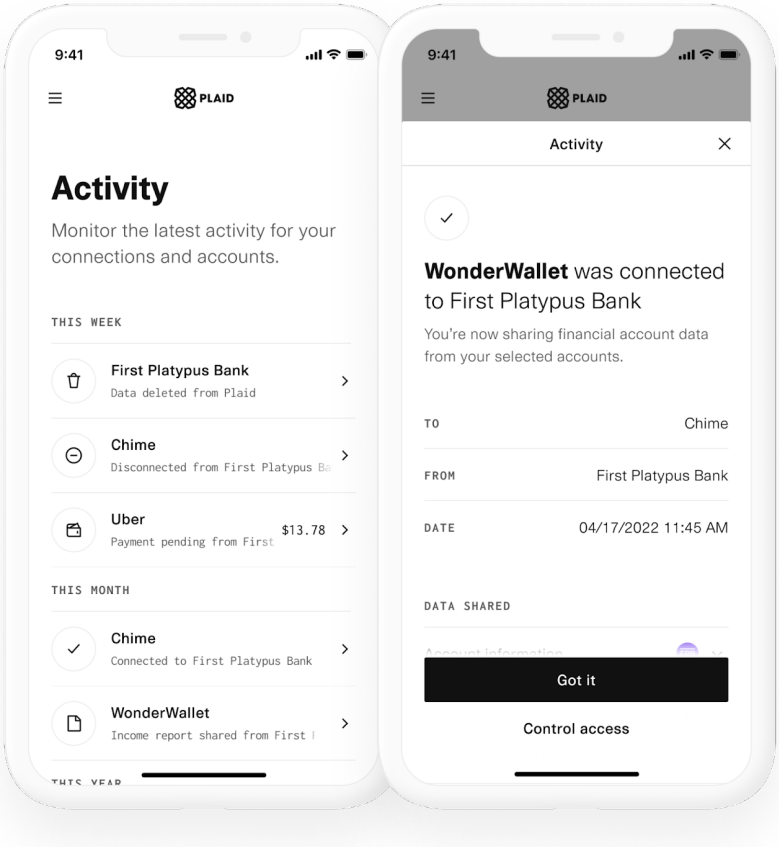
[62] Plaid offers this example only to demonstrate that the technology for data access platforms to support reauthorization exists. Although some identity verification process is necessary, consumers should not necessarily be required to create any sort of account in order to manage their reauthorization.

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

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



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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VIII. Third Party Obligations (§ 1033.421)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[82] *Id.* at 74855.

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

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

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

- **Require third parties to allow consumers to opt-out of secondary uses compatible with the primary purpose**: For uses that extend beyond the "reasonably necessary" standard, but which are still compatible with the consumer's primary purpose in sharing data, the CFPB should permit consumers the ability to opt out. Such compatible uses include, for example, marketing or advertising products or services provided by the same company with which the consumer is already a customer, like a checking account provider also offering a savings account. This type of ongoing commercial relationship between a consumer and a business is common across all industries, and is explicitly permitted, with the right to opt out, in jurisdictions such as Canada, the European Union, and Australia.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chart Demonstrating The Incongruent Treatment Of The Same Covered Data

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

IX. Remaining Considerations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

X. Conclusion

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

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

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

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

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

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

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

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

Best regards,

John Pitts
Head of Policy
Plaid

Data Appendix

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

EXHIBIT C

Submitted via electronic submission at https://www.regulations.gov

December 29, 2023

Comment Intake—FINANCIAL DATA RIGHTS
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Ribbit Capital Comment on CFPB's Proposed Rulemaking on Personal Financial Data Rights
(Docket No. CFPB-2023-0052; RIN 3170-AA78)

Ribbit Capital appreciates the opportunity to provide comments on the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") proposed rulemaking on personal financial data rights (the "Proposal"). We commend the Bureau on its work to date and support this effort to develop a pro-consumer open banking system in the United States.

Ribbit Capital ("Ribbit") is a global investment firm focused on the intersection of financial services and technology. Founded in 2012, Ribbit Capital's mission is to change the world of finance by providing capital and guidance to visionary financial services entrepreneurs around the world. Ribbit's portfolio consists of more than 130 private and public company investments across six continents and a multitude of sectors within financial services, including payments, personal finance, investments and wealth, lending, insurance, cryptoassets, financial infrastructure, and financial software.

As Director Chopra repeatedly stated in making open banking a top Bureau priority, implementation of Dodd Frank Section 1033 holds substantial promise in encouraging competition and providing consumers options to choose money that works for them. This means not only improving access to financial products today, but fostering the development of more tailored and holistic services in the future.[1] Critical to this promise is the final rule's recognition of the importance of data and the ability to use it to build personalized, automated, and multifaceted services. Yet the Proposal's current approach to secondary use of consumer data calls for blanket restrictions on such use,[2] which would severely undermine the success of open banking in this country and rollback the potential for pro-consumer innovation and competition.

---

[1] *See* Director Rohit Chopra, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct.19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/.

[2] See Consumer Financial Protection Bureau Proposal, *Required Rulemaking on Personal Financial Data Rights* (Docket No. CFPB-2023-0052), available at https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf ("Use of covered data that is not reasonably necessary to provide the consumer's requested product or service—i.e., secondary uses—would not be permitted as part of the third party's authorization to access the consumer's covered data.").

Because the future of financial services is dependent on safe, secure, and consented use of data, this comment letter will focus exclusively on why secondary use should be broadly permitted, subject to the reasonable and appropriate consumer protections included throughout the Proposal and existing privacy law. Indeed, the Bureau should ensure that Section 1033 implementation satisfies consumer interests and preferences, especially since 77% of consumers expressed in a recent survey that they would value personalized financial advice from their financial institution and 94% would want their financial data to be used to let them know of a better deal on a product.[3] This approach to secondary use would be consistent with even the most stringent domestic and international data use frameworks. It would also ensure that Section 1033 implementation properly serves consumers by unlocking the full potential of open banking and preserving a competitive ecosystem between those subject to Section 1033 and the majority of industries and firms to which it does not apply. Our feedback and recommendations below detail the following points:

A. Broad and Responsible Use of Consumer Permissioned Data is Pro-Consumer and Pro-Competition, and Should be Fostered by Section 1033.
B. Consumers Routinely Express Their Preferences for Tailored Products and Holistic and Embedded Services, which Necessitates Secondary Use of Consumer Data.
C. Artificial Intelligence Model Development Relies on Access to Quality Data, which is Especially Important for Smaller Firms, and U.S. Economic Competitiveness Relies on Such Model Development.
D. Consistent with Leading Domestic and International Data Privacy Regimes, Reasonable Consumer Safeguards Can Mitigate Risks Associated with Secondary Data Use Without Punitive Blanket Restrictions.

The CFPB Should Amend the Proposal's Punitive, Blanket Prohibitions on Secondary Data Use to Avoid Harming Consumers, Competition, and Competitiveness in U.S. Financial Services.

For the reasons detailed below, the Bureau should avoid blanket prohibitions on secondary data use in favor of a pro-consumer framework that recognizes that the future of financial services development is predicated on the safe, responsible, and permissioned use of consumer data to best serve the needs of the consumer.

A. Broad and Responsible Use of Consumer Permissioned Data is Pro-Consumer and Pro-Competition, and Should be Fostered by Section 1033.

Data will create the foundation for the next wave of financial services innovation to advance how individuals, small businesses, and our broader economy access, manage, and use money. With advancements in AI, we now expect to have the ability to contextualize and make better sense of data in order to drive actionable insights, predictions, and conclusions. In-line with the spirit of

[3] MX, *The Ultimate Guide to Open Banking*, available at https://www.mx.com/assets/resources/ult-guides/ultimate-guide-to-open-banking.pdf.

Director Chopra's remarks in releasing the proposed rule,[4] having the ability to contextualize data results from access to complete and holistic data. This allows for better analysis and understanding of the financial profile and needs of the consumer.

Highly-relevant and high-quality data sets enable financial technology ("fintech") firms to build the types of personalized and automated products that allow consumers to receive a more tailored and empowering financial experience. Much of this development derives not only from data received by the provider, but also from data generated from the consumer's interactions with an app, including both the consumer's feedback and ultimate decision making. The fintech firm can subsequently use this data to develop new, beneficial applications or use cases capable of better serving the consumer's needs.

Additionally, a company may also use collected data for a broad range of secondary uses, including product research, model development, and ongoing innovation and iteration. Responsible secondary use of this data has allowed for many of the advances we have seen in the marketplace to date, and coupled with new technologies, will allow for the ongoing development of multifaceted financial services. While smartphones have effectively "put a bank in everyone's pocket," AI-driven advances coupled with access to financial data holds promise in putting a "*banker* in everyone's pocket," which can yield better financial information, options, and consumer choice and decision-making.[5] The following is a representative set of examples that illustrate pro-consumer secondary data uses:

1. Personalized and actionable financial tools, from investing to saving.

A substantial amount of innovation is currently underway that allows for personalized financial advice for consumers, including with respect to budgets, repayment of debt, and investments. These services rely on consumer-permissioned financial data to provide tailored advice, as well as the development of multifaceted products that may address a range of financial needs. But this may only be possible with secondary use permissions. This is because a consumer may permission data to a company for a primary use case such as help with budgeting, but may then also benefit from ideas derived from a holistic assessment of the consumer's personalized financial data on where to invest to get the highest yield or find a lower interest rate loan. Under the Proposal's current prohibitions and narrow definition of primary use,[6] a consumer would be required constantly to

---

[4] *See* Director Rohit Chopra, *Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule* (Oct.19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/ ("In addition, bringing in your personal financial ledger to a new provider will let them consider your full financial history when offering you a loan, instead of relying on a summary from the credit reporting conglomerates.").

[5] *See* An Interview with David Vélez, *With AI, Nubank is pioneering a future of inclusive, personalized financial services* (Oct. 26, 2023), available at https://building.nubank.com.br/with-ai-nubank-is-pioneering-a-future-of-inclusive-personalized-financial-services/.

[6] The Proposal's definition of primary use appears to be connected to the notion of a "core function," which provides little flexibility for a third-party to offer additional consumer-desired products or services. This narrow definition and blanket preclusion of secondary use are inconsistent with the nature of financial services development. *See* Proposal, at 144 ("To

authorize a third-party provider's access to current financial data for each new use case. This would become especially cumbersome where ambiguity regarding when a use case shifts from primary to secondary results in the service provider taking a cautious approach by repeatedly seeking new authorization to avoid potentially violating the rule.

For example, pro-consumer fintech innovators may provide users access to their credit scores, but also use permissioned consumer financial data to offer personalized financial advice and budgeting tools. The service may offer detailed insights into factors affecting the user's credit score, such as credit utilization and payment history, and offer personalized tips and recommendations to help users improve their creditworthiness. The Proposal suggests that such personalized tips and recommendations regarding creditworthiness may be the "primary use" of the consumer's data.[7] But, based on a user's credit profile and financial goals, the platform may further suggest certain credit cards, loans, or other financial products that align with their creditworthiness. This potentially secondary use of data could be precluded under the current rule, at a considerable cost in fees or interest to the consumer, especially if it is considered to be marketing or cross-selling. In fact, research has shown that fintech services have already saved $360 a year in interest and bank fees for 75 percent of Americans earning less than $100,000.[8]

Another example would be next-generation financial advisory tools that break down data silos in order to provide individuals with a holistic view of their financial profile and make that data readily available to financial professionals for services like tax preparation or for pre-populating an application to secure a new financial product. By aggregating often disparate information into one place, these business models help individuals make more informed financial decisions and secure desired products and services. They can further help individuals find ways to optimize financial performance, including, for example, by identifying external deposit accounts offering substantially higher interest rates on deposit balances. In this scenario, advice and recommendations regarding such higher-yielding accounts may be considered a secondary use of consumer financial data and therefore precluded by the Proposal.[9]

As these examples demonstrate, the Bureau's current prohibitions on secondary use and narrow definition of primary use would significantly slow or preclude development of these services, despite the clear benefit to consumers. To this end, the Small Business Review Panel referenced in

---

avoid circumvention of that standard, the CFPB will treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit. For example, the scope of the product or service is not defined by disclosures, which could be used to create technical loopholes by expanding the scope of the product or service the consumer requested to include any activity the company chooses that would often benefit the third party and not the consumer."). At the very least, the Bureau should clarify that the core function can be a broad category of financial services advice, which includes multifaceted and multidimensional product and service offerings.

[7] *See id.*

[8] See The Harris Poll Report, *Fintech Effect | Consumer impact and the future of finance,* available at: https://plaid.com/the-fintech-effect-2020-consumer-report/#main-content

[9] Given the importance of broad access to consumer financial data, it is important to emphasize that the Bureau should move quickly to expand the categories of covered accounts and data subject to Section 1033. Indeed, the promise of open banking and the evolution of financial services will rely on the seamless flow of permissioned financial data. For this reason, we support including EBT data in this rulemaking and prompt expansion of Section 1033 to broader sources of financial data.

the Proposal presented evidence that market-driven consumer data access has already produced benefits for consumers, many of which likely derive from various secondary uses of data.[10] These include the offerings noted above, as well as other forms of personalized communications and data analytics that allow for personalized product offerings known to build consumer satisfaction and loyalty.[11] Based on this context—and the clear benefits that have accrued to consumers from fintech product development—it would be to the consumer's detriment to impose broad secondary use restrictions.

2. **Improved and expanded product offerings through enhanced credit scoring and risk assessment**.

Fintechs, financial institutions, and insurance providers are increasingly able to use broad sets of transactional and cash flow history, payment behavior, and alternative data to assess consumer's credit risk.[12] While this data can be utilized for a one-time product offering, it can also help create a longer-term more accurate risk assessment of an individual, advance new product development, lower costs of acquiring such data, and help a financial services provider offer subsequent, improved credit products to a consumer. As written, however, it's unclear whether the rule would preclude these pro-consumer developments.

For example, in the case of credit decisions, lenders have historically used rule-based or logistic-regression models, relying on a limited set of criteria from credit bureau reports and credit scores to determine if a customer qualifies for a loan. Because this traditional credit information system focuses primarily on historical credit use, it only provides a partial assessment of an applicant's finances, often leaving out a large segment of consumers and small businesses with no formal credit history. As a recent CFPB blog post noted, "[c]redit scores may in part reflect the unequal circumstances that people face, and there are ongoing debates regarding equity and fairness."[13]

Static credit bureau information or credit scores may be the type that can be "authorized" in a single pull—or as part of primary use in making a credit decision. This may not be the case, however, for

---

[10] See Consumer Fin. Prot. Bureau, *Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration of the Required Rulemaking on Personal Financial Data Rights*, p. 3, footnote 7, (Mar. 30, 2023), https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf (The Panel cited research showing that in 2019, 46 percent of digitally active U.S. consumers were "fintech adopters," remarking that "to the extent such opting for improved offerings is catalyzed by consumer-authorized data access, competition in consumer finance appears to benefit from the ability of consumers to permit third parties to directly access their personal financial data.").

[11] *See generally*, Akshay Chhabra and Simon Williams, McKinsey, *Fusing data and design to supercharge innovation—in products and processes* (Apr. 4, 2019), available at https://www.mckinsey.com/capabilities/quantumblack/our-insights/fusing-data-and-design-to-supercharge-innovation-in-products-and-processes.

[12] *See* McKinsey, *Building the AI Bank of the Future* (May 2021), p. 32, available at: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/building%20the%20ai%20bank%20of%20the%20future/building-the-ai-bank-of-the-future.pdf.

[13] Alexei Alexandrov, Alyssa Brown, and Samyak Jain, CFPB Blog, *Looking at credit scores only tells part of the story – cashflow data may tell another part* (July 26, 2023), available at https://www.consumerfinance.gov/about-us/blog/credit-scores-only-tells-part-of-the-story-cashflow-data/.

more dynamic models and data sets, which can provide ongoing, near real-time assessments based on a dynamic view of a consumer's financial data.

To this end, a study from FinRegLab found that cash-flow metrics used by certain lenders were generally as predictive as traditional metrics, and were found to serve consumers who may have been historically excluded from accessing credit.[14] Additionally, the adoption of more advanced analytical models that use both structured and unstructured data, allow lenders to predict the likelihood of loan defaults for unbanked and underbanked consumers and small businesses. As further discussed below, these models require high-quality, real-world training data to develop, which necessitates secondary use of a variety of data sets a lender may receive in different contexts.

Relatedly, the diversity of data required to test and develop next-generation underwriting models is inconsistent with the idea under Section 1033 that a third-party can only use a consumer's data that is "reasonably necessary" to the primary use, render a credit decision, and then delete that data—this precludes further model development, ongoing credit-risk assessment, and/or opportunities to improve the offerings presented to the consumer.

To this end, the "reasonably necessary" standard is also overly restrictive, and should be broadened to a standard such as "reasonably related" in order to provide firms with the ability to pursue consumer-beneficial product development and personalization. If the innovators who developed cash-flow based underwriting models had been required to only use data that was "reasonably necessary" to underwrite, they may not have been able to experiment and iterate with new data sets in an effort to find better ways to underwrite. Such restrictive data collection standards work to lock-in the status quo and prevent iteration that results in the development of new models that benefit consumers, such as those predicated on cash-flow underwriting.

3. The next wave of use cases will embed financial tools that provide a holistic view of a consumer's financial health and wealthness and optimize financial outcomes.

The above sections of this letter detailed how fintechs have used data for secondary purposes to improve consumer offerings. The next wave of fintech innovation, powered by advancements in AI, can turn this data into even more powerful solutions. As the Bureau finalizes its rulemaking, it is critical to consider the constantly evolving nature of financial services innovation in order to avoid the unintended consequences of impeding pro-consumer developments.

With recent advances in AI, including large language models capable of producing text and related responses and content based on probabilistic reasoning, fintechs can develop highly relevant, tailored, and automated solutions. These highly personalized models can suggest that one consumer invest excess savings in appropriate investment products, while suggesting another consumer use such excess savings to pay off high-cost debt. For example, these services could appropriately

[14] See FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (July 2019), p. 7, available at: https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

allocate a paycheck to ensure that the consumer first paid off higher APR credit card debt, then lower APR student loan debt, and then suggest how to allocate the rest of the money to retirement or savings accounts to guarantee the best tax benefits and return on investment. They could also recommend that a consumer may be eligible for a government benefit, or align bill payment due dates with incoming cash flows.

While some can afford to take advantage of such highly personalized financial advice and specific investment, tax, insurance, and debt strategies, the majority lack access to these services. This use of AI coupled with consumer financial data sets the stage for empowering consumers with the "banker in your pocket" referenced at the outset of this letter. Personalized financial advice and services for all is not a future dream, but rather a current focus for firms that recommend consumers from choosing poor financial decisions, including reliance on payday loans, high-rate credit products, and suboptimal management of cash and savings. The Wall Street Journal found that since 2019, Americans have lost out on a collective $291B in interest by keeping their savings in the biggest banks - indicating that there is indeed a need for these services.[15]

AI coupled with embedded finance will further enable consumers to access desired products and services seamlessly alongside the financial services they require within a unified experience or along a shared customer journey. Many innovators, including banks, fintechs, and third-party service providers, have invested resources to develop the necessary capabilities for integrating financial services into non-financial offerings. For example, at the checkout point embedded in a digital marketplace, AI can provide recommendations for the most suitable payment card for a transaction to maximize reward points or other benefits. It can also automatically convert the transaction into an installment loan if it's projected to deplete the user's available balance below a predefined threshold.[16]

It will be notably harder, if not impossible, however, to build these next generation models if—as the proposed rule proscribes—entities cannot use permissioned data to develop new offerings, or access data that is not specifically tied to a primary use case. This outcome is even more troubling given that consumers commonly desire these new services, but will be blocked by the rule or will be forced into a never-ending loop of new data authorizations.

B. Consumers Routinely Express Their Preference for Tailored Products and Marketing, which Necessitates Secondary Use of Consumer Data.

---

[15] Dion Rabouin, Wall Street Journal, Ditching Big Banks Could Have Saved Consumers $42B More in Interest (Jan 6, 2023), available at https://www.wsj.com/story/ditching-big-banks-could-have-saved-americans-42-billion-more-in-interest-24cf979b

[16] Responsible innovators are already shifting to embed customer journeys into partner ecosystems and platforms, allowing them to engage customers at the point of end use and in the process leverage the partners' data and channel platform to increase higher engagement and usage. *See* McKinsey (May 2021), p. 12; *see also* Deloitte, *The Ecosystem Imperative: Embedded Finance*, (2023), p. 17, available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance-transformation/us-the-ecosystem-imperative--embedded-finance.pdf.

Numerous consumer surveys and studies underscore the increasing significance of personalized interactions within the financial services sector. McKinsey's research found that a significant 71 percent of consumers now anticipate personalized interactions and 76 percent express frustration when they encounter a lack of personalization.[17] Personalization includes a desire by consumers to receive tailored and personalized communications.[18] Similarly, a recent survey of consumers found that 77 percent would value personalized financial advice from their financial institution and 94 percent would want their financial data to be used by their provider to let them know of a better deal on a product.[19] This underscores the pivotal role of personalization in bolstering customer satisfaction and engagement.

Furthermore, a study by Forrester Consulting found that 50 percent of banking customers express a desire for banks to adopt a more proactive stance in furnishing pertinent financial information and guidance. An even more substantial 65 percent of respondents believe that banks should "make it easier for consumers" to find and shop for financial products.[20] These point to the desire from consumers for financial services providers to be more proactive in offering relevant financial information and advice through smart personalization strategies.[21]

Additionally, increased economic pressures on households in the post-pandemic era is driving consumers (70 percent) to their financial institutions in search of personalized financial advice and help with savings.[22] Consumers often benefit from personalized nudges in their personal financial management tools, and many are willing to provide their personal data for additional benefits and services. Notably, this aligns with the Organization for Economic Cooperation and Development's (OECD) observations regarding consumers' willingness to share more data in exchange for "priority services, pricing benefits, [and] more personalized products," particularly among the younger and digitally savvy demographic.[23]

These collective insights highlight the importance of personalization in effectively meeting consumers' expectations and desire for proactive financial information and advice. Absent clear

---

[17] *See* McKinsey, *The value of getting personalization right—or wrong—is multiplying*, (November 12, 2021), available at: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying.

[18] Adlucent, *71% of Consumers Prefer Personalized Ads,* available at https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/#:~:text=57%25%20say%20they%20would%20click,looking%20to%20buy%20a%20product.

[19] MX, *The Ultimate Guide to Open Banking*, available at https://www.mx.com/assets/resources/ult-guides/ultimate-guide-to-open-banking.pdf; see also J.D. Power's "U.S. Retail Banking Satisfaction Study" highlighted that 78 percent of banking consumers expressed an expectation for personalized assistance.

[20] See Forrester Consulting on behalf of Blend, How Banks Can Unlock Quick Wins And Lasting Benefits Through Smart Personalization, March 2022, https://blend.com/ebooks-infographics-guides/thought-leadership/forrester-personalization/.

[21] Also see PWC 2021 Digital Banking Consumer Survey, available at: https://www.pwc.com/us/en/industries/financial-services/library/digital-banking-consumer-survey.html.

[22] See Forrester Consulting in partnership with IPSOS, "Sopra Banking Survey" (March 2023), https://fintechmagazine.com/articles/banking-customers-want-more-personalised-financial-advice.

[23] *See* OECD (2020), Personal Data Use in Financial Services and the Role of Financial Education: A ConsumerCentric Analysis, p. 20. available at: https://www.oecd.org/finance/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf.

evidence of consumer harm, it is therefore anti-consumer to preclude product tailoring and personalized experiences offered through secondary data use.

C. Artificial Intelligence Model Development Relies on Access to Quality Data, which is Especially Important for Smaller Firms, and U.S. Economic Competitiveness Relies on Such Model Development.

As discussed earlier, advances in AI hold tremendous promise in improving the quality of financial services in the United States and further enhancing the competitiveness of the US economy on a global stage. Indeed, the recent White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence calls for the safe and responsible development of AI given the technology's potential "to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure."[24]

The safe and responsible development of AI relies on access to high-quality data sets used to train models.[25] The importance of this requirement is heightened in the context of smaller firms and startups, which may lack access to such data sets relative to larger incumbents with established customer bases. It will also impact companies that primarily rely on Section 1033 data as compared to companies and banks that create data in direct interaction with a consumer. Notably, the Proposal's prohibition on secondary use, including in the AI model development context, would create a fragmented and two-tiered regulatory structure around financial data. Entities that directly generate data from consumers would be able to use that data for secondary purposes under all other data privacy regulations (as discussed further below in greater detail), while those receiving Section 1033 data would be prohibited.

In the financial services context, the use of data for model development purposes will almost always be a secondary use and is intrinsic to new model and product development. A ban on secondary use of financial data for this purpose would therefore severely undermine AI development in financial services and could result in the purchasing of datasets to train these models outside of Section 1033 or the use of lower-quality data sources. As noted above, the impact will accordingly be most severe on smaller entities, including fintechs and smaller banks, that are building products reliant on consumer-permissioned data and do not have access to large pools of direct consumer data required for AI model development. This will mean that entities with large customer bases will have a substantial competitive advantage in developing next generation AI-based financial services products and services because of their direct access to consumer data that flows through their existing consumer relationship.

---

[24] The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, (October 30, 2023), Articles 5.2, and 7.3., available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[25] *See* McKinsey, *Building the AI Bank of the Future* (May 2021), p. 32, available at: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/building%20the%20ai%20bank%20of%20the%20future/building-the-ai-bank-of-the-future.pdf.

To the extent that the CFPB has concerns regarding consumer privacy, a simple solution would be permitting broad secondary use by a provider when data is de-identified. De-identified and anonymized data are commonly used by AI model developers to build, test, and refine such models.[26] Additionally, the Small Business Review Panel referenced in the Proposal strongly encouraged the CFPB to explore alternatives that would allow for the utilization of data, including de-identified or anonymized data, to enhance product maintenance or improvements, provided that suitable consumer safeguards are implemented. The Panel also proposed that the CFPB assess opportunities for granting flexibility to third parties while simultaneously upholding its core consumer protection objectives.[27]

To this end, if there are specific secondary uses where evidence shows negative consumer impact, then it would be appropriate to identify those situations and place reasonable limitations on such activity. However, we encourage the CFPB to consider the effects of bans on activities, including on competition in financial services and technology, writ large. Based on the consumer surveys discussed above, however, when it is clear that product innovation is desired by consumers and when consumer data is required to develop AI technologies meant to serve that objective, then secondary use restrictions are not appropriate. Concerns regarding data privacy in this context should be readily mitigated by permitting use of de-identified data.

D. Consistent with Leading Domestic and International Data Privacy Regimes, Reasonable Consumer Safeguards Can Mitigate Risks Associated with Secondary Data Use Without Punitive Blanket Restrictions.

The transparency, express informed consent, revocation, and annual reauthorization requirements in the Proposal serve to address reasonable consumer protection concerns in a way that is aligned with existing strong data privacy laws. These are important consumer protections that will benefit consumers. However, the Proposal's secondary use restrictions are an outlier when compared to recent prevailing global and domestic data privacy rules, norms, and practices designed to protect consumers and will result in the numerous consumer and competition harms outlined above.

For example, internationally recognized data privacy regimes, such as the European Union General Data Protection Regulation (GDPR), take a vastly different approach than that proposed by the Bureau. Rather than imposing bans on secondary data use, these regulations prioritize the principles such of transparency, consent, and data protection. Under the GDPR, organizations are required to inform individuals about the purposes of data processing and seek consent where

---

[26] Deloitte Report Preserving Privacy in AI applications through anonymization of sensitive data, December 2022, available at https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Deloitte_Trustworthy%20AI%20_Data%20Anonymization_Feb2022.pdf; Mastercard blog, "How Anonymized and aggregated transactional data powers new AI models" https://b2b.mastercard.com/news-and-insights/blog/how-anonymized-and-aggregated-transaction-data-powers-new-ai-models/.

[27] See Consumer Fin. Prot. Bureau, Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration of the Required Rulemaking on Personal Financial Data Rights, at 30-31 (Mar. 30, 2023), https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf.

applicable. This approach ensures that consumers are well-informed and can exercise control over how their data is used.[28]

Similarly, the United States' California Consumer Privacy Act (CCPA) does not prohibit secondary data use, but rather empowers consumers to opt out of the sale of their personal information. Moreover, it grants individuals the right to understand what personal information is being collected about them and for what purposes. This approach promotes transparency and individual autonomy without resorting to blanket prohibitions.[29]

Furthermore, the Singapore Personal Data Protection Act (PDPA) does not ban secondary data use, but rather also relies on well-understood concepts of informed consent. To this end, it mandates organizations to obtain consent or rely on other lawful bases when processing personal data. This encourages data controllers to offer clear and easily accessible information about their data processing practices.

Leaning into the Proposal's existing protections to adopt an approach more aligned with established global and domestic data privacy practices, characterized by transparency, informed consent, and individual control, would better serve the interests of consumers without undermining the full potential of open banking. It would also avoid a scenario where only data collected under Section 1033 is treated differently than under all other data privacy regimes, which will accordingly place third-parties reliant on Section 1033 data at a substantial competitive disadvantage—these firms will frequently include smaller companies and startups seeking to compete with incumbents. We accordingly encourage the Bureau to emphasize the importance of clear disclosure and properly informed consumer consent as the right way to safeguard consumer interests, while also ensuring a framework for consistent and responsible data handling in our evolving digital landscape.

***

Ribbit looks forward to a future of better money for consumers, one in which consumers have access to the tools that holistically understand their financial lives and can help them make the best financial decisions. We agree with the Bureau on the importance and value of consumer financial data and believe it should be used to deliver value back to the consumer by improving financial access, choice and opportunity. The best way to ensure that value is received by consumers through Section 1033 implementation is by ensuring that secondary use of the consumer's financial data is permitted in a way that will unlock further financial services transformation. Indeed, over the past ten years, fintechs have emerged to compete with traditional banks and to help eliminate unfair consumer practices—they are now positioned for the next wave of financial services development, a

[28] *See* European Union General Data Protection Regulation (GDPR) 2016/679, Articles 5(1)(b), 6(4), 9, 25, and 89(1), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1807-1-1. *See* also European Commission's website Q&A, *Can we Use Data for Another Purpose*, available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en.

[29] *See* California Consumer Privacy Act (CCPA), Sections 1798.115.(d), 1798.120(a) and 1798.120(b), 1798.140(e)(6), available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

wave where every consumer will have access to advice and services previously only available to those with a personal banker on speed dial. Section 1033 provides the Bureau and the financial services industry with the opportunity now to make this vision a reality.

Sincerely,

Katie Suskind

Katie Suskind
Ribbit Capital

EXHIBIT D

stripe

December 27, 2023

Via email to 2023-NPRM-Data-Rights@cfpb.gov

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

Re: Stripe, Inc. comments on the CFPB's Proposed Rule under section 1033 of the Dodd-Frank Act (Docket No. CFPB– 2023–0052)

To Whom It May Concern:

Stripe, Inc. appreciates the opportunity to comment on the Proposed Rule (Proposal) that the Consumer Financial Protection Bureau (CFPB) published as part of its efforts to implement section 1033 of the Dodd-Frank Act (Section 1033). As stated in our earlier comment on the Outline of Proposals and Alternatives Under Consideration (SBREFA Comment),[1] Stripe believes that the CFPB's Section 1033 rule will be an important catalyst for competition by empowering consumers to choose products and services that best meet their financial needs.

As anticipated, the CFPB's Proposal establishes a legal right for consumers to access and share their data, and requires data providers to build dedicated application programming interfaces (APIs) to make data available to consumer-permissioned third parties. Given the complicated market interests at stake, and the inherent difficulty of regulating technical processes in a fast-developing marketplace, Stripe is grateful for the CFPB's commitment to protect fair competition as it advances consumers' rights under Section 1033.

Stripe is a technology company that builds economic infrastructure for businesses to transact on the Internet. Millions of businesses around the world use our software and tools to accept payments and manage their businesses online. In our decade of existence, we have been focused on making payments more efficient and inclusive for those businesses and their consumers. In

[1] Stripe Comment on Financial Data Rights SBREFA Outline (Jan. 25, 2023), *available at* https://www.regulations.gov/comment/CFPB-2023-0011-0052.

particular, bank payments are typically a lower cost payment method, and thus making it easier for merchants to accept such payments safely can help drive down transaction costs across the ecosystem. To that end, Stripe developed its Financial Connections product to streamline consumers' interactions with financial services by enabling consumers to elect seamless and secure bank payments online without being required to navigate burdensome (and unnecessary) manual verification processes: instant bank account verification takes only minutes, replacing cumbersome micro-deposit verifications which take days to complete and have a much lower success rate. Financial Connections reduces merchants' technical integration efforts and reliance on third-party verification systems, while enabling consumers to control access to their data to leverage innovative financial services and complete their purchases more conveniently.

Stripe believes that consumers' ability to share their financial data with third parties of their choice will accelerate the market's ability to further leverage bank payments. Such access to broad categories of financial data can be used to develop and provide a diverse range of financial tools to consumers. Accordingly, as stated in its SBREFA Comment, Stripe encourages the CFPB to adopt a final rule that stimulates market innovation in both the immediate and long-term by empowering consumers and their authorized third parties to reliably and seamlessly access permissioned financial data. To further support these interests, Stripe strongly supports the CFPB's swift finalization of the rule.

In light of the Proposal, Stripe is submitting the comments below to build on the themes from its SBREFA letter, which focused on the final rule's implementation of broad consumer data access rights to facilitate fair market competition that benefits consumers. In particular, Stripe urges the CFPB to consider the following amendments while refining its Proposal:

- The CFPB should not endorse tokenization or other security technology for account and routing numbers. While encryption is meant for the protection of consumers' sensitive information, today's tokenization practices create opportunities for fraud. Tokenization can also create unfair competitive advantages that would lead to the sort of market consolidation that the CFPB has warned about. Therefore, the final rule should not endorse tokenization; instead, the CFPB should lead a separate inquiry into tokenization before rushing to a final rule that would have significant and lasting negative impacts on the payments ecosystem.

- Authorized third parties and data aggregators should be permitted to use data for certain "secondary" purposes with a consumer's informed consent. As drafted, the Proposal's "reasonably necessary" standard could be interpreted in a manner that would block any innovation that depends on "secondary" data insights. 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 avoid that outcome, the final rule should take a more nuanced approach to protecting consumer data. Importantly, authorized third parties and data aggregators should be permitted to use anonymized data to develop models and product features that will benefit consumers.

- The final rule should clarify when authorized third parties and data aggregators could be subject to data provider obligations. As written, the Proposal could be interpreted to subject authorized third parties and data aggregators to data provider obligations merely because they obtained data from the data provider. To avoid confusion, the final rule should include detail or examples to clarify when parties possess or control data in a way that would subject them to data provider obligations.

- Pass-through digital wallets should be excluded from data provider obligations. By granting data access rights to pass-through digital wallet transaction data, the final rule could create an end-run around the genuine data provider and create a potentially conflicting second data source. To avoid this result, the final rule should determine that when a pass-through digital wallet initiates a transaction from a bank account or credit card, the service being provided is not the transaction itself; rather, the service is convenient access to an array of external accounts. Therefore, the bank would be the data provider as the ultimate payment instrument provider (and not the digital wallet).

- Standard-setting organizations (SSO) should enable the industry to efficiently scale the data access framework. To enable efficient operationalization of standards across the marketplace, Stripe requests that the final rule encourage SSOs to promote adoption of reasonable policies and procedures to achieve efficiency at scale, including standard approaches to considering risk management concerns.

- SSO certifications should not unduly delay enforcement of the final rule. The final rule should clarify that failure of data providers and authorized third parties to align on relevant standards is not a reasonable basis to delay the rule's implementation. To mitigate the risk of such delay, the CFPB should clarify its SSO authorization processes to enable industry participants to plan their upcoming efforts.

- Strong data provider performance standards are important for preventing anti-competitive market behaviors. The CFPB should determine that blank, stale, and inaccurate data fields are not considered proper responses for the purposes of calculating a data provider's response rate. The CFPB should also require data providers to achieve response times as fast as their own consumer interfaces and faster than 3,500 milliseconds when necessary to align with market practice.

- The final rule should further clarify its prohibition on fees to avoid confusion about what costs the data provider is permitted to recover, if any. As written, the Proposal states that data providers will not be permitted to charge a consumer or authorized third party for establishing or maintaining a developer interface, or for receiving requests or producing data in response to such requests. To avoid misinterpretations of this provision, the final rule should clearly define certain terms used in the Proposal, including what constitutes interface "maintenance" to avoid potential confusion about what fees may be charged.

- The final rule should more narrowly define reasons a data provider can deny access requests for risk management concerns. Stripe shares the CFPB's concern that data providers may have incentives to deny access, particularly where third parties are offering a competing product or service. To mitigate that risk, the final rule should limit the relevant risk types to those grounded in the data provider's established risk management policies, so long as such policies are not pretext for favoring the data provider’s own service or product.

- The final rule should permit authorized third parties to report denials directly to the CFPB. Rather than relying only on data providers to report their access denials, the CFPB should align competition incentives by permitting authorized third parties to report such denials directly. Moreover, data access denial reports should be kept

confidential in order to protect the interests of the denied third party who made the request.

- Data access caps should be prohibited by default. As written, the Proposal grants data providers significant discretion to limit access, even if the data providers are motivated by competition with the authorized third party. To avoid anti-competitive behaviors, data access limits should be viewed as unreasonable and discriminatory *by default*, until the data provider can show otherwise.

- The final rule should protect consumers from excessive inquiries. Stripe is concerned that the Proposal gives data providers permission to reach out to consumers directly for clarification of data access requests, which could create unnecessary burden and risk for abuse for anti-competitive purposes. Data providers should be required to clarify data requests with the authorized third party instead. In addition, the final rule should permit the third party to request a consumer's reauthorization to extend an existing connection no more than once each year.

A more detailed discussion of each of these recommended changes to the proposed rule follows.

I. The final rule should not endorse tokenization or other security technology for account and routing numbers.

According to the Proposal, the CFPB tentatively plans to permit data providers to provide authorized third parties with tokenized account numbers (TAN) in lieu of primary account and routing numbers (PAN). While Stripe strongly supports the CFPB's intention to protect consumers' sensitive information, it also has significant concerns about the potential negative impacts that the use of tokenization could have on consumers and competition. Account and routing numbers have been a critical means of facilitating bank payments for decades and facilitate the movement of trillions in payment volume every year. Stripe is concerned that the final rule's endorsement of TANs without a more thorough analysis of the potential outcomes could have unintended negative impacts on efforts to create a safe payments system with fair competition. To the extent the CFPB believes account and routing numbers need greater security, Stripe strongly urges it to conduct a separate inquiry to review potential security approaches before endorsing the use of potentially risky and anti-competitive tokenization

practices in this rulemaking.

A. When data providers withhold PANs, authorized third parties have fewer methods for detecting and preventing consumer fraud and financial crimes.

Stripe recognizes that there can be benefits to the use of TANs, such as security of credentials and consumer privacy. Nevertheless, without standard approaches to such tokenization, the CFPB's endorsement of TANs could cause system weaknesses that could be easily exploited by data providers and even fraudsters.

Because some TANs may be issued on a per "application" basis, Stripe may receive a unique TAN whenever a consumer links their bank account via our Financial Connections product. As a consequence, a data provider's production of TANs in lieu of PANs will make it difficult for Stripe to identify unique accounts used to perpetrate fraud across merchants. In other words, 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. Similarly, a data provider's production of TANs in lieu of PANs would prevent Stripe from relying on certain external providers of fraud signals on new accounts. Indeed, 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, which causes the payment to fail. As a consequence, the fraudster will receive the purchased goods (which were shipped after the merchant receives payment is authorized but before settlement), and our merchant users suffer 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).[2]

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; subsequently, Stripe can trace the payment method usage across different transactions. However, if PANs are tokenized (and therefore unable to be linked to a specific consumer across transactions), Stripe will lose an important tool used to support anti-financial crimes

[2] Unlike card payments, bank payments made through the Automated Clearing House (ACH) are not guaranteed.

investigations. To avoid these negative outcomes, Stripe suggests that the final rule should not endorse TANs before conducting a separate inquiry to consider the risk that it would introduce to the payment system.

B. Permitting only production of TANs will create an anti-competitive market environment.

Due to the non-standard and impermanent nature of TANs, nothing in the Proposal prevents data providers from setting the lifecycle of the TAN such that it expires and effectively revokes access between an account holder's initial authentication and consent to execute payments. As a consequence, permitting data providers to rely on TANs gives them broad control over when to deactivate an account number, even if that is not the consumer's intention. Moreover, merchants might be 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 data provider may implement its own proprietary tokenization technology. In that scenario, third parties would only be able to partner with the network provider of the data provider's choosing, as only that provider would have the capability to de-tokenize 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 data providers. Stripe agrees with Director Chopra's statement that such an outcome would be detrimental to consumers: "Control of the open banking system by such players threatens competition and the consumer's control of their own financial affairs."[3] Accordingly, Stripe urges the CFPB to conduct a separate inquiry into the potential anti-competitive impacts of TANs before endorsing them in this rulemaking.

C. The Proposal's deference to TANs has the potential to cause consumer harm.

Stripe's experience has been that institutions that use TANs fail due to account validity at much higher rates than comparable institutions. Specifically, if the final rule permits data providers to provide only TANs (and withhold PANs), a consumer's decision to revoke access to Stripe will cause any debits which we send them to fail, including ones which may not have been submitted

[3] *See* Chopra, Rohit, Laying the foundation for open banking in the U.S. (June 12, 2023), *available at* https://www.consumerfinance.gov/about-us/blog/laying-the-foundation-for-open-banking-in-the-united-states/.

yet or are in flight. In other words, the payment would fail even though the consumer may not have intended to prevent the payment from going through. In contrast, PANs are stable identifiers regardless of whether the consumer chooses to revoke Stripe's access, thereby allowing in-flight payments to settle. Therefore, Stripe is concerned that permitting only TANs will introduce an additional factor that leads to breaking payment flows and less reliable bank payments. To avoid this outcome, the CFPB should conduct a separate inquiry to identify the potential impacts that its endorsement of TANs could have on consumer payments.

II. Authorized third parties should be permitted to use data for certain secondary purposes with a consumer's informed consent.

The Proposal's limits on authorized third party data use to what is "reasonably necessary" to provide the consumer's requested product or service could be interpreted in a manner that would stifle innovation. While this approach would substantially limit data use for the purported benefit of consumers, it would also prevent consumers from giving their informed consent for the use of data for other beneficial purposes. 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 avoid that outcome, the final rule should take a more nuanced approach to protecting consumer data.

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 against entities receiving data pursuant to the Gramm-Leach-Bliley Act (GLBA) guardrails. In addition, consistent with the SBREFA small business recommendation, 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. The CFPB may choose to ask SSOs to set standards to ensure that data is adequately anonymized for the protection of consumers.

We believe these use cases 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 should be permissible, particularly with consumer permission. Precluding

consumers from making the choice to make their information available for such uses would be inconsistent with the intention of Section 1033 to enable consumers to make their own choices about the use of their financial data.

III. The final rule should further clarify key provisions to enable its swift implementation.

As the global economy becomes more reliant on online commerce, the ability to authorize "pay by bank" and access to payment account data are increasingly important for the provision of innovative consumer services.[4] For that reason, the market is moving toward an open banking system, yet its natural progression has been hampered by slow negotiation of direct access agreements, inconsistent performance expectations, and disparate technical standards. Until these barriers are solved, consumers will not have ubiquitous access to convenient, safe, and secure payments that data access has promised to deliver.

With the adoption of Section 1033, Congress specifically recognized the importance of personal data access rights. To effectuate those data access rights, the CFPB's Proposal would provide a regulatory framework ensuring that consumers can request access to their financial data directly or through an authorized third party. As the CFPB adopts a final rule, however, it is clear that its implementation will require a significant collective effort that could prolong full implementation of the rule. To facilitate swift, effective implementation (and avoid unintended and detrimental impacts), Stripe encourages further clarity in key areas of the Proposal.

A. The final rule should clarify that authorized third parties and data aggregators are not necessarily subject to data provider obligations.

Stripe encourages the CFPB to further clarify the Proposal's definition of "data providers," which are subject to important data access requirements. As written, the Proposal's definition of "data provider" includes "[a]ny other person that controls or possesses information concerning a covered consumer financial product or service *the consumer obtained from that person*." § 1033.111(c)(3) (emphasis added). That definition aligns with language in Section 1033 that limits

[4] The Proposal clearly recognizes the importance of payments data, stating "Payment data from these products and services support common beneficial consumer use cases today, including transaction-based underwriting, payments, deposit account switching, and comparison shopping for bank and credit card accounts." 88 Fed. Reg. 74796, 74803 (Oct. 31, 2023).

consumer's rights to access data that is "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). While Stripe strongly agrees that consumers should have a right to obtain data from the covered person providing the relevant product or service, the Proposal could be interpreted to mean that authorized third parties and data aggregators (collectively "third parties") are also always data providers, which could undermine the intent of Section 1033.

As written, third parties could be viewed as a person that "controls or possesses" data once it obtains that data from the entity otherwise providing a consumer financial product or service (*e.g.* a consumer bank account). On the contrary, Stripe believes the data obtained by the third party relates to the account provided by the account-holding institution, not the service being provided by the third party to the consumer. Moreover, interpreting the rule as treating all third parties as data providers would lead to unintended results. For example, if the Proposal aims to treat third parties as data providers, then every third party would also become a data provider obligated to make the same account data further available via API (compounding data privacy and security concerns) and would be unable to charge fees to facilitate access to the data (which is the market incentive for third parties to facilitate such transactions in the first place).

To mitigate this risk of confusion, Stripe encourages the CFPB to clarify in the final rule that a third party acting solely at the direction of consumers to obtain data from another person is not subject to data provider obligations, unless the third party uses that data to provide another covered product or service subject to data access rights under the final rule.

B. <u>The final rule should exclude pass-through digital wallets because they are different from digital wallets that enable storage of funds.</u>

As written, the Proposal's concept of "digital wallet" is broad and undefined, and therefore could be applied to a wide range of digital payment services, including "pass-through" services that only facilitate payments from accounts offered by other institutions. In its explanation of why digital wallets are covered, the Proposal states that "digital wallet providers hold valuable data that can provide a complete understanding of a consumer's finances" (noting that digital wallets "can initiate payments from multiple cards, prepaid accounts, and checking accounts."). 88 Fed. Reg. 74796, 74803. Given that rationale for including digital wallets, it is important to note that

pass-through transaction data alone provides far fewer insights than when provided with a stored funds feature, which is more comparable to a consumer bank account. Rather than creating multiple layers of data provider obligations and multiple sources for the same data, which could have a variety of negative unintended consequences discussed below, data provider obligations should sit solely with the institution holding the covered consumer account—not with intermediaries through which consumer account information may pass.

Stripe is concerned that implementation of the Proposal as written could lead to unintended consequences. In particular, granting access rights to pass-through transaction data through digital wallets (where there is no capacity to store funds) could develop into an end-run around seeking data from the genuine data provider and create a second potentially conflicting data source. Requiring a digital wallet's production of pass-through transaction data would seem to exceed the rights granted by Section 1033, which limits the consumer's rights to information "in the control or possession of the covered person concerning the product that the consumer *obtained from such covered person*" (emphasis added.) When a pass-through digital wallet initiates a transaction from a bank account or credit card, the service being provided to the consumer is easy access to that underlying account and service. Requiring every intermediary to be treated as the owner of the underlying account data that passes through it would create unnecessary burden and unnecessarily numerous sources of data. Instead, consumers should be empowered to access data associated with these transactions with the ultimate payment instrument provider as the data provider.

To mitigate these concerns, Stripe suggests excluding pass-through wallets (where there is no capacity to store funds) from data provider obligations. Stripe also encourages the CFPB to consider an extended implementation timeframe, since there is no immediate use case for Section 1033 data access rights to digital wallets in the market today. This would allow us to learn from initial implementation efforts and leverage the resulting systems to make digital wallet implementations more cost efficient.

IV. The final rule should encourage SSOs to timely adopt standards that promote market efficiency.

The Proposal's reliance on SSOs is a critical component that will enable the final rule to evolve alongside product offerings and their supporting technologies. Given their importance to near-term technical standards and implementations, Stripe is deeply committed to ensuring

that certified SSOs appropriately represent a cross-section of market participants, some of whom may have conflicting interests.[5] Accordingly, Stripe requests the CFPB to provide greater clarity regarding their composition, operations, and roles.

A. The final rule should encourage SSOs to promote standards that ensure the Section 1033 framework can be efficiently operationalized at scale.

Efficient operationalization of data access will lead to lower costs, cheaper and faster services, and safer transfer of data between market participants. To enable efficient operationalization, Stripe requests that the final rule encourage SSOs to promote adoption of standard approaches to risk management concerns that commonly lead to denial of data access requests. For example, in order to ensure efficient confirmation of data security controls of authorized third parties, SSOs should identify industry certifications or other information that authorized third parties can easily present to reliably pass muster, rather than permit data providers to delay API access (or prohibit permissioned access) through prolonged contract negotiations and security reviews. Moreover, SSOs should further develop a list of authorized third parties who are certified as meeting such requirements. The final rule should include a liability shield for data providers who rely on such determinations or certifications issued by SSOs. Finally, the Proposal's requirements for reasonable policies and procedures under section 1033.351 should specifically create an expectation for efficiency at scale, which is especially important wherever the data provider has business interests that conflict with the authorized third party; a data provider's unreasonable approach to efficient operationalization at scale should be subject to enforcement under the final rule.

B. Certification of an SSO and its development of standards should not unduly delay the CFPB's enforcement of the final rule.

Stripe strongly believes that SSO certifications and standards development are critical to successful implementations of the final rule, and that such standards will take time to develop and implement effectively. Nevertheless, we recognize there is a heightened risk of delay where

[5] This approach is consistent with CFPB's prior statements. *See* Chopra, Rohit, Laying the foundation for open banking in the U.S. (June 12, 2023) ("To thrive, [SSOs] must not skew to the interests of the largest players in the market."), *available at* https://www.consumerfinance.gov/about-us/blog/laying-the-foundation-for-open-banking-in-the-united-states/.

data providers and authorized third parties are unable to agree on workable standards. Notably, a lack of stakeholder agreement has impeded the advancement of similar initiatives in other jurisdictions, such as in the European Union, where differences in standards slowed down efforts to leverage permissioned access for product innovation. To avoid undue delay, the CFPB should adopt aggressive but still achievable implementation timelines that it delays only upon SSOs' demonstration of a reasonable basis for doing so. It should be made clear that data providers' failure to agree on relevant standards is not a reasonable basis to delay implementation and would result in regulatory scrutiny.

Stripe also encourages the CFPB to clarify its process (including timelines) around authorizing an SSO, which will enable industry participants to engage in early efforts toward obtaining such certification. Meanwhile, in the absence of certified SSOs, Stripe urges the CFPB to view data providers' adherence to provisions of existing direct access agreements that are consistent with the final rule as constructive compliance with the final rule (and their unreasonable non-compliance as a potentially enforceable unfair practice) until full implementation of the final rule.[6]

V. Stripe supports the implementation of strong performance standards to prevent anti-competitive behaviors.

Stripe strongly agrees with the CFPB's preliminary determination that "it is necessary to propose a firm quantitative floor to ensure that the performance improves in the near term." 88 Fed. Reg. 74796, 74816. Specifically, the Proposal insightfully recognized the benefits of setting such standards, stating, "The CFPB has preliminarily determined that the performance of data providers' developer interfaces needs both to improve and to become more consistent and predictable from where that performance is today." 88 Fed. Reg. 74796, 74816. Such consistency and predictability will bring efficiency to operationalization, and will ensure that consumers receive better products and services.

To achieve those ends, the Proposal establishes that the quantitative minimum performance specification proposed would be a response rate of "at least 99.5 percent." 88 Fed. Reg. 74796, 74816. As the Proposal notes, the 99.5 percent response rate would be calculated as "the number

[6] SSO standards are not necessary to enforce the final rule. While the Proposal says conformance to SSO standards is indicia of compliance, it notes that "an entity does not have to show adherence to a [SSO] to demonstrate compliance with a provision of the rule, as long as its conduct meets the requirement of the rule provision." 88 Fed. Reg. 74796, 74807.

of proper responses by the interface divided by the total number of queries to the interface." While Stripe believes this is a logical approach to determining a response rate, the final rule should be clear about what constitutes a "proper" response and that scheduled downtime needs to be reasonable in duration in order to ensure consistent and fair representations of response rates across the industry. Importantly, the CFPB notes that a satisfactory response, other than an error message during scheduled downtime, would "fulfill[] the query or explains why the query was not fulfilled" and otherwise complies with the requirements of the rule. However, through Stripe's direct access agreements today, data providers commonly return blank data fields or stale information in response to the query. Accordingly, Stripe encourages the CFPB to explicitly exclude from the response rate formula any incomplete, inaccurate, or stale responses (defined as data that has not been updated on a frequency consistent with data updates visible to consumers via the data provider's direct consumer interface and reasonably reflecting the current state of the account) and require parity with the data provider's own consumer interface to ensure fair competition and consumer choice among innovative products and services.

In addition to response rates, the Proposal determines the amount of time for a response to be provided by the interface "cannot be commercially reasonable if it is more than 3,500 milliseconds." § 1033.311(c)(1)(i)(d)(3). Stripe appreciates the CFPB's effort to establish a ceiling on acceptable response times, as well as its recognition that "[i]t is possible under the CFPB's proposed rule that the amount of time for the response would not be commercially reasonable even if it were less than 3,500 milliseconds." 88 Fed. Reg. 74796, 74816. This is particularly important because many data providers in the industry already perform better than 3,500 milliseconds today; moreover, standard response times are likely to decrease as technology improves over time. Accordingly, the CFPB should require data providers to improve performance based on market conditions.

Notwithstanding its support for a standard, Stripe is concerned that the Proposal's 3500-millisecond standard (excluding during scheduled downtime for the interface) is too vague without quantifying *how often* responses must exceed the standard. To resolve that concern, Stripe urges the CFPB to specify that a commercially reasonable response must be at least less than 3,500 milliseconds at least 90 percent of the time. In addition, the CFPB's monitoring of the publicly posted performance metrics will be key to ensuring data providers' adherence to the final rule. Importantly, the CFPB may confront data providers that publicly post performance

metrics that lag behind their competitors; while that would not have an immediate impact on market practices, it could serve as a motivator for data providers.

VI. The final rule should further clarify its prohibition on fees to avoid confusion about what costs the data provider is permitted to recover, if any.

As written, section 1033.301(c)(2) of the Proposal prohibits data providers from charging a consumer or authorized third party for establishing or maintaining a developer interface, or charging for receiving requests or producing data in response to such requests. These bright-line rules will prevent consumers from being impeded from exercising their statutory rights because of fees. However, the Proposal could more clearly define its terms (including "establishing," "maintaining," and "making available covered data") to avoid potential confusion about whether any interface fees may be charged, including one-time or periodic initiation or integration fees.

VII. The final rule should limit the scope of data providers' ability to deny data access requests based on risk management concerns.

A. The final rule should limit the types of concerns that can be a reasonable basis for data access denials.

Stripe understands that many data providers are subject to prudential oversight that requires a robust risk management framework, and that such frameworks inure to the benefit of consumers and the public at large. Accordingly, Stripe supports the Proposal's determinations that denials for objectively legitimate security concerns or lack of certain information about third parties are necessary under the rule. 88 Fed. Reg. 74796, 74820-21. Nevertheless, Stripe also shares the CFPB's concerns that a data provider "may have incentives to deny access, particularly where third parties are offering a competing product or service." 88 Fed. Reg. 74796, 74820.

As the proposal notes, there is substantial risk that a data provider could abuse risk management as pretext for denying access, especially where the authorized third party is offering a competing product or service. Stripe has already observed such practices in some parts of the market. To avoid exploitation of risk management denials, Stripe urges the CFPB to more narrowly define the scope of potential risk management denials. For example, the final

rule could explicitly limit the risks to those specifically cited by prudential regulators (while the CFPB also works with prudential regulators to issue a joint bulletin addressing the balance of risk management against Section 1033 obligations), so long as such risks are not pretext for favoring the data provider's own service or product.[7] Moreover, data providers must be able to cite approved risk management policies and procedures to help ensure that such denials are grounded in applicable policies that are subject to prudential examination, rather than a pretext for access denials. Finally, the CFPB should make clear that unreasonable denials and risk management policies, procedures, and practices may be prosecuted as a violation of Section 1033 and/or UDAAP.

B. The final rule should permit authorized third parties to report denials directly to the CFPB.

The Proposal states that data providers would be required to notify the CFPB when they deny a third party access to a developer interface, including the reasons for denial. Stripe supports the CFPB's efforts to oversee data providers' compliance with the rule. However, Stripe has concerns that such a reporting process would be infrequent and therefore ineffectual for enforcement purposes. If the CFPB implements this process, Stripe urges it to consider including requirements for frequent denial reporting to ensure the CFPB has adequate information to monitor data provider practices (and pursue enforcement as needed).

In addition, consistent with the CFPB's concerns about unreasonable data access denials, Stripe also suggests giving authorized third parties the option to report data provider denials; this would ensure that the incentive to report denials promptly and accurately is aligned with the consumers' interests under Section 1033.

Regardless of the reporting mechanism, Stripe encourages the CFPB to consider what information must be reported, with particular attention to whether the information associated with denials would become available to the public. Stripe is mindful that data access denials could be based on a data provider's view of potential risk management concerns such that it would negatively reflect on a merchant user. Therefore, Stripe urges the CFPB to tailor the data

[7] As a Board member of the Federal Deposit Insurance Corporation (FDIC) and a member of the Financial Stability Oversight Council (FSOC), the CFPB could advocate for amendments to the prudential regulators' joint third-party risk management guidelines in a manner that ensures that the Section 1033 rulemaking can be efficiently implemented.

access reporting requirement to ensure that identifying information does not become available to the public.

VIII. The final rule should prohibit data access caps by default.

According to the Proposal, section 1033.311(c)(2) would allow access caps "only if they reasonably target a limited set of circumstances in which a third party requests information in a manner that poses an unreasonable burden on the data provider's developer interface and impacts the interface's availability to other authorized third party requests." 88 Fed. Reg. 74796, 74817. Stripe strongly supports the CFPB's proposed approach to addressing access caps. While Stripe recognizes that data providers may need to limit access where it legitimately detects fraud to protect consumers (and the authorized third party) from harm, the rule would still assign the data provider excessive discretion to limit access where it also directly competes with an authorized third party in a product or service. Therefore, Stripe feels that any limits on data access should be *by default* viewed as unreasonable and discriminatory and it should be up to the provider to show why they are not.[8]

Moreover, the CFPB asks for comment on whether there should be restrictions permitted on the total amount of covered data that third parties request over a given period of time. Stripe believes that the CFPB's proposed reasonableness standard already would permit data providers to impose data access caps where fraud is evident or where the data obtained exceeds the amount reasonably necessary to provide the product or service. These accommodations should be sufficient to enable data providers to guard against nefarious activities without impeding consumers' data access rights.

IX. The final rule should protect consumers from excessive inquiries.

The Proposal notes that in some circumstances the scope of information requested by an authorized third party might be ambiguous. To clarify the scope of covered data to be made available in response to a request, the Proposal allows a data provider to clarify the scope of an authorized third party's request *with a consumer*. Stripe has concerns that this practice could be abused by data providers to interrupt the consumer's access to third party services. Instead, Stripe suggests that the final rule requires the data provider to make reasonable attempts to

[8] Stripe also suggests that the final rule explicitly requires data providers to keep records that demonstrate their compliance with this standard.

clarify the requested data with the authorized third party first, before the data provider attempts to clarify directly with a consumer.

In addition, proposed section 1033.421 would enable authorized third parties to act on behalf of the consumer for a maximum duration of collection of one year after the consumer's authorization, unless the consumer reauthorizes the third party's access. 88 Fed. Reg. 74796, 74832. This approach could provide an effective check against data collection that consumers no longer need or want; yet it would seem to permit more frequent requests for reauthorization that may unnecessarily deter consumers from continuing to use the third party service. To avoid this outcome, the final rule should permit the authorized third party to request a consumer's reauthorization to extend an existing connection no more than once each year. In addition, because the rule would permit the authorized third party to seek reauthorization in a "reasonable manner," Stripe suggests establishing flexibility for reasonable reauthorization methods, including options provided directly to consumers via electronic means. 88 Fed. Reg. 74796, 74835.

X. Conclusion

Stripe strongly supports the CFPB's efforts to adopt rules implementing Section 1033 to empower consumers through control over their personal data. In doing so, the CFPB will unlock market competition for innovative financial services that better serve consumers' needs.

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,

Katherine Carroll

Katherine Carroll
Global Head of Public Policy and
Regulatory Legal

EXHIBIT E

Wise
30 W 26th St
New York, NY 10010
wise.com

December 29, 2023

Filed via Electronic Submission: https://www.regulations.gov

Comment Intake—FINANCIAL DATA RIGHTS
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights
(Docket No. CFPB-2023-0052; RIN 3170-AA78)

Wise appreciates the opportunity to submit comments to the Consumer Financial Protection Bureau's (the "Bureau") Notice of Proposed Rulemaking on Personal Financial Data Rights to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

As a supporter of consumer-centric financial services regulation, Wise warmly welcomes the Bureau's continuation of the Section 1033 rulemaking process. Wise has closely followed and engaged in the Bureau's development of the U.S. open banking regime. Wise responded to the Bureau's previous request for comment on Proposals and Alternatives Under Consideration Related to the Rulemaking on Personal Financial Data Rights[1]. We look forward to continuing to share our perspective based on experience in both the U.S. market and abroad, where we have had firsthand experience implementing open banking in recent years.

Background

Wise is a global payments company building the best way to move money around the world. 16 million people and businesses use Wise, which processes over $10 billion in cross-border transactions every month, saving customers over $1.5 billion a year. Wise launched in the United Kingdom in 2011 under its original name TransferWise, and is traded on the London Stock Exchange under the ticker symbol "WISE PLC."

In the United States, Wise is a licensed money transmitter in 48 states and is also appropriately licensed and/or regulated in every country where it operates. It satisfies its compliance requirements with large in-house financial crime, identity verification, due diligence, and customer support teams. Wise has over 5,000 employees in 17 offices, including offices in New York City, Tampa, Florida, and Austin, Texas.

Comments

At Wise, we believe consumers have a fundamental right to access and control their financial data. We believe that when this data is shared securely at the direction of consumers, it can help them better manage their finances, while receiving improved and innovative products and services. Authorized data access improves the efficiency, utility, and stability of the financial sector by increasing competition and breaking down barriers to entry for new entrants with

[1]https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf

consumer-driven business models. Delivering an open banking rulemaking will be a crucial step forward in unlocking competitive, affordable products for American consumers and in parallel ensuring the U.S. remains competitive globally.

In Wise's previous comment letter to the Bureau, Wise laid out three recommendations in regards to the Outline that Wise sees as critical to the success of open banking in the U.S. Wise urged the Bureau to ensure that any final rule will:

(1) Facilitate standard-setting and open banking governance to better incentivize data-sharing;
(2) Guarantee data parity & mandate sufficient coverage (e.g. ensuring the same data points such as fees, including foreign exchange information, are available via application programming interface, or API); and
(3) Expand its scope to cover broader financial accounts, and include payment initiation.

While the Rulemaking on Financial Data Rights takes steps towards these priorities, Wise encourages the Bureau to revisit these recommendations. Wise has already integrated open banking into its product for several years, and was one of the first to implement payment initiation on a major scale in the U.K. Through this process, Wise has also been closely engaged in the implementation of open banking policymaking in both the U.K. and the EU. We have learned firsthand from our experiences, including implementation challenges, what must be done in order to establish an effective open banking environment. Notably, years after the introduction of the EU's Revised Payments Services Directive (PSD2), open banking in the U.K. and Europe still is not fully functioning. Wise is confident the CFPB can leverage best practices from around the world, and at the same time avoid past mistakes.

In addition to Wise's recommendations above, Wise urges the Bureau to consider three recommendations on this proposal:

Wise encourages the CFPB to ensure the composition of the proposed standards setting organization (SSO) is representative of the financial services industry.

Wise supports the CFPB's proposal to recognize a standards setting organization (SSO) to issue industry standards. Wise urges the CFPB to ensure that any SSO is inclusive of all types of financial institutions, including financial technology companies. 82 percent of Americans use digital payments[2]. As such, it is vital that any SSO includes digital payments companies to advise on governance that truly represents U.S. consumers and the industry.

The U.K. offers an example of an unsuccessful standard setting body. In 2018, the government established an Open Banking Implementation Entity ('OBIE'), but the country's nine top banks funded the establishment of the entity. This led to undue influence of these banks on the rollout of open banking, to the hindrance of wider fintech participants.

Further, the Bureau should encourage an SSO to discourage data providers from using disclosures to needlessly create friction for consumers and barriers to them sharing their personal financial information. In no way should disclosures be used for anti-competitive

[2]https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/new-trends-in-us-consumer-digital-payments

purposes. A diversity of stakeholders could help the U.S. from choosing one industry approach over another, to protect against possible incentives for banks to design standards that allow them to maintain a tighter hold on consumer data. It is essential that any standards focus on consumer rights, access, and outcomes, not the protection of competitive interests. We encourage the Bureau to establish principles and expectations for any resulting standards.

Governance is important: we would recommend any SSO prioritize the establishment of a governance framework to check APIs and enforce APIs' uptime, availability, data points and quality, and provide a clear mode of redress if those objectives are not being met. An open and fair governance process is necessary to both ensure that all parties are listened to, and consumer outcomes have prioritization over industry ease. As seen with the U.K. case, any potential governance entity must represent not only incumbents but the entire open banking value chain.

Require data parity and sufficient coverage (e.g. ensuring the same data points - including on fees, including foreign exchange information - are available via API).

In addition to standard-setting and good governance, guaranteeing data parity in transactions, or ensuring all data points currently available via a customer's mobile banking interface is accessible via an open banking API, is crucial.

Wise reiterates from its previous letter that the Bureau can achieve this by explicitly defining more data fields within the Outline, especially foreign exchange information, which provides key comparison data on fees and helps consumers comparison shop, notably for remittance payments. Firsthand experience with open banking initiatives in the U.K. and Europe - where some data points were mandated within the law and others were optional - has taught difficult lessons on the importance of guaranteeing data parity. In those markets, Wise observed that when data fields such as foreign exchange pricing data are not explicitly mandated in the data-sharing rulemaking, providers choose not to make certain pricing information available via API.

Foreign exchange is a service offered within standard payment account usage, and as such should be a standard data point to be shared in an open banking environment. Without this, consumers sending and receiving international payments will not be able to access comprehensive price comparison.

In addition to consistent and reliable APIs, the frequency and availability of data collection is equally important. In practice, this means requiring that information be available 'current to request'. For example, the foreign exchange rate used for a payment should be stamped with an accurate date and time. Otherwise, as Wise has observed in the U.K., providers can choose to show old, more favorable exchange rates. This hinders consumers' ability to compare prices and services between providers.

Clarify use of Tokenized Account Numbers (TANs).

Wise urges the CFPB to establish clear standards around the use of Tokenized Account Numbers (TANs) to avoid anticompetitive behavior or unnecessary customer friction. The Bureau's Proposal currently allows a data provider to transmit TANs in lieu of non-tokenized account and routing numbers to reduce fraud risks.

While there are benefits of TANs for mitigating fraud and account security, they also may serve as a barrier to consumers accessing basic account information. Specifically, use of a TAN that can be refreshed automatically has the potential to break the chain of a customer granting permission to a financial services company to pull funds because that authorization is tied to a specific account and routing number paid. If the number changes, a financial institution must then reverify and reauthorize, resulting in significant inconvenience to the customer. Guidance as to when TANs are to be reissued, or whether customer-driven agreements can be put in place between authorized payments companies who have been given access to the account, would be useful tools. If a customer sets up a recurring direct debit on their account, a TAN would at some point break this contract. Account and routing information are commonly used forms of identifying information, and their obfuscation may undermine the goals of open banking.

* * *

Wise welcomes the Outline's initial proposed coverage, which will give consumers control over some of their own financial data. In order to maximize consumer benefit. Wise would support an expansion of the Outline's coverage to include a broader range of financial accounts, such as savings and pension accounts, brokerage accounts, payroll, telecommunications, utilities, and government-related accounts.

Furthermore, in an ideal open banking environment, there are two types of access providers are required to give through their APIs. Payment initiation API, an API which allows third parties to log in to a different account and make a payment, remains absent from the Proposal. Payment initiation allows the customer to pay by bank transfer, with the ease of a card payment, but at a lower cost. Payment initiation is a key competition and innovation driver that will facilitate alternatives to card-based payment methods and provide consumers with more secure options. Delivering account information services only, without being paired with payment initiation services, will be a huge missed opportunity to deliver cheaper, more convenient ways to pay to American consumers.

Wise appreciates the opportunity to provide our comments and commends the Bureau on its efforts to consider the impact of consumer access to financial records. Please do not hesitate to contact us if you have any questions regarding these comments or if we can be of any assistance.

Best,

Rina Wulfing, NorthAm Policy and Campaigns Senior Manager, Wise Inc.

re

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE,

Plaintiffs,

v. Case No. 5:24-cv-00304-DCR

CONSUMER FINANCIAL PROTECTION BUREAU and RUSSELL VOUGHT, in his official capacity,

Defendants.

PROPOSED ANSWER AND AFFIRMATIVE DEFENSES OF THE FINANCIAL TECHNOLOGY ASSOCIATION TO PLAINTIFFS' AMENDED COMPLAINT

Pursuant to Rule 24(c) of the Federal Rules of Civil Procedure, the Financial Technology Association ("FTA") submits this Proposed Answer responding to the allegations in Plaintiffs' Amended Complaint. Headings in the Amended Complaint do not constitute well-pleaded allegations of fact and therefore require no response. To the extent FTA does not specifically admit any allegation in the Amended Complaint, the allegation is denied. FTA expressly reserves the right to seek to amend or supplement its Answer as may be necessary.

INTRODUCTION

1. This is a case about a federal agency overstepping its statutory mandate and injecting itself into a developing, well-functioning ecosystem that is thriving under private initiatives. The rule that Plaintiffs challenge seeks to cut off that private development and replace it with a complicated, expensive, mandatory regulatory framework that Congress never authorized. Worse yet, the framework the agency has adopted is fundamentally unsafe, so the primary result of its overreach will be to harm the very consumers it is charged with protecting.

ANSWER: FTA denies the allegations in this paragraph.

2. A bank's fundamental mission is to safeguard its customers' deposits while providing services that allow those customers to access and deploy their financial assets in the ways they choose. In recent years, third-party technologies have afforded consumers a number of new ways to access, analyze, and use their financial data, such as their transaction history, account balances, spending trends, and more. While this movement toward "open banking"—a term used to describe the model where consumers authorize third parties to access their financial data in order to provide a finance-related product or service—has provided many benefits to consumers, sharing such sensitive data inherently presents risks to the security of customers' deposits and sensitive financial information.

ANSWER: FTA admits that a bank is obligated to safeguard its customers' deposits and to give consumers the right to access and deploy their account information. FTA admits that third-party technologies have provided consumers with innovative ways to access, analyze, and leverage their financial data, such as their transaction history, account balances, spending trends, and more. FTA admits there is a movement toward "open banking" and that this term is used to describe the model where consumers authorize third parties to access their financial data

in order to provide a finance-related product or service. FTA otherwise denies the allegations in this paragraph.

3. As one example of such a product, a financial-technology (or "fintech") company will offer an app that consolidates and displays in one place a consumer's financial data and assets across various accounts. To provide that service, the fintech company needs to (i) obtain access to data about the consumer's various individual accounts (either directly or through another third-party company known as a "data aggregator"), (ii) make its own copies of the consumer's data, and then (iii) frequently update that information as often as the company deems appropriate (often multiple times a day, even if the consumer is not actively using the service).

ANSWER: FTA admits that certain fintech companies offer apps that (among other things) consolidate and display in one place a consumer's financial data and assets across various accounts. To the extent the remainder of this paragraph makes categorical statements about the practices of fintech companies and financial institutions, FTA denies the allegations.

4. Initially, such third-party access could occur only through rudimentary methods such as "screen scraping"—*i.e.*, using the customer's login information to access and download account details from online banking portals designed for consumers. But these methods necessarily entail giving those third-party companies access to more data than they need, including the customer's login credentials. This form of data access, as well as the continued storage of the customer's credentials, exposes consumers to serious risks of unauthorized access to and misuse of their accounts and sensitive data.

ANSWER: FTA admits that, initially, consumer-permissioned login information, i.e., screen-scraping, has at times been used as a method to allow the consumer to access their

account information. FTA otherwise denies the allegations in this paragraph.

5. To enable consumers to participate in open banking in a safer way, market participants have developed more secure data-sharing practices that "allow[] third-party financial service providers to access consumer banking and financial data via application programming interfaces."[1] Application programming interfaces (APIs) are software-based protocols that allow two different applications to communicate with each other. These interfaces facilitate targeted, safer sharing of information between financial institutions and fintech companies authorized by customers to receive their information, without sharing login credentials. Over the past three years, secure APIs have displaced screen scraping as the preferred method by which banks participate in open banking.

ANSWER: With respect to the first sentence, FTA admits that market participants have developed "secure data-sharing practices." With respect to the second sentence, FTA admits that APIs are software-based protocols that allow two different applications to communicate with each other. To the extent the remainder of this paragraph makes categorical statements about the practices of banks and/or fintech companies, FTA denies the allegations.

6. In the United States, the developing open-banking system has achieved substantial progress through private-sector efforts. Banks, including Plaintiffs and their members, have embraced this opportunity for innovation because it allows them to develop secure and attractive products for their customers. In other words, open banking is already flourishing through a private, market-based "consumer data sharing ecosystem" in which industry members have been actively participating. Bank Policy Institute & The Clearing House,

[1] Alexey Shliakhouski, *Security in Open Banking: Concerns and Solutions*, Forbes (Aug. 19, 2021), https://www.forbes.com/councils/forbestechcouncil/2021/08/19/security-in-open-banking-concerns-and-solutions/.

Comment Letter on Rule, Docket No. CFPB-2023-0052, at 45 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0918 (BPI & TCH Cmt. Ltr.).

ANSWER: FTA admits that the open-banking system has advanced, to an extent, through private sector efforts, alongside Congress passing Section 1033 of the Consumer Financial Protection Act (CFPA) and the CFPB's subsequent focus on implementing the Rule. FTA otherwise denies the allegations in this paragraph.

7. But all sharing of consumer data—including through more secure APIs—carries risks. Placing additional copies of consumers' private financial data in the hands of more nonbank third parties necessarily increases the opportunities for that data to be stolen, compromised, or otherwise misused. And those third parties are less regulated than banks, which are subject to extensive oversight and supervision by financial regulators. Indeed, a number of fintech companies have been victimized by data breaches.[2]

ANSWER: FTA denies the allegations in this paragraph.

8. Banks, under the supervision of their prudential regulators, have expertise in managing these kinds of risks. Applying that expertise in this context, industry participants have successfully developed and refined open-banking practices that balance consumers' desire to use the valuable tools fintech companies provide against the foremost priority of protecting

---

[2] *See, e.g.*, Pierluigi Paganini, *Data Leak at Fintech Giant Direct Trading Technologies*, Security Affairs (Jan. 31, 2024), https://securityaffairs.com/158384/security/data-leak-at- fintech-direct-trading-technologies.html; Robert Lemos, *Cyberattack on Fintech Firm Disrupts Derivatives Trading Globally*, Dark Reading (Feb. 2, 2023), https://www.darkreading.com/cyberattacks-data-breaches/cyberattack-fintech-firm- disrupts-derivatives-trading; Olivia Powell, *Revolut Data Breach Exposes Information for More Than 50,000 Customers*, Cyber Security Hub (Sept. 21, 2022), https://www.cshub.com/attacks/news/revolut-data-breach-exposes-information-for-more- than-50000-customers.

consumers' deposits and private data. The result has been a flourishing and secure private open-banking system.

ANSWER: FTA denies the allegations in this paragraph.

9. That all changed when the CFPB stepped in to announce its new open-banking regulatory regime. Claiming the authority of a provision of the Dodd-Frank Act enacted more than 14 years ago, the Bureau now seeks to jettison the developing, industry- driven system and replace it with a complicated, costly, and fundamentally insecure mandatory data-sharing framework. *See Required Rulemaking on Personal Financial Data Rights* (Oct. 22, 2024), https://www.consumerfinance.gov/rules-policy/final- rules/required-rulemaking-on-personal-financial-data-rights/ (to be codified at 12 C.F.R. part 1033) (the Rule or Final Rule). Rather than increasing consumers' ability to securely access and share their data, the Rule will impede banks' ability to protect consumers, stifle growth and innovation in open banking, and increase risks to consumers' deposits and data. Simply put, forcing banks to liberally share customers' sensitive financial information while handcuffing banks from managing the risks of doing so is a recipe for fraud and misuse of customer data.

ANSWER: FTA admits that the CFPB issued the Final Rule and relied on the authority granted to it under the Consumer Financial Protection Act of 2010 ("CFPA"). FTA denies the remainder of the allegations in this paragraph.

10. In its proposed rule, published October 31, 2023, the Bureau proposed to install for the first time a federal regulatory regime governing "open banking"—a term or concept that appears nowhere in the governing statute. Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Oct. 31, 2023), https://www.govinfo.gov/content/pkg/FR-2023-10-31/pdf/2023-23576.pdf (Proposed Rule). Among other things, the Bureau proposed to (i)

mandate the sharing of sensitive customer data such as transaction history, account balances, and even account and routing numbers with a seemingly unlimited number of third parties through a mandated "developer interface" all data providers (*i.e.*, banks) must create; (ii) force banks to oversee and be responsible for those third parties' security practices, while simultaneously limiting banks' authority to stop sharing based on risk-management concerns; (iii) outsource authority to private "standard setters" to set the rules of regulatory compliance; (iv) prescribe vague criteria that will be used to determine whether the performance of the new developer interfaces is "commercially reasonable"; (v) set entirely unrealistic deadlines to come into compliance with the new rule; and (vi) prohibit banks from collecting any fees from third parties in exchange for the newly mandated service.

ANSWER: FTA admits that the CFPB released the Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights and that it was published in the Federal Register on October 31, 2023. See 88 Fed. Reg. 74796 (Oct. 31, 2023) ("Proposed Rule"). FTA refers the Court to the Proposed Rule for a full and accurate description of its contents, and denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

11. Given these deeply problematic aspects of the proposal, the Bureau heard from more than 11,000 commenters, many of whom requested substantial changes. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 6; JPMorgan Chase & Co., Comment Letter on Rule, Docket No. CFPB-2023-0052 (Jan. 2, 2024), https://www.regulations.gov/comment/CFPB-2023-0052-0975 (JPMC Cmt. Ltr.). The Bureau nonetheless finalized its rule largely as proposed on October 22, 2024, retaining nearly all the problematic features of its proposal. Yet the Bureau chose to exempt from compliance with the Rule any depository institution with less than $850 million in

assets, a decision that is difficult to square with its apparent view that consumers have a statutory right to participate in this information-sharing framework.

ANSWER: FTA admits that the CFPB received more than 11,000 comments. FTA admits that the CFPB issued the Final Rule that was published in the Federal Register on October 22, 2024. FTA refers the Court to the Final Rule itself for a full and accurate statement of its contents, and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

12. The CFPB's bureaucratic intervention into a well-functioning area that is rapidly developing and improving through private initiatives is not just unnecessary; it is counterproductive, and it will ultimately harm consumers, the very group the Bureau is charged with protecting. For a number of reasons, it is also unlawful.

ANSWER: FTA denies the allegations in this paragraph.

13. *First* and most fundamentally, the Bureau exceeded its statutory authority by requiring banks to broadly provide their customers' financial information to purportedly "authorized" third parties like fintech companies and data aggregators. The Bureau issued the Rule pursuant to Section 1033 of the Dodd-Frank Act, which requires banks to "make available *to a consumer*, upon request, information in the control or possession of the [bank] concerning the consumer financial product or service that *the consumer obtained*" from the bank. 12 U.S.C. § 5533(a) (emphases added). That provision—sandwiched between a provision requiring periodic affirmative disclosures "*to consumers*" about the risks and benefits of their financial products, 12 U.S.C. § 5532(a) (emphasis added), and a provision concerning banks' and regulators' timely "response *to consumers*" regarding "complaints" or "inquiries," 12 U.S.C. § 5534(a) (emphasis added)—requires banks to give *consumers* their *own* information. And

although the Act generally defines "consumer" to include "an agent, trustee, or representative acting on behalf of an individual," 12 U.S.C. § 5481(4), the Rule requires data providers to share consumer information with thousands of commercial entities that plainly do not qualify as agents, trustees, or representatives of those consumers. In short, nothing in Section 1033 authorizes the Bureau to dictate terms on which banks must furnish consumers' data to innumerable, as-yet-unidentified *third parties*—with unknown credentials or security protocols—that are far less regulated than banks, pose potentially novel risks, and have no special relationship with the consumer who requests the data.

ANSWER: FTA denies the allegations in this paragraph.

14. *Second*, the Bureau inexplicably designed the Rule in a way that substantially increases security risks to consumers while refusing to increase—or even reducing—the level of security protection that will be afforded to those customers' deposits and data. On the risk side, the Bureau decided to require banks to provide access not only to information about a customer's account, but also to information enabling third parties to *initiate payment from that account*. On the security side, having ordered banks to provide this sensitive data to third parties, the Bureau declined to assume the primary responsibility for ensuring those third parties can be trusted with that data. Instead, the Rule:

- imposes upon *banks* a vague duty to "[d]ocument" the compliance with consumer authorization requirements of potentially thousands of fintechs and data aggregators, which are not subject to the same data security requirements and expectations as banks, *see* Final Rule at 576 (to be codified at 12 C.F.R. 1033.331(b)(1)(iii));
- substantially limits banks' ability to denies access to those third parties on risk-

management grounds by purporting to confine that discretion to narrowly prescribed circumstances, *see* Final Rule at 574 (to be codified at 12 C.F.R. 1033.321);

- declines to require the third-party fintech companies and data aggregators to use the APIs that the banks will be forced to build, thus permitting the continued use of the screen-scraping method of obtaining consumer data that even the Bureau admits is a serious security risk; and
- refuses to articulate any principles for allocating liability among the various actors in this transmission chain when consumer data is misused, compromised, or stolen.

The Bureau failed to persuasively justify why it rejected comments pointing out these issues (and in fact made some of them even worse in the Final Rule). The end result is a regime that, in addition to exceeding the Bureau's statutory authority, is quintessentially arbitrary and capricious.

ANSWER: FTA denies the allegations in this paragraph.

15. *Third*, in addition to tasking banks with the obligation to "document" third-party security practices and regulatory compliance, the Bureau outsourced the authority to set standards for compliance to private, third-party organizations. In several key respects, the Rule provides that banks' compliance with the obligation to share information will be measured by compliance with standards set by private organizations. But nothing in Section 1033 or any other statutory provision authorizes the Bureau to let private organizations decide policy or legal questions that determine banks' compliance with regulatory mandates. The Bureau explained that technical specifications for APIs may become obsolete more quickly than the Bureau can

act. *See* Proposed Rule at 74,801. But reference to private standard setters for technical formatting requirements is a far cry from relying on standard setters for policy and legal questions regarding banks' risk- management practices and reasonable frequency limitations on interface access, among other matters. This kind of delegation of regulatory authority to a private organization raises serious constitutional questions, but is in any event unauthorized by the statute.

ANSWER: FTA denies the allegations in this paragraph.

16. *Fourth*, the Rule sets performance standards that data providers' new developer interfaces have to meet, but those standards are entirely unclear and often overlapping, leaving data providers effectively to guess what they need to do to comply. The Rule sets a "quantitative" requirement that developer interfaces must provide a "proper response" to at least 99.5% of data requests. But even achieving that demanding metric is not sufficient; the Bureau has retained discretion to determine that an interface that meets this quantitative measurement is nonetheless performing inadequately based on an array of other qualitative performance metrics that will be measured in vague and confusing ways.

ANSWER: FTA denies the allegations in this paragraph.

17. *Fifth*, the Rule imposes a timeline for data providers to come into compliance with the Rule that is fundamentally incompatible with its dependence on standard setters to determine rules for compliance. As explained, the Bureau will depend heavily on private standard-setting organizations to give particularized content to many more general provisions of the Rule. But no such "consensus standards"—as the Bureau calls them— exist today; indeed, the Bureau has not even recognized a single standard-setting organization. The Bureau's decision to set compliance deadlines on dates certain, without regard to when any such standard

setter issues any such "consensus standard," is arbitrary and irrational because it starts a clock for compliance with entirely unknown standards.

ANSWER: FTA denies the allegations in this paragraph.

18. *Sixth* and finally, having imposed these enormous out-of-pocket costs and exposed banks to a substantial and unreasonable risk of liability, the Rule impermissibly bans banks from charging *any* fees designed to recoup those costs to the third-party fintechs and aggregators who will profit from the new framework. Section 1033 does not authorize the Bureau to adopt such a one-sided fee prohibition that effectively gives a windfall to commercial entities like fintechs and data aggregators. Nor has the Bureau adequately justified its fee prohibition, even if Section 1033 allows it.

ANSWER: FTA denies the allegations in this paragraph.

19. For all these reasons and as explained below, this Court should bring a halt to the Bureau's unlawful efforts to force banks to engage in unsafe dissemination of their customers' personal financial information and set aside the Rule under the Administrative Procedure Act (APA).

ANSWER: FTA denies the allegations in this paragraph.

PARTIES

20. Plaintiff Forcht Bank, N.A., is a federally chartered, community-focused bank that has been serving Kentuckians since 1985 and has its principal place of business at 2404 Sir Barton Way, Lexington, Kentucky 40509. Forcht Bank has over $1 billion in total assets.

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that Plaintiff Forcht Bank, N.A., is a federally-chartered bank with offices in Lexington, Kentucky.

21. Plaintiff Kentucky Bankers Association (KBA) is a Kentucky non-stock,

nonprofit corporation created pursuant to Kentucky Revised Statutes 273.161 through 273.369 that has its offices at 600 W. Main Street, Suite 400, Louisville, Kentucky 40202. KBA is a trade association that has as members approximately 150 national banks, state banks, and savings banks representing virtually all the commercial banking industry in Kentucky. KBA has been in existence since 1891, and it was formally incorporated in its present form in 1911. According to Article III of KBA's Articles of Incorporation, the "purposes of the Association are to promote the general welfare and usefulness of banks, trust and title companies, and financial institutions doing business in the Commonwealth of Kentucky; to cultivate a more intimate social and business relation between the representatives of such institutions; to collect and disseminate financial and economic information; to secure unity of action." KBA has members who reside and/or operate in the Eastern District of Kentucky, have at least $850 million in total assets, and will be adversely affected by the Rule. KBA also has members with at least $250 billion in total assets that are therefore subject to the Rule's shortest compliance deadline. *See* Final Rule at 562 (to be codified at 12 C.F.R. 1033.121(b)(1)).

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that Plaintiff Kentucky Bankers Association ("KBA") is a trade association.

22. To further its core purposes of advocating for the financial-services industry, KBA has challenged numerous rulemakings and other actions of federal agencies, including the Bureau. *See, e.g.*, *Monticello Banking Co.* v. *CFPB*, No. 6:23-cv-148-KKC (E.D. Ky. filed Aug. 11, 2023).

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that KBA sued the CFPB to challenge

a rule issued by the CFPB in *Monticello Banking Co. v. CFPB*, No. 6:23-cv-148-KKC (E.D. Ky. filed Aug. 11, 2023).

23. Plaintiff Bank Policy Institute (BPI) is a nonpartisan public policy, research, and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. BPI produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial-services industry with respect to cybersecurity, fraud, and other information-security issues. A 501(c)(6) nonprofit headquartered in Washington, D.C., BPI has members who operate in the Eastern District of Kentucky, have at least $850 million in total assets, and will be adversely affected by the Rule. BPI also has members with at least $250 billion in total assets that are therefore subject to the Rule's shortest compliance deadline. *See* Final Rule at 561 (to be codified at 12 C.F.R. 1033.121(b)(1)).

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that Plaintiff Bank Policy Institute ("BPI") is a nonprofit.

24. To further its core purpose of advocating for the financial-services industry, BPI has frequently submitted comments on proposed agency rules and participated in litigation concerning regulation of banks. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 6; Bank Policy Institute, Comment Letter on Proposed Agency Information Collection Activities (Mar. 26, 2024), https://bpi.com/wp-content/uploads/2024/03/BPI-Call-Report-FFIEC-101- and-FFIEC-102-Revisions-Comment-Letter-3.26.24-.pdf; Br. for BPI & TCH as *Amici Curiae*, *Custodia Bank* v. *Fed. Res. Bd. of Govs.*, No. 24-8024 (10th Cir. Sept. 4, 2024); Br. for BPI as *Amicus Curiae*, *McShannock* v. *JPMorgan Chase Bank, N.A.*, No. 19-80030 (9th Cir. Mar. 15, 2019).

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that BPI submitted a comment on the Proposed Rule.

25. KBA and BPI bring this action on behalf of their members to advance their members' interests, as well as the interests of the entire financial-services community. As part of advocating for their members, these association Plaintiffs are committed to ensuring safe banking practices and a stable and predictable regulatory environment that allows banks to protect their customers and manage their own liability.

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph.

26. The Rule imposes direct, burdensome obligations on the association Plaintiffs' members. Accordingly, BPI and its members submitted comments opposing many features of the Rule. *See, e.g.*, BPI & TCH Cmt. Ltr., *supra* ¶ 6; JPMC Cmt. Ltr., *supra* ¶ 11; Wells Fargo & Company, Comment Letter on Rule, Docket No. CFPB-2023- 0052 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0881.

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph except to admit that BPI, JPMC, and Wells Fargo & Company submitted comments on the Proposed Rule.

27. Defendant Consumer Financial Protection Bureau is a U.S. governmental agency headquartered in Washington, D.C. The Bureau is subject to the APA pursuant to 5 U.S.C. § 551(1).

ANSWER: Admitted.

28. Defendant Rohit Chopra is the Director of the Bureau. He is sued in his official

capacity and is also subject to the APA pursuant to 5 U.S.C. § 551(1).

ANSWER: Denied.

JURISDICTION AND VENUE

29. Plaintiffs bring this action under the APA, 5 U.S.C. § 551 *et seq*. This Court has jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs' claims arise under the Constitution of the United States and the APA. The Court has the authority to grant the requested declaratory and injunctive relief under the APA, 5 U.S.C. §§ 702-706, and the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations in this paragraph.

30. Forcht Bank has standing because it is directly and adversely affected by the Rule's requirement to develop interfaces for third-party access to its consumers' data, including the substantial compliance costs imposed by the Rule and the prohibition on charging any fees to third parties or aggregators to recoup those costs. Forcht Bank is also adversely affected by the increased risk of liability it faces because the Rule does not permit it to take adequate steps to safeguard the security of its customers' financial information or protect itself from liability in the event of misuse.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations in this paragraph.

31. KBA and BPI each have associational standing to bring this suit on behalf of, and to seek judicial relief for, their respective members. Their members are directly and

adversely affected by the Rule and accordingly have standing to sue in their own right. Specifically, Plaintiffs' members will be harmed by the Rule's requirement to build an expensive interface for disseminating consumers' information; by the unpredictable framework the Rule prescribes, which is heavily dependent on external standard setters who lack regulatory authority (as well as democratic accountability); by uncertain liability regimes that are likely to leave Plaintiffs' members facing significant legal costs because of the Rule's compelled dissemination of information to non-consumer third parties; and by the inability to charge fees for the services the Rule compels them to provide—even fees charged to commercial fintech companies or data aggregators that profit from use of the data. Finally, neither the claims asserted nor the declaratory and injunctive relief requested requires an individual member to participate in the suit. *See Association of Am. Physicians & Surgeons, Inc.* v. *U.S. Food & Drug Admin.*, 13 F.4th 531, 537 (6th Cir. 2021) (citing *Hunt* v. *Wash. State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA admits that KBA and BPI have associational standing to bring this suit and that the claims and relief requested do not require an individual member to participate in the suit, but otherwise denies the specific allegations in this paragraph regarding the purported harms and adverse effects of the Rule.

32. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e) because it is an action against an agency and officer of the United States, no real property is involved, and Plaintiff Forcht Bank resides in this district. Venue is proper in this division because Plaintiff Forcht Bank resides in this division.

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the

truth of the allegations in this paragraph except to admit that this is an action against an agency and officer of the United States and that no real property is involved. This paragraph also consists of legal conclusions to which no response is required.

BACKGROUND

A. Open Banking

33. Open banking generally refers to a model of structuring the financial-services industry in which a bank customer's financial data, with the customer's permission, can be easily shared with other companies, including other financial-services providers.

ANSWER: FTA admits the allegations in this paragraph.

34. An explosion in the number of fintech companies offering various finance-related services to consumers has driven the expansion of the open-banking system. Visa reports that 87% of Americans use some sort of open-banking service.[3] For example, a fintech company might offer a product that aggregates all of a consumer's information and assets across all their accounts so the accounts and information may be viewed in one place. Another type of fintech company includes payment-processing applications that allow for transferring funds held at banks among individuals.[4] Still other fintech companies serve more specialized functions, such as applications designed for those who are self-employed, or for landlords, or for other categories of consumers or market participants who face common financial issues.

---

[3] Visa, *What Is Open Banking?* (Jan. 27, 2023), https://usa.visa.com/visa-everywhere/blog/bdp/2023/01/27/what-is-open-1674845638965.html; *see* J.P. Pressley, *Open Banking and APIs: What IT Leaders Need To Know*, BizTech Magazine (Apr. 30, 2024), https://biztechmagazine.com/article/2024/04/open-banking-and-apis-what-it-leaders- need-know-perfcon ("Have you used CashApp or Venmo to pay friends back for picking up a dinner check? That's open banking.").

[4] *See* Marielle Segarra, *You May Already Be Using "Open Banking." What Exactly Is It?*, Marketplace (June 24, 2021), https://www.marketplace.org/2021/06/24/you-may- already-be-using-open-banking-what-exactly-is-it.

ANSWER: FTA admits the allegations in this paragraph.

35. Rather than individually communicate with every financial institution fintech companies' customers use, these companies will often delegate data collection to data aggregators to assist them in compiling and updating consumers' account information. Data aggregators—as the name implies—are companies that aggregate a particular dataset from various sources. In the open-banking context, the Bureau defines data aggregators as "person[s] that [are] retained by and provide[] services" to a company "to enable access to covered [consumer] data." Final Rule at 564 (to be codified at 12 C.F.R. 1033.131). Such persons include business "entities." *Id.* at 102.

ANSWER: FTA respectfully refers the Court to the Final Rule itself for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

36. In recent years, industry-led developments have improved the security of open-banking practices. Initially, sharing customers' financial information occurred through screen scraping, an insecure process of sharing financial data whereby a third party obtains access to the consumer's login credentials in order to "scrap[e]" that user's "account data." Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment*, 30 Wash. Int'l L.J. 28, 30 (2020). But when screen scraping is used, the consumer generally has no knowledge or control over what and how much data is actually being "scraped," or how frequently. In addition, screen scraping presents excessive risks to the consumer. Third parties often retain the login credentials and (potentially all) account information indefinitely— rendering it vulnerable to being stolen or misused—and/or scrape

"more information than is necessary to provide the beneficial service the customer wants."[5] For these reasons, many banks have resisted or actively blocked screen scraping.[6]

ANSWER: FTA admits that, as a general matter, industry participants have made efforts to continue to improve the security of digital financial services. FTA otherwise denies the allegations in this paragraph.

37. Increasingly, the industry is transitioning to more secure and targeted sharing of customers' data through APIs. An API operates like a set of instructions by which a third party, pursuant to a consumer's directive, requests certain specified information from the customer's bank account, and the bank responds to that request with the appropriate information. This method removes any need for the customer to share (or the third party to use or retain) the customer's login credentials. And because APIs allow the consumer and the bank to control what data is shared in response to requests controlled and verified by the consumer, they allow for the targeted transmission of data consumers want to be shared without allowing the indiscriminate "scraping" of data from an online banking portal.

ANSWER: FTA admits this paragraph to the extent it suggests that industry participants, along with the CFPB, are generally supportive of API technology and characterizes an API as a way for two services to communicate with each other. FTA otherwise denies the allegations in this paragraph.

38. Banks have been active participants in developing API-based open banking

---

[5] *Fidelity Takes Steps to Address Screen Scraping*, Fidelity (Sept. 18, 2023), https://newsroom.fidelity.com/pressreleases/fidelity-takes-steps-to-address-screen-scraping/s/2f33bc18-f16d-4b66-9868-626ada9ba32b.

[6] *See, e.g.*, *id.*; Robin Sidel, *Big Banks Lock Horns with Personal-Finance Web Portals*, Wall St. J. (Nov. 4, 2015), https://www.wsj.com/articles/big-banks-lockhorns-with-personal- finance-web-portals1446683450; *see also* Proposed Rule at 74,797 (referring to the "inherent risks" of screen scraping, "such as the proliferation of shared consumer credentials and overcollection of data").

through private-sector initiatives. The Financial Data Exchange, a nonprofit industry-standards body whose members include financial institutions, fintech companies, financial data aggregators, and others, has developed an open-banking API specification that is being used by 94 million consumer accounts.[7]

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph.

B. Information-Sharing Risks

39. Data is only as secure as the weakest link in the chain of transmission. As open banking has facilitated more widespread transmission of consumer data, hackers and other bad actors have more targets to choose from in attempting to access that data for illicit or other improper purposes. Unsurprisingly, they have been trying (and at times succeeding). *See* Paganini, *supra*, note 2; Lemos, *supra*, note 2; Powell, *supra*, note 2.

ANSWER: FTA denies the allegations in this paragraph.

40. One reason that sharing customer data increases risks is because fintech companies and data aggregators are subject to far less robust requirements and significantly less oversight and supervision than traditional financial institutions. Statement of Donna Murphy, Deputy Comptroller, OCC, Before the Subcommittee on Digital Assets, Financial Technology and Inclusion Committee on Financial Services, U.S. House of Representatives, 4–5 (Dec. 5, 2023), https://www.occ.gov/news-issuances/congressional-testimony/2023/ct-occ-2023-133-written.pdf (referring to risks posed by "non-bank fintech companies"). Such companies also

[7] *FDX Hits 94 Million Accounts, CFPB Publishes FDX's Standard-Setting Application*, Financial Data Exchange (Sept. 26, 2024), https://financialdataexchange.org/FDX/News/Announcements/FDX%20Hits%2094%20Million%20Accounts,%20CFPB%20Publishes%20FDX's%20Standard-Setting%20Application.aspx.

have less experience in safeguarding information, which can lead to basic mistakes.[8] And of course, once data has left the hands of the bank, it is no longer subject to the bank's monitoring and compliance requirements, or the bank's fraud detection systems.

ANSWER: FTA denies the allegations in this paragraph.

41. These third parties also have fundamentally different business models and incentives as compared to banks. Banks' principal mission is to ensure their customers can securely deposit, access, and use their funds to further their financial goals. Fintech companies, in contrast, may offer services to customers in exchange for targeted advertising or referral fees for other services.[9] Data aggregators, for their part, are literally in the business of collecting and selling as much customer data as possible.[10]

ANSWER: FTA denies the allegations in this paragraph.

42. Customers can suffer serious consequences when their financial data is compromised while in the possession of commercial third parties that lack the extensive security practices (and regulatory supervision) that banks have.

ANSWER: FTA admits that customers can suffer serious consequences when their

---

[8] *See, e.g.*, Felix Hacquebord et al., *Ready or Not for PSD2: The Risks of Open Banking*, Trend Micro Research 11 (2019), https://documents.trendmicro.com/assets/white_papers /wp-PSD2-The-Risks-of-Open-Banking.pdf (describing a fintech company that allowed its customers' "email address[es], password[s], [and] client secret authentication[s] [to be] visible in the path of the [f]in[t]ech's API URL"—as in, in the website address for their API).

[9] *See, e.g.*, Tom Sullivan, *How Does Fintech Make Money? 9 Business Models Explained*, Plaid (Oct. 3, 2022), https://plaid.com/resources/fintech/how-does-fintech-and- plaid-make-money/.

[10] *See generally* Julian Alcazar & Fumiko Hayashi, *Data Aggregators: The Connective Tissue of Open Banking*, Federal Reserve Bank of Kansas City (Aug. 24, 2022), https://www.kansascityfed.org/Payments%20Systems%20Research%20Briefings/documents/9012/PaymentsSystemResearchBriefing22AlcazarHayashi0824.pdf; Karl Popp, *Revenue Models for Aggregator Companies*, Dr. Karl Michael Popp (May 6, 2024), https://www.drkarlpopp.com/karl-michael-popps-blog/revenue-models-for-aggregator-companies.

financial data is compromised, but otherwise denies the allegations in this paragraph.

43. For instance, consider the widespread fraudulent technique of social engineering.[11] Many consumers may be accustomed to ignoring random text messages inquiring about a recent $100 purchase at a retailer that they know they did not make. But if the bad actor sending the text message has obtained the consumer's transaction history, the bad actor may be able to refer instead to an actual transaction the consumer did undertake, thereby increasing the risk that the consumer will believe the text is credible and comply with the bad actor's requests.

ANSWER: FTA admits that social engineering is a type of fraudulent technique. FTA otherwise lacks knowledge or information sufficient to form a belief about the truth of the hypothetical allegations in this paragraph.

44. Compromises of other kinds of consumer financial data can lead to even more direct consequences. A bad actor that gains access to certain information required to initiate payment from a bank account—such as the routing and account numbers—may be able to trigger payments from the account without interacting with the customer at all.

ANSWER: FTA admits that there may be consequences when a bad actor gains access to certain information required to initiate payment from a bank account but otherwise lacks knowledge or information sufficient to form a belief about the truth of the hypothetical allegations in this paragraph.

45. These consequences frequently are borne by vulnerable persons. The FBI reported that fraud-related losses by those age 60 and over increased 11% in 2023, to $3.4 billion total. *Elder Fraud, In Focus*, FBI (Apr. 30, 2024), https://www.fbi.gov/news/stories/elder-

[11] *See* IBM, *What Is Social Engineering?* (accessed Oct. 17, 2024), https://www.ibm.com/topics/social-engineering.

fraud-in-focus. Many of those losses result from technology-related scams—such as those related to cryptocurrency, offers of tech support, and personal data breaches. *Id.*

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph.

46. Before the Rule at issue here, banks had been managing the risks related to open banking consistently with their commitment to protecting their customers and the guidance of their prudential regulators. More broadly, those regulators have recognized the obvious fact that sharing customer financial information with third parties poses risks. In recent interagency guidance addressing third parties that banks *choose* to form a contractual relationship with, the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency warned banks that "the use of third parties, especially those using new technologies, may present elevated risks to banking organizations and their customers." *Interagency Guidance on Third-Party Relationships: Risk Management*, 4 (June 6, 2023), https://occ.gov/news-issuances/news- releases/2023/nr-ia-2023-53a.pdf; *see id.* at 13 (reporting that a number of commenters on the proposed guidance "discussed . . . relationships with fintech companies" and "data aggregators" as examples of third-party relationships that "may pose heightened or novel risk management considerations"). The appropriate way to manage those risks, the banking agencies advised, is for banks to implement "a flexible, risk-based approach to third-party risk management that can be adjusted to the unique circumstances of each third-party relationship." *Id.* at 15.

ANSWER: FTA denies the allegations in the first and second sentences of this paragraph. The third and fourth sentences of this paragraph consist of Plaintiffs' characterization of an interagency guidance document. FTA respectfully refers the Court to that

document for a full and accurate statement of its contents and otherwise denies the allegations to the extent that they are inconsistent with the interagency guidance document.

47. These risks are even more substantial in the context of open banking, where banks must decide whether and how to share consumers' personal and financial information with potentially thousands more third parties with which banks have no voluntary, ongoing relationship. As Acting Comptroller of the Currency Michael Hsu cautioned in a recent speech about open banking, "[s]ecurity is a prerequisite for the sharing and receiving of consumer financial data," and the "increase in the volume and complexity of consumer- permissioned sharing" brought about by open banking "may introduce new risks and necessitate new controls." Michael J. Hsu, Remarks at FDX Global Summit: "Open Banking and the OCC," at 4 (Apr. 19, 2023), https://www.occ.gov/news- issuances/speeches/2023/pub-speech-2023-38.pdf.

ANSWER: FTA denies the allegations in the first sentence of this paragraph. The second sentence of this paragraph consists of Plaintiffs' characterization of remarks by Acting Comptroller of the Currency Michael Hsu. FTA respectfully refers the Court to that document for a full and accurate statement of its contents and otherwise denies the allegations to the extent that they are inconsistent with the document.

48. Bank regulators outside the United States also have long recognized the risks associated with open banking, especially when it involves payment initiation. European regulators have had a regulatory framework governing open banking in place since 2015. Although those jurisdictions' regulatory frameworks have their own serious flaws, they have notably carved out an active role for regulators in ensuring the safety and security of open banking. For example, in the United Kingdom, any third party seeking to access consumers'

financial data must receive authorization to do so from the Financial Conduct Authority, which then monitors the third parties' compliance with applicable regulations. *See, e.g.*, Dan Awrey & Joshua Macey, *The Promise & Perils of Open Finance*, 40 Yale J. on Reg. 1, 15-16 (2023) (citing Open Banking Implementation Entity (OBIE), Enrolling onto the OBIE Directory: How to Guide (2021), https://perma.cc/J249-CNFL).

ANSWER: FTA denies the allegations in the first sentence. FTA admits the allegations in the second sentence. FTA denies the allegations in the third sentence. FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in the fourth sentence in this paragraph.

49. Also relevant here, regulators in both the European Union and the United Kingdom recognize that certain consumer financial data is so sensitive that it warrants extra protection. Specifically, they draw a distinction between "account information services" and "payment initiation services"—the latter of which involves the sharing of information sufficient to remove money from an account (such as an account and routing number)—and require significantly heightened supervision, liability, and security for payment-initiation services. *See* BPI & TCH Cmt. Ltr., *supra* ¶ 6, at 12.

ANSWER: FTA lacks knowledge or information sufficient to form a belief about the truth of the allegations in this paragraph.

50. In the Rule at issue in this case, the CFPB has sought to install a regulatory framework governing open banking for the first time in the United States. The most fundamental problem is that Congress did not authorize the Bureau to do so. But on top of that, the Bureau inexplicably adopted an approach that—contrary to federal banking regulators' guidance and in stark contrast to other open-banking regimes—puts customers' most sensitive information at

risk, yet abdicates the Bureau's responsibility to mitigate that substantially increased risk. The end result is a framework that threatens significant harm to consumers and the entire financial-services ecosystem.

ANSWER: FTA admits that CFPB has engaged in a rulemaking as part of implementing a regulatory framework to govern open banking in the United States. FTA otherwise denies the allegations in this paragraph.

THE BUREAU'S RULEMAKING

51. The rule at issue in this case purports to be the rulemaking required under Section 1033 of the Dodd-Frank Act. The CFPB proposed the rule on October 31, 2023, thirteen years after Dodd-Frank was passed. Having neglected its obligation to issue a rule under Section 1033 for so long, the CFPB proposed a rule that goes far beyond what anyone could have contemplated in 2010. Section 1033(a) states:

> Subject to rules prescribed by the Bureau, a covered person shall 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, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

12 U.S.C. § 5533(a). As stated in the Senate's section-by-section analysis of the Dodd-Frank Act, "[t]his section ensures that consumers are provided with access to their own financial information." S. Rep. No. 111-176, at 173 (2010).

ANSWER: With respect to the allegations of the first sentence of this paragraph, FTA admits that the Final Rule implements Section 1033 of the CFPA but otherwise denies the

allegations in that sentence. With respect to the allegations of the second sentence of this paragraph, FTA admits that the CFPB released the Proposed Rule that was published in the Federal Register on October 31, 2023, but otherwise denies the allegations in that sentence. FTA denies the allegations in the third sentence of this paragraph. The fourth sentence of this paragraph consists of Plaintiffs' characterization of the CFPA. FTA respectfully refers the Court to that statute for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the statute. The final sentence of this paragraph consists of Plaintiffs' characterization of a senate report in the legislative history of the CFPA. FTA respectfully refers the Court to that report for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the report.

52. From the outset of its Proposed Rule, the Bureau all but admitted it was seeking to achieve an objective far beyond the scope of Section 1033. "*In addition* to ensuring consumers can access covered data in an electronic form from data providers," the Bureau stated, it was also proposing to "address" what it perceived as "the challenges . . . with respect to the open banking system by delineating the scope of data that third parties can access on a consumer's behalf, the terms on which data are made available, and the mechanics of data access." Proposed Rule at 74,799 (emphasis added).

ANSWER: FTA denies the allegations in the first sentence. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

53. Below, Plaintiffs describe the Bureau's rulemaking in four parts. First, Plaintiffs summarize the components of the Bureau's proposed framework that are relevant to this

challenge. Second, Plaintiffs summarize the relevant comments submitted to the Bureau regarding its proposal. Third, Plaintiffs describe the partial final rule the Bureau adopted regarding how it would recognize "standard setters" under its new regime. Finally, Plaintiffs explain how, despite the comments the Bureau received, it nonetheless adopted a Final Rule that retains the unlawful and harmful aspects of the Proposed Rule.

ANSWER: The first four sentences of this paragraph consist of Plaintiffs' characterization of the Proposed Rule and Final Rule. FTA respectfully refers the Court to the Proposed Rule and Final Rule for a full and accurate statement of their contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule and Final Rule. The fifth sentence of this paragraph contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

A. The Bureau's Proposed Rule

54. The Bureau issued its Proposed Rule on October 31, 2023. As the core mandate underlying its attempt to install a new regulatory regime governing open banking, the Proposed Rule required banks to "maintain a consumer interface" and "establish and maintain a developer interface" through which consumers' financial information could be shared with consumers and a broad range of third parties. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.301(a)).

ANSWER: FTA admits that the CFPB released the Proposed Rule and that it was published in the Federal Register on October 31, 2023. The remainder of this paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

1. Required Disclosure to "Authorized Third Parties"

55. As its central requirement, the Proposed Rule stated that a "data provider"—*i.e.*, a bank—"must make available to a consumer *and an authorized third party*, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties." Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.201(a)) (emphasis added). This requirement tracked the language of Section 1033 *except* for the significant addition of the term "authorized third parties," which does not appear in Section 1033. The Proposed Rule would require banks to provide consumer data to these third parties through the "developer interface" it required data providers to establish and maintain. *Id*.; *see generally* Proposed Rule at 74,870-73 (Subpart C—Data Provider Interfaces; Responding to Requests) (proposed 12 C.F.R. 1033.301, 1033.321, 1033.331, 1033.341, 1033.351).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule and of Section 1033 of the CFPA. FTA respectfully refers the Court to the Proposed Rule and to Section 1033 for a full and accurate statement of their contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule and statute.

56. The Proposed Rule defined an "authorized third party" as any entity that complied with certain procedures for obtaining the consumer's informed consent— procedures that *banks* would be tasked with ensuring the third party had followed. Proposed Rule at 74,869, 74,873 (proposed 12 C.F.R. 1033.131, 1033.401). These procedures included (i) providing the consumer with details about what information from the consumer's bank account the third party seeks to access and why; (ii) obtaining the consumer's express informed consent to such access; (iii) agreeing to abide by a series of obligations set forth in the Proposed Rule on how the third

party would collect, use, and retain the consumer's data; and (iv) advising how the consumer could revoke the third party's access. *Id*. at 74,873 (proposed 12 C.F.R. 1033.401, 1033.411, 1033.421). The proposal expressly permitted the third party to use a data aggregator to perform these authorization procedures on its behalf, so long as the customer is advised of the data aggregator's involvement and the data aggregator agrees to the same obligations as the authorized third party. *Id*. at 74,874 (proposed 12 C.F.R. 1033.431). The consumer had no ability to select a different aggregator to facilitate the transfer of data.

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

57. After satisfying those authorization procedures, the authorized third party may collect, use, and retain the consumer's data to the extent "reasonably necessary to provide the consumer's requested product or service." *Id.* (proposed 12 C.F.R. 1033.421(a)(1)). The third party was then permitted to use and retain the consumer's data for the longer of (i) up to a year after the most recent authorization form was obtained, or (ii) as long as necessary to continue providing the consumer's requested product. *Id.* at 74,873-74 (proposed 12 C.F.R. 1033.421(b)(3), (b)(4)(ii)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

58. The Proposed Rule would then allow that authorized third party to share the

consumer's data with *other* third parties, provided that the first third party "require[s] the other third party by contract to comply with the" rules governing third-party data access and use. *Id.* at 74,874 (proposed 12 C.F.R. 1033.411(f)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

59. The Bureau did not explain why it was interpreting Section 1033 to allow such a broad swath of third parties to obtain customers' sensitive financial information. After citing the general statutory definition of "consumer" as including "an agent, trustee, or representative," 12 U.S.C. § 5481(4)), the Bureau simply asserted *ipse dixit* that the statute grants the Bureau "authority to establish a framework that readily makes available covered data in an electronic form usable by consumers *and third parties acting on behalf of consumers*, upon request." Proposed Rule at 74,802 (emphasis added). But it did not explain why it thought that any "third part[y] acting on behalf of consumers" would qualify as an "agent, trustee, or representative" of a consumer—terms that indicate a fiduciary- like relationship with an ongoing duty of loyalty to the consumer.

ANSWER: This paragraph continues Plaintiffs characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The second sentence of this paragraph also consists of Plaintiffs' characterization of the CFPA. FTA respectfully refers the Court to the statute for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent

that they are inconsistent with the statute. The first and final sentence of this paragraph also contain legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

60. Notably, the Bureau had not always thought this interpretation was clear: in its advance notice of proposed rulemaking, the Bureau asked, "Who should be considered 'an agent, trustee, or representative' of an individual consumer for purposes of implementing section 1033 access rights?" Advance Notice of Proposed Rulemaking Regarding Consumer Access to Financial Records, 85 Fed. Reg. 71,003, 71,010 (Nov. 6, 2020). The Proposed Rule did not address comments the Bureau had received or explain its reasoning in answering this question so broadly.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Advanced Notice of Proposed Rulemaking ("ANPRM") Regarding Consumer Access to Financial Records, see 85 Fed. Reg. 71003 (Nov. 6, 2020), and the Proposed Rule. FTA respectfully refers the Court to the ANPRM and the Proposed Rule for a full and accurate statement of their contents, and otherwise denies the allegations, including to the extent that they are inconsistent with the ANPRM and Proposed Rule. This paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

2. The "Covered Data" Banks Must Share

61. The Proposed Rule required banks to make "covered data" available to any authorized third party. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.201). It defined covered data to include certain information about the customer's account(s) with the bank, such as information pertaining to transaction history and pending transactions, account balances, upcoming bill information, and account verification information. *Id*. (proposed 12 C.F.R.

1033.211). Covered data also included "terms and conditions" associated with the account, which generally mean the contract terms between the data provider and the consumer, such as "the applicable fee schedule," interest rates, "rewards program terms," and whether the consumer "opted into overdraft coverage" or "entered into an arbitration agreement." *Id.* (proposed 12 C.F.R. 1033.211(d)).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

62. The Proposed Rule also required banks to share an additional category of "covered data" defined in terms of its functionality, rather than information about the customer's product. Specifically, the Proposed Rule would require banks to share "[i]nformation to initiate payment" from an account, which "includes" a consumer's account and routing number in either tokenized or non-tokenized form. *Id.* (proposed 12 C.F.R. 1033.211(c)). The Bureau did not address the unique risks posed by the sharing of payment-initiation information, particularly when shared on the scale of potentially tens of millions of consumers with thousands of third parties. Nor did the Proposed Rule draw any distinction in treatment for this information, instead requiring that it be shared on the same terms as any other information about a consumer's account.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The final two sentences of this paragraph also contain

legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

63. The Bureau did not acknowledge (much less distinguish) its prior guidance recognizing an important difference between "[a]uthorized data access" and "payment authorization." *See* CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, 4 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf ("Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities.").

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. This paragraph also consists of Plaintiffs' characterization of the CFPB's Consumer Protection Principles released on October 18, 2017. FTA respectfully refers the Court to that document for a full and accurate statement of its contents[12] and otherwise denies the allegations, including to the extent that they are inconsistent with the document. This paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

3. Ensuring Third-Party Security

64. Although the Bureau proposed to require banks to share customers' most

[12] Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, CFPB (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

sensitive financial information with countless third parties, the Proposed Rule did not expressly provide *any* role for the Bureau to play in ensuring that those third parties' security practices are sufficiently robust or even that they comply with the same requirements imposed on banks by the Proposed Rule. Instead, the Bureau generally tasked *banks* with that role—while at the same time limiting banks' tools for fulfilling it.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

65. *First*, the Proposed Rule provided that the mandate that banks "*must* make available covered data" is triggered whenever the bank receives information from a third party that "[c]onfirm[s] the third party has followed the authorization procedures" prescribed by the Proposed Rule. Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.331(b)(1)(i)-(iii) (emphasis added)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

66. *Second*, the Proposed Rule sought to circumscribe in numerous ways banks' ability to denies third parties' access to the developer interface based on risk-management concerns.

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement

of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

67. For starters, the Proposed Rule deemed a denial of access to be "not unreasonable" if the denial was "necessary to comply with" the bank's obligations under relevant provisions of the Federal Deposit Insurance Act or the Gramm-Leach-Bliley Act. Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.321(a)). Troublingly, the Bureau did not specify who would determine what is "necessary," nor did it address the untenable choice banks with risk-management concerns would be put to: denies access on safety-and- soundness grounds and risk enforcement by the CFPB for *overly restrictive* access policies, or allow access based on the Proposed Rule and risk enforcement by prudential regulators for *overly lax* policies. *Id*.

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The final sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

68. The Proposed Rule recognized that a bank may also "*reasonably* denies[]" access on risk-management grounds, *id*. (proposed 12 C.F.R. 1033.321(a) (emphasis added)), but provided that a denial would be considered reasonable only if, "at a minimum," the denial is "directly related to a specific risk of which the data provider [was] aware." *Id.* (proposed 12 C.F.R. 1033.321(b)). The Proposed Rule did not specify or give any illustrative examples of what constitutes a "specific" risk or how serious such a risk must be. Nor did the CFPB explain

how this standard interacted with its additional caveat that access could be denied if "the third party does not present evidence that its data security practices are adequate to safeguard the [consumer's] data." *Id.* (proposed 12 C.F.R. 1033.321(d)(1)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

69. The Proposed Rule vaguely warned that such risk-based denials must be carried out "in a consistent and non-discriminatory matter," a hazy and subjective standard that leaves banks with no assurance that a denial based on legitimate risk-management concerns—even those deemed necessary to meet expectations of its primary financial regulator—would not expose it to an enforcement action by the Bureau. *Id.* (proposed 12 C.F.R. 1033.321(b)). Instead, banks making risk-management decisions must wonder whether a legitimate denial of access will ultimately leave them exposed if the CFPB concludes that a bank previously granted what the Bureau perceives as a materially similar request.

ANSWER: This first sentence of this paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations. The second sentence of this paragraph consists of Plaintiffs' predictions of the likely effects of the Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its expected effects and

otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

70. *Third*, puzzlingly, the Bureau did not require that all authorized third parties use the new developer interface that banks would be required to establish and maintain. Nor did it ban the riskiest method of accessing customer financial data: screen scraping. The Bureau repeatedly acknowledged "screen scraping's inherent overcollection, accuracy, and consumer privacy risks," *id.* at 74,813; that "screen scraping creates data security, fraud, and liability risks for data providers," *id.* at 74,854; and that there is "nearly universal consensus that developer interfaces should supplant screen scraping," *id.* at 74,798. Yet the Proposed Rule did not actually ban screen scraping despite its acknowledged risks; it assumed that "the market [will] move away from screen scraping" based on the onerous obligations put on data providers regarding developer interfaces. *Id*. Banks, by contrast, are required to walk a very fine line: the Proposed Rule further warned that the Bureau would "evaluate whether data providers are blocking screen scraping without a bona fide and particularized risk management concern" during the implementation period; if so, the Bureau would "consider using the tools at its disposal to address this topic ahead of the proposed compliance dates." *Id.* at 74,800.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

71. *Finally*, having compelled broad sharing of consumers' most sensitive information, required banks to assume primary responsibility for managing the risks of that sharing, and at the same time limited banks' authority to mitigate those risks, the Proposed Rule

declined to articulate any limitations on banks' liability if customer data is breached. The Bureau rejected proposals to ensure that liability for data misuse or compromise when data is in the hands of a third party should rest with that third party. Instead, the Proposed Rule left banks exposed to unspecified and unpredictable potential liability for data breaches that could have been avoided only by denying third parties access to their API in the first place, not to mention complaints by fintech companies and potential Bureau enforcement actions. *See, e.g.*, U.S. Bank, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 3 (Dec. 27, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0795.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The final sentence of this paragraph consists of Plaintiffs' characterization of a comment on the Proposed Rule submitted by U.S. Bank National Association. FTA respectfully refers the Court to that comment for a full and accurate statement of its contents[13] and otherwise denies the allegations, including to the extent that they are inconsistent with the comment.

4. Standard Setters

72. Having already proposed to task data providers with overseeing the security and compliance of purportedly authorized third parties, the Bureau also proposed to delegate to private organizations much of its claimed authority to set substantive standards for compliance with the Rule.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed

[13] https://www.regulations.gov/comment/CFPB-2023-0052-0795.

Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. This paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

73. In addition to employing standard-setting organizations to provide technical requirements, such as the appropriate format in which to present data, the Bureau also proposed to give private standard setters a significant role to play in measuring banks' compliance with substantive and policy-oriented requirements. For example, the Bureau proposed to look to private organizations to set "qualified industry standard[s]" for:

- how much "scheduled downtime [of the API] may be reasonable," Proposed Rule at 74,871 (proposed 12 C.F.R. 1033.311(c)(1)(i)(C));
- whether "any frequency restrictions" on the number of requests a bank will process through its developer interface "are reasonable," *id.* (proposed 12 C.F.R. 1033.311(c)(2));
- whether a bank's "method to revoke any third party's authorization" is "reasonable," *id.* at 74,872 (proposed 12 C.F.R. 1033.331(e));
- whether "a data provider's policies and procedures regarding accuracy [of information it provides] are reasonable," *id.* at 74,873 (proposed 12 C.F.R. 1033.351(c)(3)); and
- whether a bank's risk-management-related denial of access to the developer interface was "reasonable," *id.* at 74,871 (proposed 12 C.F.R. 1033.321(c)).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed

Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

74. For these substantive requirements, the Bureau generally proposed that a regulated party's "adherence to a qualified industry standard" would constitute "[i]ndicia" that the entity had complied with its obligations under the Proposed Rule. *See, e.g.*, *id*. The Bureau did not explain what the phrase "indicia of compliance" means, but made clear that meeting any such "indicia" would be neither necessary nor sufficient to demonstrate compliance. *See* Proposed Rule at 74,807 ("[A]n entity does not have to show adherence to a qualified industry standard to demonstrate compliance with a provision of the rule . . . Conversely, adherence to a qualified industry standard would not guarantee that the entity has complied with the rule provision.").

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

75. The Proposed Rule did not identify anything in the statute that permitted the Bureau to delegate the formulation of substantive policy "standards" to private organizations. To explain its decision, the Bureau pointed to the "granular coding and data requirements" involved in developing the interfaces that "risk[] becoming obsolete almost immediately," which led the Bureau to prefer the "efficient evolution of technical standards" that external standard-setting organizations facilitate better than government agencies. Proposed Rule at 74,801. But that plainly does not explain why private organizations should have a role in setting compliance

standards that go beyond technical coding and data requirements, including such substantive regulatory requirements as whether a bank's risk-management determinations are "reasonable" or its policies and procedures are appropriate. *Id.*

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The first and third sentences of this paragraph also contain legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

5. Developer Interface Performance

76. The Bureau also proposed to set performance standards for the developer interfaces that data providers would be required to develop. But those standards were both stringent and confusing. The Proposed Rule's baseline requirement was that a developer interface's performance "must be commercially reasonable." Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.311(c)(1)). But the Proposed Rule then went on to propose particular performance standards, including that the interface must respond properly to at least 99.5% of queries it receives, must not have excessive downtime, and must respond to requests quickly—within 3,500 milliseconds. *Id.* at 74,781 (proposed 12 C.F.R. 1033.311(c)(1)(i), 1033.311(c)(1)(i)(C), 1033.311(c)(1)(i)(D)(*3*)).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The second sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required,

FTA denies the allegations.

77. Satisfying these performance standards would not be sufficient to demonstrate commercially reasonable performance, however. The Proposed Rule additionally provided that "[i]ndicia" of commercially reasonable performance included that the interface performance meets the specifications of a qualified industry standard and "[m]eets the applicable performance specifications achieved by the developer interfaces . . . [of] similarly situated data providers." *Id.* (proposed 12 C.F.R. 1033.311(c)(1)(ii)). The Bureau did not explain in the proposal how these "indicia" interacted with or would be weighed against the more specific performance specifications provided.

ANSWER: This paragraph consists of Plaintiffs characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

6. Compliance Deadlines

78. Despite the substantial new obligations the Proposed Rule would impose, the Bureau proposed to give the largest banks—depository institutions with at least $500 billion in total assets and nondepository institutions that generated $10 billion in revenue in 2023 or expect to in 2024—a mere six months after publication of the final rule in the Federal Register to come into compliance. Proposed Rule at 74,869 (proposed 12 C.F.R. 1033.121(a)).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule.

79. In addition to the unreasonably short deadline, the Proposed Rule did not explain why the Bureau did not key the compliance deadlines off of the promulgation of standards by the standard-setting organizations it proposed to recognize. As commenters pointed out, that failure would pose challenges because "some of the industry standards mentioned by the CFPB do not yet exist, and they will not exist until qualified industry body(s) are recognized and publish such standards." JPMC Cmt. Ltr., *supra* ¶ 11, at 31.

ANSWER: The first sentence of this paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations. With respect to the allegations in the second sentence of this paragraph, FTA respectfully refers the Court to the agency comments and the preamble of the Final Rule for a full and accurate description of those comments, e.g., 89 Fed. Reg. at 90858-61, and otherwise denies the allegations, including to the extent that they are inconsistent with those comments and the Final Rule.

7. Access-Fee Prohibition

80. Finally, the Bureau proposed to forbid data providers from "impos[ing] any fees or charges on a consumer or an authorized third party" to compensate for establishing or maintaining its interfaces or processing requests for consumers' data. Proposed Rule at 74,870 (proposed 12 C.F.R. 1033.301(c)). In other words, banks would be required to provide the extensive services mandated by the Proposed Rule—including the significant oversight, compliance, and liability costs—for free. According to the Bureau, the fee prohibition is "necessary . . . to effectuate consumers' rights" under Section 1033 to receive their data "upon

request." *Id.* at 74,814. But the Bureau did not square that explanation with its later acknowledgement that banks may still indirectly lawfully "pass[] on to consumers" some of the costs of their APIs in the form of, for instance, "higher account fees." *Id*. at 74,853. Nor did the Bureau explain why consumers should bear the costs of significantly expanded third-party access to their data, rather than the third parties that directly benefit from that access.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Proposed Rule. The final two sentences of this paragraph also contain legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

81. The Bureau proposed this prohibition on banks even recouping their costs from third parties despite recognizing the immense costs of compliance. The Bureau itself cited a median annual cost of maintaining a developer interface of $21 million (or $210 million over a decade), which ranged as high as $47 million annually for certain banks. *Id.* at 74,847-48. As commenters explained, even these estimates "vastly underestimate[d] the amount of work that even the largest and most technologically advanced" banks would "have to undertake to achieve compliance." BPI & TCH Cmt. Ltr., *supra* ¶ 6, at 14, 67-68. And the CFPB proposed no corresponding prohibition on third parties' charging fees related to their data access and transmission, or the products or services they provide using that data.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Proposed Rule. FTA respectfully refers the Court to the Proposed Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are

inconsistent with the Proposed Rule.

B. The Comment Period

82. The Bureau received more than 11,000 comments on its Proposed Rule. The comments were submitted by a range of financial-services institutions, consumer organizations, and public-interest groups. A number of commenters raised serious concerns about the Proposed Rule, such as (among many others):

- **Teller, Inc.:** The Proposed Rule exceeds the CFPB's authority by attempting to turn a "modest provision intended to provide 'consumer rights to access information'" into a license to "reinvent consumer banking" by "inaugurat[ing] 'open banking' in the United States." Teller, Inc., Comment Letter on Rule, Docket No. CFPB-2023-0052, at 1-2 (Dec. 30, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0903 (Teller Cmt. Ltr.). In particular, third parties are not "consumer[s]" within the meaning of the statute, and the Bureau thus cannot compel dissemination of consumers' financial information to them. *See id.* at 8-12.
- **Credit One:** The Proposed Rule "creates significant risk for consumers' sensitive financial data to be exposed to bad actors" and "appears to place unfair burdens on financial institutions," including "to ensure third parties have followed [appropriate] authorization procedures." Credit One, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 1 (Jan. 2, 2024), https://www.regulations.gov/comment/CFPB-2023-0052-0953. The Bureau should also ensure third parties are "held to the same exacting standards that regulated financial institutions are held to" with respect to data protection. *Id.* at

2. The Proposed Rule is also deficient because it fails to "expressly prohibit . . . screen scraping." *Id.*

- **JPMorgan Chase & Co.:** The Proposed Rule inappropriately relies on standard setters for many choices that "tend to be in the spirit of regulatory enforcement," such as caps on frequency with which data may be accessed, the level of accuracy in responses that data providers must maintain, and the permissible amount of platform downtime. JPMC Cmt. Ltr., *supra* ¶ 11, at 16-17. The Proposed Rule also exceeds the CFPB's authority insofar as it would require banks to share information to initiate payment from a Regulation E account. *Id.* at 8-11. Finally, even with "a sizable team" of "engineers, product managers, analytics, design, [and] legal" professionals, it would take "at least two years" to perform the "extensive work" needed to generate "performance metrics that meet the CFPB's new definitions," to enable "support for required data" that banks are not already sharing, to develop many new policies, and to implement significant technological upgrades. *Id.* at 30-31.

- **BPI & TCH:** The Proposed Rule's use of standard setters could result in privately promulgated qualified industry standards receiving "extraordinary weight by market participants." BPI & TCH Cmt. Ltr., *supra* ¶ 6, at 13. Reliance on standard setters should be abolished with respect to certain provisions, such as the permissible total amount of API downtime and access restrictions. *Id.* at 37. Moreover, "the fee prohibition . . . is not grounded in the statutory text." *Id.* at 42.

- **Consumer Bankers Association:** The CFPB lacks legal authority for the

Proposed Rule because Section 1033's "plain statutory language is fundamentally centered on a consumer's right to access their own information." Consumer Bankers Ass'n, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 9 (Dec. 29, 2023), https://www.regulations.gov/comment/CFPB-2023-0052-0951. To the extent the Bureau has authority to regulate in this realm, it should exercise that authority itself, rather than rely on standard setters. In particular, the Bureau itself should clarify the content of certain requirements the Proposed Rule would impose, such as what would constitute an "unreasonable" restriction on the frequency of data requests. *Id.* at 18. And the Bureau should allow reasonable fees to be charged to authorized third parties. *Id.* at 15-17.

- **American Bankers Association:** The Proposed Rule's "prohibition on fees" is "unsupported by law" and "represents nothing less than a forced transfer of value" from data providers to "data aggregators and third parties seeking to monetize the information." Am. Bankers Ass'n, Comment Letter on Rule, Docket No. CFPB-2023-0052, at 4, 11 (Jan. 2, 2024) (ABA Cmt. Ltr.), https://www.regulations.gov/comment/CFPB-2023-0052-0962. The Proposed Rule also presents grave security risks because, instead of CFPB oversight of risk management, "far too many portions of the [Proposed Rule] are reliant on data providers or standard-setting bodies." *Id.* at 5. In addition, data providers should be given at least two years to comply "after the later of: 1) standards to be deemed to comply are named; or 2) the final rule is published." *Id.* at 20. This timeframe is necessary because of several "completely new concepts" in the Proposed Rule, including requiring sharing of categories of data such as upcoming bill

information. *Id.*

ANSWER: With respect to the allegations in the first sentence of this paragraph, FTA admits that the CFPB received more than 11,000 comments on the Proposed Rule from a variety of sources. FTA respectfully refers the Court to the preamble of the Final Rule, as well as the comments themselves, for a full and accurate description of those comments and the CFPB's responses, e.g., 89 Fed. Reg. at 90843-53, and otherwise denies the allegations to the extent that they are inconsistent with the Final Rule or comments submitted on the Proposed Rule. The remainder of this paragraph consists of Plaintiffs' characterization of comments submitted by Teller, Inc., Credit One, JPMorgan Chase & Co., BPI and TCH, the Consumer Bankers Association, and the American Bankers Association. FTA respectfully refers the Court to those comments for a full and accurate statement of their contents and otherwise denies the allegations, including to the extent that they are inconsistent with those comments.

83. Based on these concerns, commenters called for rescission of the Rule or at least substantial changes to numerous key elements of the Proposed Rule. *See, e.g.*, Teller Cmt. Ltr., *supra* ¶ 82.

ANSWER: With respect to the allegations in this paragraph, FTA respectfully refers the Court to the preamble of the Final Rule for a description of the comments received and the CFPB's responses, e.g., 89 Fed. Reg. at 90844-45, as well as to the comments themselves, and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

C. The Final Rule Regarding Standard Setters

84. On June 11, 2024, the CFPB finalized a portion of its Proposed Rule concerning standard setters. In particular, the CFPB published the procedures by which it would recognize external standard-setting bodies, whose "consensus standards" the Bureau proposed to rely on

in interpreting various provisions of the Rule. *See* Industry Standard Setting, 89 Fed. Reg. 49,084 (June 11, 2024) (to be codified at 12 C.F.R. 1033.101, 1033.131, 1033,141), https://www.govinfo.gov/content/pkg/FR-2024-06-11/pdf/2024- 12658.pdf (Standard-Setter Rule).

ANSWER: With respect to the allegations in the first sentence of this paragraph, FTA admits that the CFPB finalized a portion of the Proposed Rule concerning industry standard-setting on June 11, 2024. See 89 Fed. Reg. 49084 (June 11. 2024) ("Standard-Setting Rule"). The remainder of this paragraph consists of Plaintiffs' characterization of the Standard-Setting Rule. FTA respectfully refers the Court to Standard-Setting Rule for a full and accurate description of its contents, and otherwise denies the allegations, including to the extent that they are inconsistent with the Standard-Setting Rule.

85. In the Standard-Setter Rule, the Bureau explained that it would select standard-setting organizations via application based on a number of characteristics, such as the organization's openness to all interested parties, balancing decision-making power among all interested parties, transparency with respect to procedures, operation by consensus, and a system of entertaining objections and appeals that comports with due process. *See* Standard-Setter Rule at 49,091.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Standard-Setting Rule. FTA respectfully refers the Court to the Standard-Setting Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Standard-Setting Rule.

86. In response to comments questioning the Bureau's authority to recognize standard setters at all, it cited a series of statutory provisions that delegate certain rulemaking

authority *to the Bureau*. *See id.* at 49,086 (citing 12 U.S.C. § 5533(a) (information shall be made available to consumers "[s]ubject to rules *prescribed by the Bureau*") (emphasis added); 12 U.S.C. § 5533(d) (similar); 12 U.S.C. § 5512(b)(1) ("*The Director* may prescribe rules and issue orders and guidance, as may be necessary or appropriate to enable *the Bureau* to administer and carry out [its duties].") (emphases added)). The Bureau did not identify any statutory provision giving the Bureau authority to delegate its rulemaking authority to private organizations.

ANSWER: This paragraph continues Plaintiffs' characterization of the Standard-Setting Rule. FTA respectfully refers the Court to the Standard-Setting Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Standard-Setting Rule. The final sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

87. The Standard-Setter Rule also repeated the Bureau's rationale for delegating policy standards to standard-setting bodies—that "very granular technical requirements could rapidly become obsolete" if prescribed by regulators, "while industry-led standard- setting would be better able to keep pace with changes in the market and technology" if the standard setters had been recognized pursuant to fair and appropriate procedures. *Id.* at 49,084.

ANSWER: This paragraph continues Plaintiffs' characterization of the Standard-Setting Rule. FTA respectfully refers the Court to the Standard-Setting Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Standard-Setting Rule.

D. The Final Rule Challenged In This Case

88. The Bureau issued the Final Rule on October 22, 2024. As an initial matter, the

Final Rule exempted a substantial number of institutions from compliance. The Rule "do[es] not apply to data providers . . . that are depository institutions that hold total assets equal to or less than the SBA size standard," Final Rule at 560-61 (to be codified at 12 C.F.R. 1033.111(d)), which the Rule later specifies is $850 million, *id.* at 563. The Final Rule does not address (or explain) the apparent contradiction between the Bureau's view that Section 1033 gives consumers a statutory right to have their information shared through this framework and its denial of that purported statutory right to a substantial number of consumers.

ANSWER: With respect to the allegations in the first sentence of this paragraph, FTA admits that the CFPB released the Final Rule and that it was published in the Federal Register on October 22, 2024. The remainder of this paragraph consists of Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate description of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

89. Despite the numerous objections raised during the comment period, the Bureau persisted in finalizing a rule that not only retains largely all the fundamentally problematic aspects of the Proposed Rule, but even exacerbates some commenters' concerns.

ANSWER: This paragraph consists of Plaintiffs' characterization of the Final Rule and comments received on the Proposed Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents, as well as the comments received, and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. This paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

90. *First*, the Rule still compels disclosure of customers' information to any

"authorized third parties," which are defined broadly to include any third-party company that purportedly completes authorization procedures prescribed in the Rule.

ANSWER: This paragraph continues Plaintiffs characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

91. *Second*, the Rule persists in implementing an unsafe and irrational regulatory framework. The Bureau continued to:

- require the sharing not only of data about the customer's account, but of "information to initiate payment" in or out of the customer's account, Final Rule at 567 (to be codified at 12 C.F.R. 1033.211(c));
- decline to assert a clear role for itself in ensuring third parties' compliance with authorization procedures, instead vaguely relying on banks to "[d]ocument" such compliance, *id.* at 576 (to be codified at 12 C.F.R. 1033.331(b)(1)(iii));
- impose significant limits on banks' ability to engage in risk-management- based denials of access to third parties, even in the event that banks denies such access because of the "safety and soundness standards of a prudential regulator," which is not a sufficient basis to denies access, *id.* at 574-75 (to be codified at 12 C.F.R. 1033.321(a), (b));
- refuse to require third parties to use the new developer interfaces or ban screen scraping, *see id.* at 318-19; and
- refuse to set forth any rules for fairly apportioning liability among data providers, authorized third parties, and data aggregators in the event a customer's data is

breached or misused, in light of the unsafe framework the CFPB had created.

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

92. *Third*, the Rule continues to outsource substantial policymaking authority to private standard-setting organizations, which will promulgate "consensus standards" to which regulated parties may adhere and thereby demonstrate "indicia" of their compliance with various aspects of the Rule.[14] Far from looking to private standard setters for only "granular technical requirements," Standard-Setter Rule at 49,084, the Rule delegates broad authority to define as many as 12 other elements of the Rule, including such substantive compliance issues as what constitutes "reasonable" denial of interface access on risk-management grounds or "reasonable" amounts of downtime, access limits, and other similar substantive issues, including those over which prudential bank regulators exercise substantial control and oversight authority. Final Rule at 571-74 (to be codified at 12 C.F.R. 1033.311(c), 1033.311(d), 1033.321(c)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. This paragraph also contains legal conclusions, to which no response is

[14] The Standard-Setter Rule and Final Rule use the terminology "consensus standard" to refer to what the Proposed Rule had called a "qualified industry standard."

required. To the extent a response is deemed to be required, FTA denies the allegations.

93. While the Final Rule retains the language that adherence to a consensus standard would constitute "indicia of compliance" with various provisions of the Rule, the Bureau still did not explain what it means by "indicia of compliance," and continued to warn that meeting any such indicia would be neither sufficient nor necessary to demonstrate compliance with the Rule. *Id.* at 93.

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. This paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

94. *Fourth*, the Bureau made even more vague the Proposed Rule's already-convoluted framework for assessing whether a developer interface's performance is "commercially reasonable." The Bureau abandoned the quantitative requirement that the interface respond to any request within 3,500 milliseconds, instead turning to standard setters yet again to promulgate rules governing the speediness of a response. *Id.* at 572 (to be codified at 12 C.F.R. 1033.311(c)(1)(iv)(C)). But the Bureau retained the confusing approach of (i) requiring a baseline quantitative requirement that the developer interface provide a "proper response" to third-party requests 99.5% of the time, and (ii) stating that compliance with that requirement would not be sufficient to demonstrate "commercially reasonable" interface performance. *See id.* at 201-02 (discussing the possibility "that a data provider's interface has not complied with the commercially reasonable performance requirement . . . notwithstanding that the interface met the quantitative minimum").

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

95. Unlike the Proposed Rule, however, the Final Rule provides additional standards by which the Bureau will assess whether an interface's performance is commercially reasonable (without ruling out the possibility the Bureau would also consider other issues). The Final Rule provides that an interface's performance will be assessed based on "[t]he interface's total amount of scheduled downtime," "[t]he amount of time in advance of any scheduled downtime by which notice of the downtime is provided," "[t]he interface's total amount of unscheduled downtime," and "[t]he interface's response time." Final Rule at 572-73 (to be codified at 12 C.F.R. 1033.311(c)(2)(ii)(B)-(E)).

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

96. The Rule does not prescribe particular standards that govern an interface's performance in these newly identified areas, but instead returns to its vague "indicia of compliance" formulation. "Indicia that a developer interface's performance is commercially reasonable" with respect to the specified metrics include whether its performance conforms to a consensus standard, "[h]ow the interface's performance compares to the performance levels

achieved by the developer interfaces of similarly situated data providers," and "[h]ow the interface's performance compares to the performance levels achieved by the data provider's consumer interface." *Id.* at 572 (to be codified at 12 C.F.R. 1033.311(c)(2)(i)(A)- (C)).[15] This approach—mentioning various metrics by which an interface's performance will be assessed, and then listing only vague "indicia" of compliance with those metrics— leaves data providers essentially to guess how the Bureau might determine whether their interfaces are performing in a "commercially reasonable" manner.

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

97. *Fifth*, the Bureau persisted in setting an arbitrary and irrational compliance schedule based on dates certain, rather than the issuance of "consensus standards" by standard-setting organizations. On the date the Bureau unveiled the Final Rule, it had not yet recognized a single qualified standard-setting organization. It did not state when any such recognition would occur, let alone when any such organization would actually issue *any* of the numerous consensus standards that the Bureau made critical to compliance with the Rule. As a result, the compliance clock is ticking now, despite data providers having no knowledge of what "consensus standards" they might need to comply with. And even though the CFPB warns that adhering to these

[15] The comparison to the data provider's consumer interface appeared for the first time in the Final Rule; no such metric was even suggested in the Proposed Rule.

consensus standards will not guarantee compliance, the standards will necessarily be a critical source of guidance regarding data providers' otherwise vague obligations. Moreover, without offering any substantive explanation for rejecting commenters' specific concerns with compliance deadlines shorter than 24 months—let alone one that accounted for the current and indefinite lack of "consensus standards"—the Bureau set an 18-month compliance period for the largest data providers.

ANSWER: This paragraph continues Plaintiffs' characterization of the Final Rule. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule. The first sentence of this paragraph also contains legal conclusions, to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations.

98. *Finally*, notwithstanding the enormous burdens and costs described above, the Rule continues to prohibit banks from charging *any* fees to authorized third parties and data aggregators to compensate for the costs of establishing and providing access through the APIs mandated by the Rule. Final Rule at 570 (to be codified at 12 C.F.R. 1033.301(c)).

ANSWER: This paragraph consists of Plaintiffs' characterization of the Final Rule and its likely effects. FTA respectfully refers the Court to the Final Rule for a full and accurate statement of its contents and expected effects, and otherwise denies the allegations, including to the extent that they are inconsistent with the Final Rule.

CLAIMS FOR RELIEF

COUNT I
Administrative Procedure Act
(In Excess of Statutory Authority – Unlawful Interpretation of "Consumer")
5 U.S.C. § 706

99. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

100. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

101. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because the Bureau does not have authority to compel provision of covered data to "authorized third parties" who are not the consumer, or at least in an agency or fiduciary-type relationship with the consumer. *Id.*

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

102. Section 1033 requires a bank to provide the *consumer*, "upon request," with information about financial products or services the *consumer* is obtaining from the bank. *See* 12 U.S.C. § 5533(a). The purpose of this provision is to keep consumers informed about their own financial products and services. That is confirmed by the structure of the Dodd- Frank Act, as Section 1033 is sandwiched between a provision requiring periodic affirmative disclosures

"*to consumers*" about the risks and benefits of their financial products, *id.* § 5532(a) (emphasis added), and a provision concerning banks' "response *to consumers*" regarding "complaints" or "inquiries," *id.* § 5534(a) (emphasis added), neither of which plausibly contemplates obligations to potentially thousands of third-party fintech companies or data aggregators. And it is also confirmed by the legislative history of Section 1033 itself, which unambiguously states that the provision "ensures that consumers are provided with access to their own financial information." S. Rep. No. 111-176, at 173 (2010).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

103. The general definitional provision cited by the Bureau does not alter this plain textual meaning. At the beginning of the Consumer Financial Protection Act of 2010 (Title X of Dodd-Frank), the Act defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 5481(4). But that definition does not authorize the Bureau to mandate that banks share consumer data with any "authorized third party." Companies that establish arm's-length commercial relationships with consumers are neither agents, nor trustees, nor representatives of those consumers within the meaning of this definition. Those words, which are themselves undefined, are legal terms of art that are presumed to take their established, common-law meaning. *Evans* v. *United States*, 504 U.S. 255, 259 (1992).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

104. At common law, agents and trustees have a fiduciary relationship that requires

an unusual level of trust and confidence and that imposes a duty of loyalty to act for the principal's benefit. *See, e.g.*, Restatement (Third) of Agency § 1.01 (Am. Law Inst. 2006); Restatement (Third) of Trusts § 2 (Am. Law Inst. 2003). Fintech companies and data aggregators do not qualify as agents or trustees. That leaves only the term "representative," which must be understood "by the company it keeps." *See McDonnell* v. *United States*, 579 U.S. 550, 569 (2016) (internal quotation omitted).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

105. Although the term "representative" may have a broader meaning in some contexts, here that term must be interpreted as similar in nature to an "agent" or "trustee"—*i.e.*, to mean a third party that has a special, fiduciary-like relationship with or duty of loyalty to the consumer. *See, e.g.*, *Dubin* v. *United States*, 599 U.S. 110, 124-127 (2023). Accordingly, in this statute, a "representative" means "someone who represents another as agent, deputy, substitute, or delegate" and is typically "invested with the authority of the principal." *Representative*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/representative (accessed Oct. 21, 2024). Fintech companies and data aggregators seeking to profit off of consumers' financial data in exchange for providing a discrete product or service do not have any of those characteristics, and cannot be considered a customer's financial "representative" simply because the customer authorized limited access in order to obtain the product or service.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

106. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

COUNT II
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking by Placing Consumer Data At Risk)
5 U.S.C. § 706

107. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

108. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

109. The Rule is final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" because the Bureau adopted a fundamentally irrational regulatory framework that increases the risk of misuse or compromise of consumer data while reducing protections that banks could afford to that data.

ANSWER: This paragraph consists of legal conclusions to which no response is

required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

110. Requiring banks to share their customers' financial data with third-party commercial actors, with limited and ill-defined ability to denies access, necessarily increases the risk of compromise of that data. That is particularly true given that these third parties have no fiduciary relationship or duty of loyalty to consumers, nor are they comprehensively regulated for security as banks are. Yet the Bureau's framework is set up to maximize that risk while reducing protections against it. Viewed as a whole, that framework amounts to arbitrary and capricious rulemaking. *See Alliance for Hippocratic Med.* v. *U.S. Food & Drug Admin.*, 78 F.4th 210, 246 (5th Cir. 2023), *rev'd on other grounds*, 602 U.S. 367 (2024).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

111. First, the Bureau unjustifiably required banks not only to share information about the customer's account, but information sufficient to initiate a payment from a consumer's account.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

112. Second, despite commenters' pleas, the Bureau chose not to mandate that third parties use the developer interfaces when available rather than use screen scraping, notwithstanding its acknowledgement (and the near-universal agreement) that the latter practice poses unacceptable risks to consumers. Although the CFPB asserted that "[a] core objective of

the final rule is to transition the market away from using screen scraping to access covered data," the Bureau took actions in the Rule that undermine that supposed objective. Final Rule at 213. In particular, the Bureau puzzlingly suggested that a data provider may under certain circumstances "violate the CFPA's prohibition on acts or practices that are unfair, deceptive, or abusive" if it blocks screen scraping, and the Rule's exemption for data providers with under $850 million in assets will effectively ensure that screen scraping will persist for those data providers. *Id.* at 214-215.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

113. Third, the Bureau declined to assume responsibility for assessing and verifying these third-party actors' security practices and compliance before they are permitted to access consumers' data. Instead, the Bureau deputized banks to fulfill those functions. The Rule vaguely requires banks to "[d]ocument" that the third parties have complied with the Rule. *Id.* at 576 (to be codified at 12 C.F.R. 1033.331(b)(1)(iii)). And while it purports to expressly authorize banks to determine that third-party security practices are inadequate, that authority is sufficient to justify a denial of access only if the third party "does not present *any* evidence that its information security practices are adequate to safeguard the covered data." *Id.* at 575 (to be codified at 12 C.F.R. 1033.321(d)(1) (emphasis added)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

114. Fourth, inserting itself into an essential banking function, the Bureau placed

limits on banks' ability to manage the risks of their business by deniesing any particular third party's access to its developer interface. In particular, the Rule prescribes an overly demanding standard for when a risk-management-based denial is permissible, relies on standard setters to give content to this paradigmatically regulatory issue related to safety and soundness, and imposes an ill-explained "consisten[cy]" requirement for access denials that will hamstring banks that may have to make thousands of risk-management decisions daily in connection with these APIs. Notably, the Bureau's demanding standard and consistency requirement apply *even if* the bank denies access pursuant to policies and procedures that further the safety and soundness standards of its prudential regulators.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

115. These features create a framework that unacceptably puts consumers' sensitive financial data at risk and hobbles banks in their ability to protect that data. Yet the Bureau nonetheless declined to address the serious liability concerns that its regime creates. Specifically, the Bureau failed to set rules for which parties will bear liability (and under what circumstances) when a consumer's financial data is compromised under the broad sharing regime it mandated.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

116. The Bureau's approach of forcing banks to share their customers' most sensitive data and then potentially leaving banks holding the bag when that data is misused or compromised is arbitrary and capricious and fundamentally unfair.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

117. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT III
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking with Respect to Access Denials Based on Risk Management)
5 U.S.C. § 706

118. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

119. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

120. In addition to the fundamentally irrational nature of the Rule's data-security

framework that would put consumers and their data at risk, the Rule's provisions governing risk-management-based denials of interface access are themselves "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Id.* The Rule's limitations on data providers' ability to make risk-management-based denials of access irrationally restrict their ability to protect their and their customers' data, including pursuant to the safety-and-soundness requirements of their prudential regulators.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, while FTA does not agree with the Final Rule's approach to risk-management-based denials in all respects, FTA denies the allegations in this paragraph.

121. As explained above, the Rule provides that a data provider's decision to denies access to its developer interface on risk management grounds will be reasonable—and thus compliant with the Rule—only in narrow circumstances, where a denial is "[d]irectly related to a specific risk of which the data provider is aware" and "[a]pplied in a consistent and non-discriminatory manner." Final Rule at 574-75 (to be codified at 12 C.F.R. 1033.321(b)). Notably, while the Rule acknowledges that banks may need to denies interface access to comply with the safety-and-soundness standards of a prudential regulator, the Rule expressly says that is not enough to make such denial reasonable. Instead, any such denial based on safety and soundness principles must *also* meet the requirements that denials be "[d]irectly related to a specific risk of which the data provider is aware" and "[a]pplied in a consistent and non-discriminatory manner." *Id.* In other words, the Bureau warns banks that complying with safety-and-soundness standards of their prudential regulators is *not* enough to demonstrate compliance with the Rule, if the Bureau determines in its own wide and vague discretion that the denial was

not "reasonable."

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, while FTA does not agree with the Final Rule's approach to risk-management-based denials in all respects, FTA denies the allegations in this paragraph.

122. The Bureau expressly acknowledged this remarkable overreach, explaining that a bank may denies access "to comply with safety and soundness standards of a prudential regulator . . . *and* if the denial complies with [the specific-threat and consistency requirements of] § 1033.321(b)." Final Rule at 84. But the Bureau said nothing about the impossible calculus its Rule would force upon banks, whereby a denial may be required by safety-and-soundness regulations and simultaneously forbidden by the Rule. Ensuring that regulated parties have a means to comply with *all* regulations to which they are subject is "an important aspect of" any regulatory undertaking, and failing to address such a critical issue is paradigmatically arbitrary and capricious. *Ohio* v. *EPA*, 603 U.S. 279, 293 (2024) (quoting *Motor Vehicle Mfrs. Ass'n of U.S., Inc.* v. *State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (*State Farm*)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, while FTA does not agree with the Final Rule's approach to risk-management-based denials in all respects, FTA denies the allegations in this paragraph.

123. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the significant and irrational limits it placed on data providers' risk-management authority. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, while FTA does not agree with the Final Rule's approach to risk-management-based denials in all respects, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT IV
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking with Respect to Allocating Liability)
5 U.S.C. § 706

124. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

125. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

126. In addition to the fundamentally irrational nature of the Rule's data-security framework, the Bureau's refusal to prescribe a scheme to allocate liability for data misuse under its new framework is itself "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." *Id.* Indeed, the Bureau even went so far as to warn data providers not to enter into *private agreements* with third parties as to how any such liability would be allocated. *See* Final Rule at 233. The Bureau's reliance on other liability regimes developed for contexts

that entail sharing less information, and more discretion afforded to financial institutions regarding whom to share that information with, is unreasonable and unreasonably explained.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

127. As the Bureau acknowledged, multiple commenters urged the Bureau to articulate specific principles of liability. *Id.* at 34-36. The commenters reasoned that the Rule "would increase the volume of sensitive financial data accessed by third parties, particularly sensitive information to initiate a payment," which would in turn "increas[e] the risk of unauthorized transactions or other harms arising from the compromise of a data provider's or third party's information systems, such as the risk of inaccurate data transmission." *Id.* at 34-35. Moreover, the Bureau is *forcing* data providers to share consumer information broadly, including information to allow funds to be transferred out of consumers' accounts, while simultaneously allowing data providers limited ability to denies access to their interfaces even for risk-management concerns; data providers therefore must share consumer information with third parties in circumstances in which they otherwise would not. Furthermore, data providers have no control over which third parties consumers authorize to receive access to consumer information, and indeed, consumers themselves do not even have complete control because third parties have substantial discretion in selecting a data aggregator to work with if they so choose. *See id.* at 590-91 (to be codified at 12 C.F.R. 1033.341). Under these circumstances, it is inequitable to impose primary responsibility for data misuse on data providers, who face "exposure to liability- related costs" in connection with losses caused by third parties on a scale that existing liability-allocation regimes do not contemplate. *Id.* at 35 (summarizing comments

from data providers). Instead, commenters "suggested the CFPB address liability by mandating a comprehensive approach to assigning liability or safe harbors for data providers, clarifying the role of bilateral data access agreements to allocate liability, or tak[ing] other steps to reduce harms that might create liability risk." *Id.* at 35-36.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

128. The CFPB did none of these things, instead leaving intact existing and unsuitable frameworks. Liability for electronic funds transfers is governed by Regulation E. Under Regulation E, when a consumer alleges an error such as an unauthorized or incorrect electronic funds transfer, the financial institution is generally required to promptly investigate the allegation and reimburse the consumer if it determines an error occurred. 12 C.F.R. 1005.6, 1005.11. The financial institution generally must investigate and reimburse the consumer even if a third party either made the error or caused the error through carelessness with the consumer's information. Final Rule at 39-40.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

129. As commenters explained, the Regulation E structure is inappropriate for data sharing pursuant to the Rule. The Rule *compels* data providers to share a far larger volume of data—including payment-initiation information—with many more third parties who are not subject to the same oversight and data-security requirements as banks, and over whom banks exercise no control (and the Bureau itself has generally declined to assume direct supervisory

authority over such entities). And the Rule substantially limits banks' ability to decline to share that information, even for risk-management reasons. Under such circumstances, the risks of consumer losses are substantially increased, and it makes no sense to force banks to bear those costs by default as they do in other contexts.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

130. The Bureau inadequately responded to comments raising these concerns. Attacking a straw man, it explained that commenters' concerns about costs under Regulation E "are not specific to . . . section 1033." Final Rule at 39. That response entirely misses the crucial point that, regardless of whether these concerns exist in other contexts, the Rule *exacerbates* them—with its mandatory, freewheeling data-sharing regime—to an extent that renders the application of ordinary Regulation E rules particularly inappropriate here. Moreover, even accepting at face value the Bureau's dubious assertion that various guardrails in the Rule will protect consumers' data security, *id.* at 40, there is no avoiding the reality that the sheer increase in information being transmitted will necessarily increase data compromise and risk of error overall.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

131. The Bureau failed to adequately consider and address these concerns, provide for liability rules appropriately tailored to the context of Section 1033, or allow data providers any mechanism by which to guarantee protection from liability for others' data misuse, such as

permitting data providers to require third parties—as a condition of interface access—to accept liability for data misuse for which they are responsible.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

132. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the absence of allocation of liability for data misuse. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT V
Administrative Procedure Act
(In Excess of Statutory Authority – Compulsory Provision of Payment-Initiation Information)
5 U.S.C. § 706

133. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

134. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of

statutory right." 5 U.S.C. § 706(2)(C).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

135. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.*, because the Bureau does not have authority to compel banks to provide to third parties "[i]nformation to initiate payment to or from a Regulation E account," Final Rule at 567 (to be codified at 12 C.F.R. 1033.211(c)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

136. Section 1033 requires banks to provide information about a customer's account: "information relating to any transactions, series of transactions, or to the account[s] including costs, charges[,] and usage data." 12 U.S.C. § 5533(a). Consistent with Section 1033's focus on providing "information" to customers, each of the specific listed terms—transactions, costs, charges, and usage data—constitutes a piece of descriptive data about an account's activity, features, or characteristics.

ANSWER: This paragraph consists of Plaintiffs' characterization of Section 1033 of the CFPA. FTA respectfully refers the Court to that statute for a full and accurate statement of its contents and otherwise denies the allegations, including to the extent that they are inconsistent with the statute. The final sentence of this paragraph also consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations in this paragraph.

137. But the Rule goes beyond the statute by requiring disclosure of a fundamentally different piece of information: information "to initiate payment." Final Rule at 567 (to be

codified at 12 C.F.R. 1033.211(c)). That goes beyond the scope of Section 1033. Section 1033 authorizes the sharing of information *about* a financial product or service. Yet the Bureau has impermissibly crafted this category of covered data to enable a specific *functionality*: payment initiation by third parties. Those are two different things. As even the Bureau itself has previously recognized, "[a]uthorized data access . . . is not payment authorization." *See* CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, 4 (Oct. 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data- aggregation.pdf.

ANSWER: This paragraph also consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

138. Section 1033 does not authorize the Bureau to require banks to facilitate any particular functionality for third parties, let alone functionality that would allow third parties to directly move customers' money out of their accounts.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

139. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs' requested relief,

to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT VI
Administrative Procedure Act
(In Excess of Statutory Authority – Unlawful Delegation of Regulatory Authority to Private Standard Setters)
5 U.S.C. § 706

140. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

141. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action found to be "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

142. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because nothing in the statute purports to authorize delegation to a private actor of the Bureau's regulatory authority—authority over matters such as appropriate access denials based on risk management, appropriate frequency caps on third parties' access to developer interfaces, and what constitutes a commercially reasonable amount of interface downtime to schedule. *Id.*

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

143. The Bureau has relied on a number of statutory provisions that empower *the*

Bureau to prescribe rules. Standard Setter Rule at 49,086 (citing 12 U.S.C. § 5533(a) (information shall be made available to consumers "[s]ubject to rules *prescribed by the Bureau*") (emphasis added); *id.* § 5533(d) (similar); *id.* § 5512(b)(1) ("*The Director* may prescribe rules and issue orders and guidance, as may be necessary or appropriate to enable *the Bureau* to administer and carry out [its duties]."") (emphases added)). But none of those provisions even hints at the possibility of the Bureau outsourcing those rulemaking directives to private organizations. The Bureau explained that it believed private standard setters could better modify granular technical requirements for standardized data formats as technology evolves, *see* Standard-Setter Rule at 49,084, but that is no justification for delegating responsibility for establishing standards of *substantive* compliance—such as what kinds of risk-management denials are "reasonable"—to private organizations.[16]

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

144. Nor does the statute authorize such delegation to standard-setting organizations. Reliance on private parties to prescribe standards of substantive law raises serious constitutional concerns regarding the impermissible congressional delegation of legislative power, and therefore is permissible only with "express congressional authorization." *Consumers' Research* v. *FCC*, 109 F.4th 743, 777 (5th Cir. 2024) (en banc). As noted above, there is no such authorization in Section 1033.

[16] Plaintiffs do not challenge the Bureau's ability to delegate to standard setters the authority to issue standards regarding technical requirements such as data formatting, which is arguably permitted by the statute. *See* 12 U.S.C. § 5533(d) ("The Bureau, by rule, shall prescribe standards applicable to covered persons *to promote the development and use* of standardized formats for information." (emphasis added)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

145. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT VII
Administrative Procedure Act
(Arbitrary and Capricious – Vague Developer Interface Performance Standards)
5 U.S.C. § 706

146. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

147. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

148. The Rule is final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" because the performance standards the Rule

requires developer interfaces to meet are hopelessly vague and muddled. *Id.* As part of its obligation to provide "a rational connection between the facts found and the choice made," an agency must "articulate[] the standards that guide[] its analysis." *Tripoli Rocketry Ass'n, Inc.* v. *Bureau of Alcohol, Tobacco, Firearms, and Explosives*, 437 F.3d 75, 81 (D.C. Cir. 2006) (citation omitted). An agency acts arbitrarily and capriciously by "'fail[ing] to properly specify' its rules such that [the agency] leaves 'no method by which' a regulated party can 'gauge [its] performance.'" *Pacific Choice Seafood Co.* v. *Ross*, 976 F.3d 932, 945 (9th Cir. 2020) (quoting *Ariz. Cattle Growers' Ass'n* v. *U.S. Fish and Wildlife*, 273 F.3d 1229, 1250-51 (9th Cir. 2001)). As described below, the Bureau's hopelessly vague interface-performance rules run afoul of this requirement.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

149. The Rule threatens enforcement action against a data provider whose "developer interface's performance" is not "commercially reasonable." Final Rule at 571 (to be codified at 12 C.F.R. 1033.311(c)). But the way the Rule defines what the Bureau will consider to be "commercially reasonable" is entirely unclear. The Rule requires a developer's interface to respond "proper[ly]" to at least 99.5% of requests. *Id.* (to be codified at 12 C.F.R. 1033.311(c)(1)). A proper response is one that fulfills the data request (or explains why it was not fulfilled) and is rendered "within a commercially reasonable response time." *Id.* at 572 (to be codified at 12 C.F.R. 1033.311(c)(1)(iv)(A), (C)). But exceeding the 99.5% threshold is not sufficient to demonstrate commercially reasonable performance. The Rule states that the Bureau will also assess five aspects of an interface's performance (without saying whether its list is

exhaustive or how these aspects should be weighed): the proper-response rate of the interface, the interface's total amount of scheduled downtime, the amount of notice given regarding scheduled downtime, the amount of *un*scheduled downtime, and the interface's response time to requests. *Id.* at 572- 73 (to be codified at 12 C.F.R. 1033.311(c)(2)(ii)(A)-(E)). These separate aspects of an interface's performance, in turn, are measured according to three "indicia" of commercially reasonable performance—adherence to a consensus standard, a comparison between the data provider's developer interface's performance and the performance of developer interfaces belonging to similarly situated data providers, and a comparison between the data provider's developer interface's performance and the performance of the data provider's consumer interface. *Id.* at 572 (to be codified at 12 C.F.R. 1033.311(c)(2)(i)(A)-(C)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

150. This amorphous and overlapping framework is impermissibly vague in at least three independent ways.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

151. *First*, the five performance metrics the Bureau references are unclear in several ways. For starters, it is not clear if this list is exhaustive—or, if not, what other metrics could be relevant. *See* Final Rule at 572 (to be codified at 12 C.F.R. 1033.311(c)(2)(ii)) ("[R]elevant performance specifications include . . ."). Nor is it clear how the five elements interact with each other, whether any is necessary or sufficient, whether each is of equal weight, etc. Moreover,

one element on this list of five is the interface's proper-response rate. *Id.* (to be codified at 12 C.F.R. 1033.311(c)(2)(ii)(A)). But the Bureau separately prescribed that any interface whose proper-response rate falls short of 99.5% is performing *per se* commercially unreasonably, *id.* at 571 (to be codified at 12 C.F.R. 1033.311(c)(1)), suggesting the Bureau may *further* evaluate interfaces based on where their proper-response rate falls between 99.5% and 100%. Similarly, another of the five metrics for evaluation is "[t]he interface's response time." *Id.* at 573 (to be codified at 12 C.F.R. 1033.311(c)(2)(ii)(E)). But this concept, too, is already incorporated in the 99.5% minimum threshold because for a response to be "proper," it must be "provided in a commercially reasonable amount of time." *Id.* at 572 (to be codified at 12 C.F.R. 1033.311(c)(1)(iv)(C)).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

152. *Second*, the "indicia" the Bureau will use to evaluate these five performance specifications are themselves vague and nonsensical. Two of the three indicia require a comparison between the data provider's developer interface and other interfaces—either those of other data providers or the particular data provider's own consumer interface. *Id.* (to be codified at 12 C.F.R. 1033.311(c)(2)(i)(B)-(C)). But the Rule provides no indication of how these comparisons will be measured or used in the Bureau's determination of whether the data provider's interface is performing in a "commercially reasonable" manner. In addition, the comparison between the performance of a data provider's developer interface and its consumer interface is especially inapt as between a consumer platform that serves a bank's customers directly (and generally provides numerous other functions and features as part of the customer

experience) and a developer interface that responds to automated requests from countless third parties. But the Bureau has offered no hints as to how this "compar[ison]" will be conducted. *Cf. Tripoli Rocketry Ass'n*, 437 F.3d at 82 (faulting "unbounded comparative analysis").

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

153. *Third*, the Bureau offers no guidance whatsoever on how the three "indicia" of compliance fit together when evaluating an interface's performance. It refuses to say that a data provider would be in compliance if it satisfies one, two, or even all three of these indicia. Nor does it specify the consequences of failing to satisfy one or more indicia. Indeed, nowhere in the Rule does the Bureau ever clearly explain what its foundational "indicia of compliance" standard actually means.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

154. The Bureau's hopelessly muddled performance standards make it impossible for data providers to determine their obligations under the Rule. Instead, they are left to effectively guess at what metrics the Bureau might consider and use in a potential enforcement action for supposedly inadequate performance. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the interface performance standards. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is

required. To the extent a response is deemed to be required, FTA denies the allegations. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT VIII
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking with Respect to Compliance Deadlines)
5 U.S.C. § 706

155. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

156. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

157. The Rule is final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" with respect to its compliance timelines because under the APA, an agency must explain deadlines it selects, including for compliance. *See Wynnewood Refin. Co.* v. *EPA*, 77 F.4th 767, 782-83 (D.C. Cir. 2023); *Piedra-Alvarez* v. *Barr*, 829 Fed. App'x 833, 834 (9th Cir. 2020).

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

158. Here, the Bureau set a compliance timeline that is fundamentally irrational because it is not tied to the promulgation of the consensus standards that the Bureau has made fundamental to compliance with the Rule. Whatever force the Bureau ultimately gives to these vague "indicia of compliance," many industry members will feel compelled to seek to align with those standards to achieve as much certainty as possible under the Bureau's unclear regime. But banks cannot build toward compliance with standards that do not exist. And until such standards are promulgated, any steps data providers take toward compliance come with the substantial risk of being wasted in the event that they must unwind and redo that work to adapt to standards. Left to wait some indeterminate amount of time before they can take meaningful steps toward compliance, data providers are nonetheless staring down the certain deadlines the CFPB has prescribed.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

159. At a minimum, the Bureau should have allowed large data providers the 24-month compliance period they requested. Commenters explained in detail why coming into compliance with the Rule would be a time-consuming endeavor, requiring development of new technical capabilities, enhancement of certain public-facing products and websites, and devising appropriate policies and procedures on a range of subjects. *See, e.g.*, JPMC Cmt. Ltr., *supra* ¶ 11, at 30-31. All of those changes take even longer when they must be developed and rolled out while ensuring that existing developer interfaces remain fully operable. *Id.* The Bureau failed to engage with these explanations, instead inaccurately and cursorily asserting that commenters "did not specify why 24 months would be necessary." Final Rule at 86.

ANSWER: The first and final sentences of this paragraph consist of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations. With respect to the allegations in the second and third sentences of this paragraph, FTA admits that some commenters on the Proposed Rule provided their views of the compliance deadlines under the Proposed Rule. FTA respectfully refers the Court to those comments and the preamble of the Final Rule, e.g., 89 Fed. Reg. at 90858-61, for a description of those comments and the CFPB's responses and otherwise denies the allegations, including to the extent they are inconsistent with the Final Rule and the comments submitted.

160. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the prescribed compliance periods. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT IX
Administrative Procedure Act
(In Excess of Statutory Authority – Access-Fee Ban)
5 U.S.C. § 706

161. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

162. Under the APA, the Court "shall . . . hold unlawful and set aside" final agency action that is "in excess of statutory jurisdiction, authority, or limitations, or short of statutory

right." 5 U.S.C. § 706(2)(C).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

163. The Rule is final agency action "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right" because the Bureau does not have authority to prohibit banks from charging reasonable fees to third parties or data aggregators to access banks' APIs. *Id.* Nothing in the text or structure of Section 1033 prohibits banks from charging reasonable access fees, even to cover their costs. When Congress intends to mandate provision of a product or service at no cost, it knows how to achieve that result. *See, e.g.*, 15 U.S.C. § 1681c-1(a)(2)(B) (Fair Credit Reporting Act requirement that consumer reporting agencies must provide to consumers all required disclosures "without charge to the consumer"). Notably, it even did so elsewhere in Dodd-Frank. *See* 15 U.S.C. § 1691(e)(4) (Creditors shall provide copies of written appraisals or valuations "at no additional cost to the applicant."); 15 U.S.C. § 1639h(c) (requiring creditors to provide a copy of certain appraisals "without charge").

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations in this paragraph.

164. Nor does Section 1033 implicitly delegate to the Bureau the authority to ban banks from charging reasonable access fees, thus providing a windfall to fintechs and data aggregators. Although Section 1033 broadly contemplates "rules prescribed by the Bureau," 12 U.S.C. § 5533(a), interpreting such vague language to authorize federal agencies to determine when businesses are allowed to charge for providing services in a competitive area would raise serious concerns under the U.S. Constitution about the impermissible delegation of legislative power.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

165. For these reasons, the Bureau's promulgation of the Rule was in excess of statutory jurisdiction, authority, or limitations. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. The final sentence of this paragraph also consists of Plaintiffs requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

COUNT X
Administrative Procedure Act
(Arbitrary and Capricious – Failure to Engage in Reasoned Decisionmaking with Respect to Access-Fee Ban)
5 U.S.C. § 706

166. Plaintiffs repeat and incorporate by reference all the allegations set forth above.

ANSWER: FTA incorporates by reference its responses to each of the preceding paragraphs as if set forth fully herein.

167. The APA requires a reviewing court to hold unlawful and set aside any agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A).

ANSWER: FTA admits that this paragraph accurately quotes the APA.

168. Even if the Bureau had statutory authority to prohibit data providers from

charging third parties reasonable fees for access to their developer interface, its decision to impose that access-fee ban in the Rule is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" because it is both unreasonable and unreasonably explained. *Id.*

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

169. The Bureau rejected a proposal to allow "reasonable fees" because it concluded there is no "concrete indication of a workable and administrable standard" for what is "reasonable." Final Rule at 184. That approach stands in stark contrast to the Bureau's approach in other parts of the Rule, where the Bureau prescribed vague performance standards and reserved to itself maximum discretion to enforce those standards on a case-by-case basis. *See, e.g.*, Final Rule at 571 (to be codified at 12 C.F.R. 1033.311(c)) ("A developer's interface performance must be commercially reasonable."); *id.* at 573 (to be codified at 12 C.F.R. 1033.311(d)) ("[A] data provider must not unreasonably restrict the frequency with which it receives or responds to requests."). Moreover, commenters suggested several ways to determine reasonable fees, such as by limiting fees to recouping a data provider's costs, *see* ABA Cmt. Ltr., *supra* ¶ 82, at 11; or costs plus "a margin for establishing, maintaining, receiving requests on, and transmitting covered data on developer interfaces," BPI & TCH Cmt. Ltr., *supra* ¶ 6, at 11; or a fee agreed upon following negotiations with the authorized third parties, who may themselves be profiting from the consumers' data, Indep. Commty. Bankers of Am., Comment Letter on Rule, Docket No. CFPB-2023-0052, at 7 (Dec. 29, 2023), https://www.regulations.gov/ comment/CFPB-2023-0052-0883. It is therefore hard to see the

Bureau's purported concern for precision as anything more than a pretext for reaching a predetermined outcome to force banks to fully bear the costs of the new regime. *See, e.g.*, *Nat. Res. Def. Council* v. *Nuc. Regul. Comm'n*, 879 F.3d 1202, 1214 (D.C. Cir. 2018) ("[I]t would be arbitrary and capricious for the agency's decision making to be internally inconsistent.") (citation and quotation marks omitted); *see also U.S. Sugar Corp.* v. *EPA*, 830 F.3d 579, 650 (D.C. Cir. 2016) (stating "[t]his court has 'often declined to affirm an agency decision if there are unexplained inconsistencies in the final rule,'" and collecting cases) (citation omitted).

ANSWER: With respect to the allegations in the third sentence of this paragraph, FTA admits that some commenters on the Proposed Rule provided their views of the fee prohibition provision under the Proposed Rule. FTA respectfully refers the Court to those comments and the preamble of the Final Rule, e.g., 89 Fed. Reg. at 90884-87, for a description of those comments and the CFPB's responses and otherwise denies the allegations, including to the extent they are inconsistent with the Final Rule and the comments submitted. Otherwise, this paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

170. The Bureau also failed to justify the access-fee prohibition in light of the significant collateral consequences and distortionary effects it would cause. As commenters explained, the access-fee ban would eliminate any incentive for third parties to limit their unnecessary and inefficient access requests, and would effectively force data providers to pass along their costs to customers in other ways. The Bureau meekly offered that "reasonable" caps on third-party access would satisfy the first concern, and it entirely ignored the second. Final Rule at 181, 573 (to be codified at 12 C.F.R. 1033.311(d)). Relying on access caps to correct for the effects of the first set of inefficiencies is hardly the answer, however. *Any* redundant access

request results in inefficiencies, whether or not the request is in excess of a frequency limit. And the Bureau gives little guidance as to what sort of access caps will be tolerated; it instead outsources the matter to a standard-setting organization. *See id.* at 573 (to be codified at 12 C.F.R. 1033.311(d)). In other words, the Bureau is requiring banks to provide a free service and claiming that the free service will not be abused because banks can—at risk of substantial enforcement penalties—stop providing the service when demands cross some unknown threshold of excessiveness.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph. With respect to the allegations in the second and third sentences of this paragraph, FTA admits that some commenters on the Proposed Rule provided their views on the likely effects of the fee prohibition provision under the Proposed Rule. FTA respectfully refers the Court to those comments and the preamble of the Final Rule, e.g., 89 Fed. Reg. at 90884-87, for a description of those comments and the CFPB's responses and otherwise denies the allegations, including to the extent they are inconsistent with the Final Rule and comments submitted.

171. Despite downplaying the consequences of the access-fee ban by suggesting access caps are an appropriate substitute, the Bureau was plainly aware of the major consequences of its fee prohibition. The Bureau understood the Rule imposes significant costs—indeed, ruinous costs for some banks—and that the fee prohibition would mean those costs could not be recouped. *See* Final Rule at 75 (A "credit union trade association" noted "that those [institutions] below [$850 million in assets] might discontinue services if they had to comply with the rule" due to "concerns about the costs of providing data access . . . under the terms of

the rule."). It therefore exempted from the Rule altogether data providers with assets under $850 million. *Id.* at 179-80. This step could obviously have been avoided by simply allowing data providers to recoup their costs of compliance via reasonable access fees. The Bureau did not and cannot explain why it instead chose to leave customers of small data providers without vindication of their putative rights under Section 1033.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent that a response is deemed to be required, FTA denies the allegations in this paragraph.

172. For these reasons, the Bureau's promulgation of the Rule was arbitrary and capricious with respect to the access-fee ban. Plaintiffs are therefore entitled to relief pursuant to 5 U.S.C. §§ 702, 706, and the Rule should be held unlawful and set aside.

ANSWER: This paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed to be required, FTA denies the allegations. The final sentence of this paragraph also consists of Plaintiffs' requested relief, to which no response is required. To the extent a response is deemed required, FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully request that this Court enter judgment in their favor and against the Bureau as follows:

(i) A declaratory judgment that the Rule is in excess of the Bureau's statutory authority within the meaning of the Administrative Procedure Act, *see* 5 U.S.C. § 706(2)(C);

(ii) A declaratory judgment that the Rule is arbitrary, capricious, or otherwise contrary to law within the meaning of the Administrative Procedure Act, *see* 5 U.S.C.

§ 706(2)(A);

(iii) An order setting aside the Rule pursuant to the Administrative Procedure Act, *see* 5 U.S.C. § 706(2);

(iv) An order permanently enjoining Defendants from enforcing the Rule against Plaintiffs and their members;

(v) An order issuing all process necessary and appropriate to delay the effective date and implementation of the Rule pending the conclusion of this case;

(vi) An order awarding Plaintiffs their reasonable costs, including attorneys' fees, incurred in bringing this action; and

(vii) Any other relief as the Court deems just and equitable.

ANSWER: FTA denies that Plaintiffs are entitled to the relief they seek or to any other relief in this action.

AFFIRMATIVE DEFENSES

FTA asserts the following affirmative and other defenses, without conceding that the following are in fact affirmative defenses or that FTA has the burden of proof on any issue as to which applicable law places the burden of proof upon Plaintiffs. FTA reserves the right to amend or modify the following defenses, or to raise additional defenses or claims not asserted herein.

1. The Court lacks subject-matter jurisdiction.

WHEREFORE, FTA respectfully requests that the Court enter judgment in its favor and against Plaintiffs, and order such other and further relief that this Court deems appropriate under the circumstances.

Dated: March 26, 2025

Respectfully submitted,

/s/ Michael P. Abate

Michael P. Abate
KAPLAN JOHNSON ABATE & BIRD
710 West Main Street, 4th Floor
Louisville, KY 40202
(502) 540-8280 (Telephone)
mabate@kaplanjohnsonlaw.com

Counsel for the Financial Technology Association

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY
LEXINGTON DIVISION

FORCHT BANK, N.A., KENTUCKY BANKERS ASSOCIATION, and BANK POLICY INSTITUTE,

Plaintiffs,

v. Case No. 5:24-cv-00304-DCR

CONSUMER FINANCIAL PROTECTION BUREAU and RUSSELL VOUGHT, in his official capacity,

Defendants.

[PROPOSED] ORDER GRANTING RENEWED MOTION TO INTERVENE OF THE FINANCIAL TECHNOLOGY ASSOCIATION

The Financial Technology Association ("FTA") having renewed its motion to intervene in this action, and the Court being sufficiently advised, it is hereby **ORDERED:**

1. FTA's renewed motion to intervene as a Defendant in this action is **GRANTED.**

2. The Clerk is directed to file FTA's proposed answer in the record.

_____, 2025

_____
Danny C. Reeves
Chief Judge
U.S. District Court for the Eastern District of Kentucky