October 21, 2025

Via electronic submission

Comment Intake
Personal Financial Data Rights Reconsideration
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: **Docket No. CFPB–2025– 0037– Comments on Advance Notice of Proposed Rulemaking: Personal Financial Data Rights Reconsideration**

Dear Acting Director Vought:

The Bank Policy Institute[1] appreciates the opportunity to comment on the Advance Notice of Proposed Rulemaking on Personal Financial Data Rights ("ANPR")[2] issued by the Consumer Financial Protection Bureau pursuant to Section 1033 of the Dodd-Frank Act.[3] We support innovation and the underlying principle of Section 1033 that individual consumers have the right to their financial information in standardized formats that makes it easy to use. We also agree that consumers should have the ability to control with whom their data is shared and the terms on which it is shared.

The 2024 Personal Financial Data Rights Rule ("PFDR Rule") issued under prior CFPB leadership far exceeds the authority granted it by Congress in Section 1033 and puts consumers and their data at risk. The CFPB now has an opportunity to correct that overreach. As the current CFPB leadership has recognized, Section 1033 "was intended simply to ensure that [individual] consumers would have access to their own information," and there is "no evidence that Congress in 2010 authorized (or even contemplated) a comprehensive open-banking regime or the scale of data-sharing the Rule mandates

[1] The Bank Policy Institute 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. The Institute 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.

[2] Consumer Financial Protection Bureau, "Personal Financial Data Rights Reconsideration," Advance Notice of Proposed Rulemaking, 90 Fed. Reg. 40,986 (Aug. 22, 2025).

[3] 12 U.S.C. § 5533.

when it enacted this relatively concise provision in Section 1033 . . . "[4] Indeed, Barney Frank, one of the key architects of the Dodd-Frank Act, recently confirmed that Section 1033 was never intended to support the kind of expansive data sharing mandate adopted in the PFDR Rule.[5]

Section 1033 neither requires nor authorizes the CFPB to interfere with an innovative data sharing ecosystem in the United States. Current CFPB leadership found the PFDR Rule's requirements unlawful in several respects, including that the agency lacks the authority to mandate data sharing with commercial entities or prohibit data providers from charging fees to third parties for providing secure access to consumers' sensitive financial data.[6]

Moreover, the PFDR Rule would disrupt the robust and competitive consumer permissioned data sharing ecosystem that exists today. Revising the PFDR Rule in line with a faithful reading of Section 1033 would still allow individuals to continue to access their financial information and to grant third parties access to that information as they do today but would do so in a way that protects the security and privacy of that data. As is the case today, fees, information security protections, liability, and privacy protections, among other things, would continue to be determined via arms-length negotiations between banks, fintechs, and data aggregators through normal market operations. Indeed, the market is functioning well without government regulation, as evidenced most recently by JPMorganChase and Plaid's announcement that they had reached an agreement under which Plaid will compensate the bank for the ability to access its secure data sharing API.[7]

The PFDR Rule undermines this well-functioning marketplace and places consumers and their data at substantial risk. It mandates that banks and other data providers share a massive volume of sensitive consumer financial data with third-party commercial entities, thereby exposing that data to significantly more threats. Yet, the PFDR Rule hamstrings banks' ability to protect that data. For example, the PFDR Rule fails to establish robust data protection requirements or supervisory oversight for fintechs or data aggregators, prohibits banks from charging fees for providing secure data access or the data itself, and fails to allocate liability among data providers, fintechs, and aggregators. The PFDR Rule also limits banks' risk management discretion to deny third-party data access requests. Furthermore, the mere fact of the mass data sharing mandate will significantly reduce third-party fintechs' and data aggregators' incentives to protect consumer data and limit banks' ability to negotiate the terms of sharing consumers' sensitive data. Thus, the PFDR Rule will undermine the competitive and safe functioning of the consumer financial data sharing ecosystem.

The robust data sharing ecosystem that exists today has developed solely as a result of private sector efforts and without a government mandate. The CFPB lacks authority to interfere in this market, and such interference will disrupt the ecosystem and leave consumers more vulnerable to harm. Thus,

---

[4] Defendants' Memorandum in Support of Their Motion for Summary Judgment at 11, *Forcht Bank v. Consumer Financial Protection Bureau*, 5:24-cv-00304-DCR, May 30, 2025) [hereinafter CFPB Summary Judgment Memorandum].

[5] Evan Weinberger, Bloomberg Law, *Jamie Dimon Is Right' on Data Access Fees, Barney Frank Says*, (Sept. 9, 2025), 'Jamie Dimon Is Right' on Data Access Fees, Barney Frank Says.

[6] CFPB Summary Judgment Memorandum, *supra* n. 4 at sections I.A. and I.B.

[7] JPMorganChase Press Release: *JPMorganChase and Plaid announce an extension to their data access agreement for sharing of consumer permissioned data* (Sept. 16, 2025), JPMorganChase and Plaid announce an extension to their data access agreement for sharing of consumer permissioned data.

we support the CFPB's substantial narrowing of the Rule, consistent with the authority Congress granted the agency in Section 1033. In addition, revising the Rule to align with the authority Congress granted would further the goals of Executive Order 14219 and the accompanying Memorandum, which directed agencies to identify and repeal regulations that are unlawful or that exceed the scope of their delegated authority.[8]

Below we respond to the key topics about which the CFPB requested feedback in the ANPR.

I. The CFPB Should Suspend the Compliance Dates in the PFDR Rule As Soon As Possible.

The ANPR states that as "part of its reconsideration of the PFDR Rule, the [CFPB] plans to issue a Notice of Proposed Rulemaking to extend the compliance dates," however, the agency has not yet taken any such action. The CFPB should address this issue immediately. The largest banks currently must comply with the Rule by the summer of 2026 and have already invested significant resources to prepare to do so. If the compliance deadlines are not suspended, banks will continue to expend significant time and resources to come into compliance with a rule that the CFPB itself believes is unlawful and has already begun to revise. There is no justification for forcing banks to expend substantial amounts of time and resources to comply with an unlawful rule that the agency plans to amend. The CFPB therefore should act as expeditiously as possible to suspend the compliance dates while it reconsiders the PFDR Rule.

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

a. *The statute does not authorize the CFPB to mandate consumer data sharing with third-party commercial entities*.

The ANPR seeks input regarding who may make a request on behalf of a consumer to share that consumer's data. Section 1033(a) provides in full that:

> Subject to rules prescribed by the CFPB, a covered person[9] 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.[10]

---

[8] Executive Order 14219 of February 19, 2025, *Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative*. 90 Fed. Reg. 10583 (Feb. 25, 2025).

[9] The term "covered person" is defined in the Dodd-Frank Act as "(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person." 12 U.S.C. § 5481(6). However, certain entities are exempt from the CFPB's jurisdiction. For example, the Dodd-Frank Act provides that "the Bureau shall have no authority to exercise any power to enforce [Title X of the Dodd-Frank Act] with respect to a person regulated by the Securities and Exchange Commission. 12 U.S. Code § 5517(i)(1). Entities exempt from the definition of "covered person" are not subject to Section 1033 and thus would not be subject to any rule implementing Section 1033.

[10] 12 U.S.C. § 5533(a) (emphasis added). We also note that Section 1033(a) does not actually require the CFPB to issue regulations. The relevant provision provides that "subject to rules prescribed by the Bureau…" This language contrasts with section 1033(d), which mandates that "[t]he Bureau, by rule, *shall prescribe* standards applicable to

Any rule issued pursuant to Section 1033 must be narrow, consistent with the statute, to require only that *consumers* have the right to obtain their own data. Congress passed Section 1033 to "ensure[] that *consumers* are provided with access to *their own financial information*,"[11] however, the PFDR Rule unlawfully requires that banks and other data providers make consumer data available to "authorized third parties," mandates that data providers (above a certain size threshold) establish and maintain a "developer interface" to share that consumer information, and imposes numerous other requirements on data providers. Current CFPB leadership agrees that the scope of the agency's authority is indeed limited, explaining that "the [PFDR] Rule unlawfully seeks to regulate open banking by mandating the sharing of data with "authorized third parties," whereas Section 1033 is limited to ensuring that consumers can access their own data."[12] The CFPB has further observed that "the disconnect between the narrow scope of Section 1033 and the ambitious reach of the [PFDR] Rule makes clear that the Bureau exceeded its authority in attempting to regulate the open banking system."[13]

The Dodd-Frank Act includes a general definition of consumer as "an individual or an agent, trustee, or representative acting on behalf of an individual."[14] The PFDR Rule cited this definition and then simply asserted that "the CFPB interprets [S]ection 1033 as authority to establish a framework that ensures data providers readily make available to consumers and third parties acting on behalf of consumers (including authorized third parties offering competing products and services), upon request, covered data in a usable electronic form."[15] The PFDR Rule did not explain why ***any*** "third part[y] acting on behalf of consumers," including a commercial entity that profits from access to consumer data, would qualify as an "agent, trustee, or representative acting on behalf of an individual" consumer. Indeed, these terms indicate a fiduciary or similar special relationship with an ongoing duty of loyalty to the consumer, as exists for a parent or guardian of a minor or the executor or administrator of an estate. These relationships plainly do not exist between consumers and the fintechs and data aggregators with whom the PFDR Rule mandates that banks share consumer's sensitive financial data. Consumers have a purely commercial relationship with fintechs and data aggregators.

i. *The term "consumer" in Section 1033 means an individual*.

The term "consumer" is commonly used and understood to refer to an individual—"one who buys goods or services for personal needs only rather than to produce other goods."[16] This is the meaning Congress clearly intended, as evidenced by the text, structure, and legislative history of the statute. For example, the title of Section 1033 is "Consumer rights to access information," which gives no indication that Congress intended to provide the CFPB the authority to compel banks to share their

---

covered persons to promote the development and use of standardized formats for information . . . " *Id.* § 5533(d).Therefore, Congress only mandated that the CFPB issue "standards" under Section 1033(d), and the CFPB is not required to issue a rule pursuant to Section 1033(a).

[11] S. Rep. No. 111-176, at 173 (2010).

[12] CFPB Summary Judgment Memorandum, *supra* n. 4, at 6.

[13] *Id.* at 6.

[14] 12 U.S.C. § 5481(4).

[15] 12 U.S.C. § 5481(4)); PFDR Final Rule at 90,843.

[16] *Consumer*, Webster New World Compact School and Office Dictionary (4th ed. 2002).

consumers' information with third-party commercial actors.[17] Throughout Section 1033, the word "consumer" is used in a way that could only refer to the individual customer. The statute also refers to information about the "product or service that *the consumer obtained* from" the bank, and a commercial third party does not "obtain" consumer products from a bank.[18] In addition, the statute requires that such information must be "in an electronic form *usable by consumers*."[19] This directive is consistent with the ordinary meaning of the word "consumer" as an individual and is most logically read to ensure that an individual consumer is able to obtain their data in a format that they can download or save for use on their personal computer or print and keep for their records, such as a .pdf or .csv file.[20]

Provisions of the Dodd-Frank Act adjacent to Section 1033 provide further evidence that Congress intended the term "consumer" to retain its ordinary meaning in the context of that section. Section 1032 requires certain disclosures about a "consumer financial product or service" to "consumers" for the purpose of allowing "consumers to understand" the "costs, benefits, and risks" of those products.[21] Section 1034 requires banks to adopt policies for "provid[ing] a timely response to consumers" in connection with a "complaint or inquiry of the consumer."[22] Again, these provisions, like Section 1033, are naturally read to refer to the individual consumer alone and would make little sense in the context of an "authorized third party" data aggregator or fintech.[23]

Despite the clear and natural reading of "consumer" to mean an individual in the context of Section 1033 and adjacent provisions, the PFDR Rule relied on the general definition of "consumer" in Section 1002 of Dodd-Frank to justify mandating that banks share consumer financial data with third-party commercial entities. As noted, that definition includes "an individual or an agent, trustee, or representative acting on behalf of an individual."[24]

The Supreme Court has recognized that a term defined on an "Act-wide" basis does not necessarily carry that statutory definition where "statutory context" and "the overall statutory scheme" indicate otherwise.[25] Here, all textual and contextual indications suggest that the narrower, ordinary meaning of "consumer" applies in Section 1033. A natural reading of Section 1033 does not support the expansion of the definition of "consumer" to include third parties. The PFDR Rule acknowledged that

---

[17] *See Yates* v. *United States*, 574 U.S. 528, 539-40 (2015) (plurality op.) (statutory section title serves as a "[f]amiliar interpretive guide[]").

[18] 12 U.S.C. § 5533(a) (emphases added).

[19] *Id*.

[20] *Id*.

[21] *Id*.

[22] *Id.* § 5534(a), (a)(1).

[23] *See Henson* v. *Santander Consumer USA Inc.*, 582 U.S. 79, 86 (2017) (relying on uses of a term in "neighboring provisions in the Act").

[24] 12 U.S.C. § 5481(4); *see* PFDR Final Rule at 90,843, 90,863, 90,920-21, 90,930.

[25] *Utility Air Regul. Grp.* v. *EPA*, 573 U.S. 302, 316-20 (2014); *see Envt'l Def.* v. *Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (presumption that a term takes its "statutory definition" "readily yields" when required by context). The Sixth Circuit has similarly recognized that courts should not reflexively conclude "that a term defined by statute carries the same meaning every time it is used." *Sanders* v. *Allison Engine Co., Inc.*, 703 F.3d 930, 938-39 (6th Cir. 2012) (relying on ordinary meaning of the word "claim" rather than its statutory definition).

the term "consumer" "is commonly used in various consumer finance-related contexts to refer to individuals,"[26] and principally defined "consumer" that way in the Rule.[27] In short, the general, Act-wide definition simply does not make sense in the context of Section 1033.

ii. *The general definition of "consumer" in the Dodd-Frank Act does not support the PFDR Rule's broad data sharing mandate*.

Even if the Act-wide definition of "consumer" applies, the CFPB still does not have authority to require banks to share consumer data with commercial third-party data aggregators and fintechs, even if they obtain the consumer's "authorization." The terms "agent, trustee, or representative acting on behalf of an individual" are legal "terms of art" that are presumed to have their common-law meaning.[28] 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.[29] The one-time authorization contemplated by the Rule—perhaps provided when the consumer downloads an app—does not convert the third party into the consumer's agent or trustee acting for the benefit of the consumer.[30]

Furthermore, the term "representative" is often defined as including a fiduciary-like relationship in which a representative is "invested with the authority of the principal."[31] Under long-held principles of statutory construction, that term is best understood to have a meaning similar to "agent" and "trustee" in Section 1002.[32] Therefore, in the definition of "consumer," Congress used the word "representative" to include third parties who have some form of duty of loyalty or special relationship with the individual consumer that may not rise to the level of a formal fiduciary relationship.

Fintechs and data aggregators do not have any kind of duty of loyalty or other obligations to act in the consumer's best interests, and the Rule's "authorization" requirements are insufficient to establish

---

[26] PFDR Final Rule at 90,863.

[27] 12 CFR 1033.131 provides that "Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition. Consumer also includes guardians, trustees, custodians, or other similar natural persons acting on behalf of a consumer pursuant to State law."

[28] *See Evans* v. *United States*, 504 U.S. 255, 259 (1992); *see generally Loper Bright Enters.* v. *Raimondo*, 603 U.S. 369 (2024).

[29] *See, e.g.*, Restatement (Third) of Agency § 1.01 (2006); Restatement (Third) of Trusts § 2 (2003).

[30] Consumer Financial Protection Bureau, *Bureau Symposium: Consumer Access to Financial Records, a summary of the proceedings* at 9, https://www.consumerfinance.gov/data-research/research-reports/bureau-symposium-consumer-access-financial-records-summary-proceedings/ ("The Clearing House conducted some research . . . that demonstrated that our consumers unfortunately don't understand what they're agreeing to."); Financial Health Network, Comment Letter on PFDR Proposed Rule, at 8 ("Most consumers . . . are not aware of the role that data aggregators play in the process.").

[31] *Representative*, Webster's Third New International Dictionary (2002); *see Representative,* American Heritage Dictionary (2022) ("[a]uthorized to act as an official delegate or agent").

[32] *See, e.g.*, *Dubin* v. *United States*, 599 U.S. 110, 124-27 (2023) (interpreting the verb "use" in light of narrower verbs listed alongside it). The Uniform Commercial Code similarly defines representative as "a person empowered to act for another, including an agent, an officer of a corporation or association, and a trustee, executor, or administrator of an estate." § 1-201(33)

those duties on the part of third-party commercial entities. Data aggregators, in particular, cannot be viewed as representatives acting on behalf of individual consumers. These entities exist to facilitate the sharing of data and often do so without consumer awareness that their data is likely to be used, stored and monetized by the aggregator. As the CFPB has now acknowledged, "there is no fiduciary relationship, duty of loyalty, or special relationship between a consumer and an authorized third party as defined by the [PFDR] Rule. To the contrary, an authorized third party as laid out in the Rule is a commercial actor broadly allowed to use data for purposes beyond directly serving the consumer."[33]

Indeed, consumers generally have no say at all in whether an aggregator is used or, if so, which one is used. That decision is made by the fintech or other third-party data recipient without any input from the individual consumer. These third parties are free to pursue their own commercial ends through arm's-length relationships with consumers and owe no duty of loyalty to those consumers. In short, these third parties do not remotely resemble fiduciaries or agents and thus fall outside the statutory definition of consumer as an "agent, trustee, or representative acting on behalf of an individual," because they act for their own benefit and not on behalf of an individual. For example, some aggregators use consumer data collected from banks to design and sell fraud prevention tools. The CFPB now agrees that the PFDR Rule's interpretation of the statutory definition of consumer to include authorized third parties "stretches the definition of 'consumer' past its breaking point."[34]

The statutory structure confirms this conclusion. If "representative" meant anyone who "acts on behalf of another," there would be no need to include "trustee" or "agent" in the definition: any remotely plausible trustee or agent would surely be a representative. Furthermore, if a representative is anyone who acts on behalf of another, *the entire list* of "agent, trustee, or representative" is superfluous, because anyone who is "acting on behalf of [the] individual" is a "representative" of the individual and therefore a consumer.[35] Had that been Congress's intent, it could have simply defined "consumer" as "an individual or someone acting on behalf of an individual." As a "cardinal principle of statutory construction," courts construe statutes to avoid such superfluity and "'give effect, if possible, to every clause and word of a statute.'"[36]

Construing the definition of "consumer" to include any third party that could claim to be acting on behalf of a consumer is incompatible with the Dodd-Frank Act as a whole. For instance, in a neighboring provision to Section 1033, Congress required the CFPB to "establish . . . reasonable procedures to provide a timely response to consumers, in writing where appropriate, to complaints against, or inquiries concerning, a covered person."[37] Fintechs are "covered person[s]" because they "provid[e] a consumer financial product or service," but an expansive reading of "consumer" would also make them "consumers" who have a right to complain about other covered persons.[38]

---

[33] CFPB Summary Judgment Memorandum, *supra* n. 4, at 9.

[34] *Id.* at 8.

[35] 12 U.S.C. § 5481(4).

[36] *Williams* v. *Taylor*, 529 U.S. 362, 404 (2000) (quoting *United States* v. *Menasche*, 348 U.S. 528, 538-39 (1955)).

[37] 12 U.S.C. § 5534(a).

[38] *Id*. §§ 5481(6), (6)(A). *See also, e.g.*, *id*. § 5536(a)(1)(A) ("It shall be unlawful for[] . . . any covered person or service provider[] . . . to offer or provide to a consumer any financial product or service not in conformity with Federal consumer financial law.").

The historical record also supports the use of the term "consumer" in Section 1033 to mean an individual or someone with a special, fiduciary-like relationship to the consumer. Many well-known fintechs did not even exist in 2010, and it was not even until 2018 that policymakers conducted "one of the first official [open-banking] discussions in the halls of Congress."[39] If Congress had intended to "broaden and deepen the consumer-permissioned data sharing market" by mandating that banks "share financial data with consumers' third-party representatives," it seems highly unlikely that Congress would have done so through a short, oblique provision addressing only what information banks must "make available *to a consumer.*"[40]

Finally, it bears noting that even if a broader definition of a consumer's "representative" applies, such as one that includes anyone "acting on behalf of" an individual consumer, fintechs and third parties still would not qualify as representatives. "On behalf of" is akin to "for the interest of."[41] When fintechs and aggregators access banks' customers' data, they act in their own commercial interests, not the interest of the consumer. In ordinary usage, we do not say that a provider of goods or services acts "on behalf of" a customer when it provides that good or service.

In sum, as current CFPB leadership has stated, the PFDR Rule "exceeded its authority when it used the term 'representative' as a hook to establish a comprehensive open-banking regulation, instead of adhering to the statutory authority to only make a consumer's information available to that individual consumer or those who are actually acting as agents, trustees, or representatives on that individual's behalf."[42] Therefore, a revised Rule should require data sharing only with an individual consumer and persons with whom the consumer has an established fiduciary or similar special relationship of trust.

III. Defrayment of Costs in Exercising Rights Under Section 1033.

a. *The CFPB lacks the authority to prohibit data providers from charging fees.*

Under the PFDR Rule, a data provider must not impose any fees or charges on a consumer or an authorized third party in connection with establishing or maintaining the required consumer and developer interfaces or receiving requests or making available covered data in response to requests.[43] However, the ANPR rightfully acknowledges that Section 1033 is silent on the question of how the cost of consumers' exercise of the rights it creates should be shared between the consumer and the "covered person."

Indeed, nothing in ***Section 1033 authorizes the CFPB to decide whether banks may charge fees for providing secure access to consumers' sensitive financial data***. That silence is telling because when Congress wants to prohibit private businesses from charging fees, it says so. As the CFPB now

---

[39] Steve Boms, *U.S. Way Behind the Curve on Open Banking*, Am. Banker (Sept. 21, 2018), https://perma.cc/2A8X-T4NC.

[40] 12 U.S.C. § 5533(a).

[41] *See, e.g.*, *Behalf*, Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/behalf ("for the good of or because of"); *On Behalf Of*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/on%20behalf%20of ("in the interest of").

[42] CFPB Summary Judgment Memorandum, *supra* n. 4, at 10-11.

[43] 12 C.F.R. 1033.301(c)(1) and (2).

recognizes, "if Congress had intended to require data providers to make information available under Section 1033 without the ability to charge a reasonable fee, it would have said so expressly."[44] For instance, the Fair Credit Reporting Act mandates that consumer reporting agencies provide required disclosures "without charge to the consumer."[45] Even elsewhere in the Dodd-Frank Act, Congress expressly prohibited certain fees: creditors must provide copies of appraisals to certain loan applicants "at no additional cost to the applicant," and "without charge" to applicants for high-risk mortgages."[46] The CFPB does not have the authority to impose a fee prohibition in Section 1033 that Congress chose not to include.[47] The CFPB has now admitted that the fee prohibition amounts to "a windfall to third parties" that "exceeds [the CFPB's] authority."[48] Furthermore, the CFPB has now acknowledged that the PFDR Rule failed to justify why it did not allow "reasonable fees."[49]

In attempting to support its establishment of the fee prohibition, the PFDR Rule principally relied on the fact that Section 1033 directs banks to make data available to consumers "[s]ubject to rules prescribed by the CFPB."[50] But this phrase merely permits the CFPB to issue rules about the topics addressed in the statute—such as the specific "information relating to . . . transactions" banks must provide, the "formats for [the] information," and so on. Nothing in the statute relates to fees and whether banks may charge them. Furthermore, the U.S. Code is replete with similar boilerplate grants of rulemaking authority, but such general rulemaking language does not empower agencies implementing those statutes to dictate whether and how much businesses may charge for their products and services.[51]

Inferring broad agency authority to prohibit fees would be especially inappropriate in rules related to banking. "[T]he ability to charge fees" has long been recognized as a "fundamental national bank function."[52] In fact, the federal banking regulators charged with ensuring banks' safety and soundness *direct* banks to charge fees "according to sound banking judgment and safe and sound banking principles," taking into consideration "[t]he cost incurred by the bank in providing the service."[53]

---

[44] CFPB Summary Judgment Memorandum, *supra* n. 4, at 12.

[45] 15 U.S.C. § 1681c-1(a)(2)(B).

[46] *Id.* § 1691(e)(4), *id*. § 1639h(c).

[47] *See, e.g.*, *W. Va. Univ. Hosps.* v. *Casey*, 499 U.S. 83, 87-88 (1991) (omission of "expert fees" from a provision authorizing recovery of "attorney's fees" rendered expert fees unavailable, given that the same Congress had addressed those categories separately in other statutes)

[48] CFPB Summary Judgment Memorandum, *supra* n. 4, at 12-13.

[49] *Id.* at 13.

[50] 12 U.S.C. § 5533(a).

[51] *See West Virginia*, 597 U.S. at 723 ("Extraordinary grants of regulatory authority are rarely accomplished through 'modest words,' 'vague terms,' or 'subtle devices.'") (citation omitted). The same analysis applies to the CFPB's attempt to locate its fee-prohibition authority in its broad mission "to prevent evasion of Federal consumer financial law." Final Rule at 90,884; *see* 12 U.S.C. § 5512(b)(1). Whether banks alone must bear the costs of funding the CFPB's mass data sharing regime under Section 1033 is a "fundamental detail[]" of the regulatory scheme that Congress did not authorize an agency to address via "vague terms or ancillary provisions." *Whitman*, 531 U.S. at 468.

[52] *Monroe Retail, Inc*. v. *RBS Citizens, N.A.*, 589 F.3d 274, 280, 283 (6th Cir. 2009).

[53] 12 C.F.R. 7.4002(b)(2).

Interpreting Section 1033 to authorize the CFPB to force banks to provide costly services for free is contrary to these longstanding principles.

The PFDR Rule also attempts to justify the fee prohibition by citing two examples where an agency offered interpretations that banks cannot charge fees for certain services.[54] However, those examples do not support the authority to ban fees because they implement different statutes, have never been blessed by a court, and by their terms apply only in very narrow circumstances (*i.e.*, in the event of an actual error involving billing or charges to consumers' accounts).

Some fintechs and data aggregators have claimed that Section 1033's requirement to "make information *available* upon request" supports the prohibition on fees because the word "available" is sometimes defined as allowing for use "at one's disposal." However, that plainly is not the only definition of "available;" it is also commonly defined to mean "at disposal for sale or utilization."[55] Indeed, Plaid, one of the largest data aggregators, advertises numerous products on its site as "available" but none of them are free.[56] Fintechs and data aggregators have likewise interpreted Section 1033's reference to "consumer rights" to suggest that fees are prohibited. To the contrary, the existence of a right does not necessarily mean it can be exercised for free. For example, the constitutional right of an injured person to receive medical treatment while being arrested does not require that the treatment be free.[57] Similarly, anyone has a right to file a lawsuit, but litigants still pay filing fees.[58]

In sum, none of the interpretations addressed above provide support for the PFDR Rule's prohibition on fees. Current CFPB leadership acknowledges that "there is no indication in Section 1033 that Congress authorized the Bureau to force data providers to establish a separate complex and costly system to make information about consumers available to separate commercial actors, free of charge."[59] A revised PFDR Rule should not address fees and should instead allow market forces to determine access fees for data.

b. *The rule's fee prohibition is not only illegal, but it is bad policy that distorts a well-functioning market.*

Prohibiting data providers from charging fees for providing secure access to banks' customers' data is not only illegal, it is bad policy and contrary to the PFDR Rule's stated objective to "ensure data providers make data available reliably, securely, and in a way that promotes competition."[60] The

---

[54] PFDR Final Rule at 90,884 (citing Regulation E comment 11(c)-3; Regulation Z comment 13-2).

[55] *Available*, Webster's Third New International Dictionary (2002); s*ee also Available*, Cambridge Advanced Learner's Dictionary (4th ed. 2013) ("able to be bought or used."

[56] A feature called "Enrich is available for use in all environments." https://plaid.com/docs/enrich/ But Enrich has a fee: https://plaid.com/docs/account/billing/ ("For Enrich, the flexible fee is based on the number of transactions sent to be enriched.") "An optional paid feature, Beacon Account Insights, is available to customers who want to build their own risk analysis on top of Plaid's Beacon data." https://plaid.com/docs/beacon/

[57] *City of Revere v. Massachusetts General Hosp*., 463 U.S. 239, 245 (1983).

[58] *E.g.*, *Borough of Duryea, Pa. v. Guarnieri*, 564 U.S. 379, 387 (2011) (recognizing a constitutional "right of access to courts") (citation omitted), but litigants still pay filing fees. See 28 U.S.C. § 1914.

[59] CFPB Summary Judgment Memorandum, *supra* n. 4, at 12.

[60] PFDR Final Rule at 90,839.

prohibition creates market distortion, inhibits innovation, and forces data providers to transfer economic value to third parties and data aggregators at significant cost without any compensation. The PFDR Rule argues that fees would obstruct a "data access right," yet presents no evidence to support this assertion. This assertion has proven false. As noted, Plaid and JPMorganChase reached an agreement under which Plaid will pay the bank to access its secure API to obtain the bank's customers' data. Indeed, the CFPB now agrees that "the Rule goes far beyond ensuring that fees do not get in the way of information being made available to consumers and instead forces data providers to bear significant costs in making data available for the open banking system to function."[61]

The robust data sharing ecosystem in the United States has successfully developed through normal market practices in which banks and fintechs or data aggregators enter data sharing agreements. These agreements are made in advance of data sharing by banks, fintechs, and data aggregators to assign responsibilities and liabilities, mitigate potential risks, and address unsafe data-collection practices like screen scraping. They establish the terms and conditions of the arrangement, including how the data is used, how long it is saved, and how it is protected and outline the commercial terms between companies, including fees that data middlemen must pay to securely access consumer data. While banks historically have not charged fees to third parties or aggregators for data access, that model has become unsustainable as the data sharing ecosystem has grown and calls for data have increased exponentially. Banks and fintechs and aggregators should continue to be allowed to negotiate the terms of providing secure data access, as is done in virtually every industry, including with respect to fees.

Prohibiting banks from charging fees to third parties also enables third parties to request more consumer data than is needed to provide the customer with his or her desired product or service. This increases security risks and jeopardizes the resiliency of the banks' APIs. Indeed, some of our members report that they receive billions of data pull requests monthly, of which 90 percent originate from a third party, rather than directly from the consumer.[62] This helps explains why API usage fees are standard practice f to help deter abusive data consumption patterns.[63] Fees will help instill discipline in data calls, thereby protecting consumers from unnecessary data sharing which heightens the risk of their data being stolen and unnecessarily taxes banks' risk-management systems and practices. Indeed, ***data aggregators themselves often charge fintechs and other clients based on the volume of API calls***, yet the PFDR Rule would not provide banks the same ability to negotiate in a competitive marketplace.

The PFDR Rule fundamentally distorts the market for consumer financial products and services by *requiring* banks to create scalable data sharing infrastructure from which fintechs and data aggregators profit, without allowing banks to charge fees to those fintechs and data aggregators. A fee prohibition also contradicts standard business practices relied ***on by data aggregators themselves when facilitating data transfers.***[64] Aggregators charge market rates for data that originates from financial

---

[61] CFPB Summary Judgment Memorandum, *supra* n. 4, at 13.

[62] *See*, e.g., Jeff Kauflin, "Why JPMorgan Is Hitting Fintechs With Stunning New Fees For Data Access," Forbes, (July 22, 2025), Why JPMorgan Is Hitting Fintechs With Stunning New Fees For Data Access.

[63] *See, e.g.,* Amazon (AWS API Gateway Pricing Explained); Microsoft (Microsoft Azure); X (formerly known as Twitter) (About the X API - X), and Google (Platform Pricing & API Costs - Google Maps Platform).

[64] Data aggregators currently share data downstream to their customers in non-standard formats, and the PFDR Rule fails to require aggregators to share data in a standardized format. This is relevant to data providers' ability to charge fees because banks are required to implement a standard that makes it easier for aggregators to connect to bank APIs. However, aggregators' downstream sharing in non-standard formats raises switching costs for third

institutions, with no regulatory constraints on the fees they may impose. Those fees charged by aggregators do not impact the ability of consumers to access their data or of fintechs to use that data to operate their businesses. Prohibiting banks from charging third-party commercial entities for secure data access compels them to subsidize third party business models, while aggregators freely commercialize the same data without limit or oversight.

While the CFPB has no authority to ban banks from charging fees, we highlight the significant costs banks incur ensuring data is shared securely. Banks must invest in technology and develop governance systems that address information security, privacy, and volume considerations. First, there are the fixed costs needed to build and maintain the base system, including but not limited to, authentication routes, customer experiences, access controls, consent management systems, monitoring and alerting, testing, incident management, and third-party risk management processes. Banks invest millions of dollars to stand up such scalable data sharing infrastructure and continue to invest millions year after year to ensure this infrastructure continues to function safely to protect customer data.

Banks also incur significant variable costs in servicing the data requests. Maintaining ongoing daily API access to consumer financial data for millions of accounts and products, across thousands of fintechs and other third-party providers, dramatically grows the traffic demands for a single customer.[65] This, in turn, puts significant pressure on upstream systems and creates risk to traditional servicing channels that depend on those same systems. Providing this service comes with a cost that banks must be permitted to recoup.

In addition, increased data sharing vastly expands the risk that customer data will be stolen and abused, for which banks are often the first line of defense. The costs to investigate customer claims and reimburse customers are significant and should be borne by the entities that failed to safely protect the data. Banks may charge fees to help ensure aggregators and fintechs share in the cost of keeping consumers' data safe and secure.

While banks incur significant costs to keep consumers' data safe and secure, fintechs and data aggregators derive significant value from accessing the secure systems banks have built to allow consumers to share their data securely. Fintechs and aggregators recognize this value, as they are profiting from access and re-use of consumers' sensitive data. Aggregators profit from obtaining data from banks, saving that data into their own systems and selling access to fintech developers to build financial applications. Fintechs then offer a variety of other products and services that rely on consumers' financial data for which they too are paid. Without the ability to obtain consumer data securely, aggregators' and fintechs' business models would be significantly undermined, and banks should be allowed to charge these aggregators and fintechs fees for data access that reflects the value they derive from the data and secure connections used to obtain it

---

parties, thereby stifling innovation. Thus, the PFDR Rule would allow aggregators to lower their own costs and create an ecosystem in which they can entrench themselves and engage in rent seeking behavior.

[65] As just one example, the PFDR Rule requires banks to share data for closed accounts. Sharing closed account information could impose significant costs on data providers, as institutions may have information about thousands, if not millions, of closed accounts. As we noted in our comment letter responding to the PFDR Rule, the rule should not have required providers to share data about closed accounts.

Fintechs recognize the value of the data they are able to access securely from banks, as evidenced by the fact that fintechs pay aggregators for obtaining consumers' data that the aggregator obtains via secure APIs. Aggregators, too, recognize the value of the secure data sharing access banks provide: as noted previously, Plaid and JPMorganChase announced recently an agreement under which Plaid will pay the bank to securely access the bank's customers' data.

The way in which aggregators price their data connections provides further evidence of the value ascribed to consumers' data and the ability of third parties to access the data securely. While there is no difference in the cost for an aggregator to share demand deposit account data and account validation information, publicly available pricing shows that the market prices them vastly differently. The latter is priced at orders of magnitude higher, because information that enables fintechs to initiate payments is *valuable*.

Any revisions to the PFDR rule should not address fees; instead a revised Rule should allow the market to function through regular market operations, which will help maintain a competitive and secure financial system. Allowing market participants to continue to negotiate terms of service, including fees to help cover the costs of building and maintaining the infrastructure, utility, staffing, cybersecurity, and data security, will help banks to maintain the quality and reliability of these systems. It will also encourage more responsible and efficient data-gathering practices from aggregators, minimizing the amount of sensitive consumer financial data in circulation, as well as more robust data security protections.

IV. Information Security Concerns in the Exercise of Section 1033 Rights.

a. *The PFDR Rule's forced sharing of consumer data with third-party fintechs and data aggregators unnecessarily places consumer data at risk.*

As the CFPB has acknowledged, one unfortunate byproduct of the transition to a largely digital information architecture is the increased number of threat vectors to the secure storage and transmission of data. The PFDR Rule attempts to address information security by prohibiting data providers from relying on a third party's use of screen scraping to access the developer interface required by the Rule[66] and discouraging the use of screen scraping by third parties when more secure methods of data access were available.[67] It further requires data providers and third parties to adhere to the applicable information security standards under the Gramm-Leach-Bliley Act (GLBA);[68] and provides that data providers may deny access to consumers or third parties if granting access is inconsistent with policies and procedures reasonably designed to comply with the GLBA's information security standards."[69]

---

[66] 12 C.F.R. 1033.311(e)(1).

[67] PFDR Final Rule at 90,923 ("Once data providers have enabled the safe, secure, and reliable forms of data access envisioned in this rule, the CFPB cautions that screen scraping attempts by third parties to reach data covered by such arrangements could well be limited by the CFPA's prohibition on unfair, deceptive, and abusive acts or practices.").

[68] 12 C.F.R. 1033.311(e)(2).

[69] 12 C.F.R. 1033.321(a)(1)(ii).

However, the PFDR Rule simultaneously increases the risk that consumers' most sensitive data will be compromised while limiting banks in their ability to mitigate that risk to protect their customers. As addressed above, the Rule's fundamental flaw is requiring that sensitive consumer financial data be shared with third parties when the statute only requires that data be shared with the consumer. Not only is the Rule's profound overreach legally invalid, it also unnecessarily introduces a host of information security concerns that would not exist had the PFDR Rule kept within its statutory mandate.

At its core, placing additional copies of consumers' private financial data in the hands of more nonbank third parties increases the opportunities for that data to be stolen, compromised, or otherwise misused. Those third parties are less regulated than banks, which are subject to extensive oversight and supervision by financial regulators.[70] Making matters worse, fintech companies and data aggregators have less experience in safeguarding information and have fundamentally different business models, incentives, and oversight compared to banks. Banks' principal mission is to ensure their customers can securely deposit, access, and use their funds. Fintech companies and data aggregators, in contrast, may offer services to consumers in exchange for targeted advertising or referral fees for other services.[71] Further, their business models often depend on re-sharing consumer data they obtain for free from data providers under the PFDR Rule. This results in the fintechs and aggregators having a reduced incentive to protect the consumer data they re-share because they know that the data providers are likely to face the consequences of data breaches from consumers and regulators.

Banks, under the supervision of their prudential regulators, have expertise in managing these kinds of information security risks. Applying that expertise in the data sharing context, banks have successfully developed and refined practices that balance consumers' desire to use the valuable tools fintech companies provide against the foremost priority of protecting consumers' deposits and private data. The result has been a flourishing and secure private open-banking system.

Rather than increasing consumers' ability to securely access and share their data, the PFDR Rule will impede banks' ability to protect consumers, stifle growth and innovation in data sharing, 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 security breaches, fraud, and misuse of sensitive customer data. A revised Rule should require data sharing only with the consumer herself and not with third parties.

b. ***The PFDR Rule's failure to impose information security obligations directly on fintechs and aggregators places consumer data at risk***.

The PFDR Rule's information security deficiencies are compounded by the fact that it imposes information security obligations ***primarily on the financial institution "data providers" that maintain consumer account information and places minimal direct obligations on the fintechs and data aggregators that access and use the data***. As a result, the CFPB has virtually no role in ensuring that

---

[70] 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").

[71] *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/.

third parties comply with the PFDR Rule. Instead, the PFDR Rule expects banks to ensure the third parties secure consumer data, yet leaves those institutions with no bargaining power or meaningful ability to deny data access requests. In the data sharing ecosystem today, banks that contract with aggregators and fintechs to share data through APIs already impose data security obligations on those third parties to protect their customers' data. Indeed, one of the reasons banks created APIs to share data with third parties was to discourage them from screen scraping, which exposed banks' customers' data to security and privacy risks. Banks have demonstrated they are fully capable of securely sharing customer data with third parties without intervention from the CFPB.

The PFDR Rule threatens to distort the market for consumer data sharing by forcing banks to share data with third parties that might not meet the banks' information security standards. The PFDR Rule then refuses to take any role in ensuring third parties comply with its (relatively light) information security standards for third parties. Third parties that obtain sensitive consumer data should have to adhere to information security standards. Without imposing obligations directly on third parties, the CFPB cannot bring enforcement actions against them for violations of the Rule, which creates an unlevel playing field between banks and non-banks in the consumer data sharing ecosystem. One of the CFPB's core statutory purposes is to ensure that "Federal consumer financial law is enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition . . . ."[72] Imposing the Rule's obligations primarily on data providers contravenes this core purpose. Further, it stands in stark contrast to countries with established open banking regimes where any third party seeking access to consumer data must first receive authorization from the government regulator.[73]

While data providers, particularly those that are regulated financial institutions, conduct due diligence on third parties and aggregators consistent with their third-party risk management obligations, it is not appropriate or feasible for data providers to bear responsibility for ensuring third-party compliance with the Rule's obligations. It is impossible for a data provider to determine whether all the conditions set forth for access by a third party are met for a specific consumer, especially within the short time frames required by the PFDR Rule.

Most importantly, the PFDR Rule's failure to impose direct robust substantive obligations on third parties and data aggregators makes it less likely that these companies will adequately safeguard consumer information, particularly because they are non-banks that likely are not subject to supervision and examination by the CFPB. A fintech that fails to obtain an appropriate authorization disclosure from a consumer, for example, is unlikely to be sued in an enforcement action by the CFPB. Instead, that fintech faces at most, a potential breach of contract lawsuit by the data provider or possibly a future denial of access to the institution's developer interface. But the non-compliant fintech undoubtedly knows that the financial and reputational consequences of a breach of contract suit are minor as compared to the consequences of violating a federal regulation. Further, the non-compliant fintech likely is not subject to supervision by the CFPB and has no reason to expect the CFPB will ever become aware of its failure to adhere to the PFDR Rule. As a result, third parties have less incentive to comply with the PFDR Rule.

---

[72] 12 U.S.C. § 5511(b)(4).

[73] *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).

The risk created for individual consumers from poor data security practices by fintechs and other third-party entities is particularly concentrated among data aggregators. Given the vast access to millions of consumer financial accounts the data aggregators have at their disposal, the potential risk is enormous. Despite having access to over 50% of Americans' financial data,[74] these entities are not subject to the same regulatory oversight on information security as banks. This lack of supervision could lead to a weaker security environment where a single data breach could expose vast amounts of consumer financial data that could cause significant consumer harm.

Lastly, the data security standards that the PFDR Rule expects banks to enforce against third parties are inadequate. While the Rule requires a third party to apply an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA or the Federal Trade Commission's Standards for Safeguarding Customer Information, those requirements are neither specific nor comprehensive enough to address the stringent security protocols that should be followed to protect shared consumer financial data. Fintechs and third parties who obtain data pursuant to the PFDR Rule may not even be covered by the GLBA, and even for those that are, the FTC has no supervisory authority to examine third parties for compliance with information security standards. Therefore, all third parties should be required to maintain an information security program that satisfies the standards set forth in the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook on Information Security.[75] The FFIEC Information Security Handbook standards are more comprehensive and detailed and are the standards by which banks must abide to protect consumer information.

Under the PFDR Rule, nonbanks will be in possession of the same sensitive data that banks are, and every entity to which that data is provided should be held to the same standards to ensure that consumers and their data are adequately protected. The CFPB should directly impose information security requirements on those third parties.

c. ***The PFDR Rule hamstrings banks' ability to protect their customers' data***.

In addition to placing consumer data at greater risk, the PFDR Rule hamstrings banks' ability to protect that data. The PFDR Rule prohibits banks from denying interface access based on risk management concerns, outside of narrow, demanding circumstances on which the CFPB has the last say. The Rule's narrowly drawn limits on banks' exercise of their core risk-management functions conflict with guidance from federal banking regulators, who stress the need for flexible risk management in dealing with third parties.[76]

Under the PFDR Rule, a bank's denial must be "reasonable" which the Rule defines as "[d]irectly related to a specific risk of which the data provider is aware," and "[a]pplied in a consistent and non-

---

[74] See PYMTS, *Report: Half of US Consumers Use Plaid's Payments Tech* (Jan 14., 2025) https://www.pymnts.com/news/payment-methods/2025/report-half-of-us-consumers-use-plaids-payments-tech/.

[75] FIEC Information Technology Examination Handbook Information Security (September 2016), ffiec_itbooklet_informationsecurity.pdf.

[76] *See* Board of Governors of the Federal Reserve System, FDIC & OCC, *Interagency Guidance on Third-Party Relationships: Risk Management*, 15 (June 6, 2023), https://perma.cc/D55F-26YE (hereinafter *Interagency Guidance on Third-Party Relationships*).

discriminatory manner."[77] The PFDR Rule claims—without evidence or reasoning—that "denials made in violation of these procedures carry a significant risk of being pretextual."[78] The net result is that a data provider's compliance with safety and soundness requirements is not sufficient to deny a third party's access to the developer interface because a denial must also meet the PFDR Rule's vague "reasonableness" framework. For example, prudential guidance for third-party risk management directs banks to consider, among other things, changes to a third party's key personnel involved in the activity or a change in business plan. This is a qualitative, not quantitative, consideration and likely would not "directly relate to a specific risk." Nor would a bank likely be able to easily demonstrate why personnel changes at certain third parties create risk and others do not. This creates the very real possibility of a denial that is required by safety and soundness regulations and yet prohibited by the Rule as unreasonable. Indeed, the preamble to PFDR Rule states that "safety and soundness standards … are [a] legal requirement[] that *might* justify denying access," implying that a bank could be subject to a CFPB enforcement action simply for conducting appropriate third-party risk management as required by prudential regulators.[79]

Compounding the problem, the PFDR Rule's criteria for "reasonableness" is vague and unduly restrictive. For a denial to be reasonable, it must be applied in a "consistent" manner. The requirement for consistency is nonsensical in the rapidly changing world of information security. A particular request for access by a fintech might be low risk one day and high risk the next because of a security breach at the fintech overnight. Is denying access to a third party following a breach that affects only 100 customers' data consistent with denying access to a breach involving 1,000,000 customers data? Should a data provider be required to consider whether a breach that exposed only its customers' email addresses is consistent with a breach that exposed its customers' social security numbers? Requiring consistency in access denials is unworkable in the context of third-party risk management, which is highly fact-dependent, and would limit a data provider's ability to make decisions based on changing facts. This is fundamentally at odds with prudential guidance for third-party risk management that directs banks to retain "a flexible, risk-based approach…that can be adjusted to the unique circumstances of each third-party relationship."[80]

,

The requirement that a denial be "directly related to a specific risk of which the data provider is aware" unduly limits a data provider's ability to deny access for valid security reasons. Data providers must anticipate and manage potential risks, not only those that are specifically identifiable and have already occurred, across all facets of their operations. By the time a risk is specifically identifiable, it may be too late to appropriately manage or effectively contain it. This is precisely why third-party risk management guidance permits banks to consider factors like changes in personnel, which may not indicate a specific risk but nonetheless is a legitimate reason banks may use to terminate a relationship with a third party. Given the large number of third parties in the ecosystem, and with further growth expected, it would be virtually impossible for data providers to identify specific risks in all cases and to only deny access in those instances.

---

[77] 12 C.F.R. 1033.321(b).

[78] PFDR Final Rule at 90,901.

[79] PFDR Final Rule at 90,898 (emphasis added)

[80] Interagency Guidance on Third-Party Relationships, at 15.

Risk management requires assessments of the likelihood of various types of risks and managing the possibility of those risks coming to fruition. The recent interagency guidance on third-party risk management takes into account these inherent complexities, noting "sound third-party risk management takes into account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship."[81] To require data providers to only deny access based on a specifically identified risk for each and every third party would not allow data providers to protect consumers' data or their own systems from third parties that may not appropriately manage their own risks.

Bank data providers are subject to robust and comprehensive risk management obligations to ensure that they maintain safe and sound operations, that their data remains secure, and that consumer data is protected. The PFDR Rule's limits on a data provider's discretion to deny access undercuts their ability to manage risk and, as a result, places consumer data at risk. Banks should have broad discretion to deny data sharing requests consistent with the interagency guidance on third-party risk management.

Indeed, data providers must be able to reasonably deny access for a much broader range of risk management considerations. For example, data providers should be able to require third parties to meet minimum risk management standards, such as requiring them to accept liability for unauthorized transfers or data breaches, indemnify data providers for harm resulting from these incidents, requiring third parties to obtain insurance as a backstop to liability, and requiring third parties to undergo routine audits.

Tellingly, *data aggregators themselves* require third parties to meet similar risk management standards before sharing data with those parties. Aggregators' contracts with their own customers often require those customers to indemnify the aggregator for data breach losses, to maintain cybersecurity and other liability insurance, and generally to accept liability for certain events.[82] Data providers should similarly be able to require these sensible protections before sharing consumer data with data aggregators or third parties.

Requiring third parties to accept liability, indemnify data providers, and obtain insurance as a backstop not only helps ensure that liability is borne by the parties responsible for the harm that occurs, but also helps ensure that third parties take their obligations seriously, particularly those related to data security, given the risk of consumer harm and financial consequences. Without the risk of loss, third parties do not have a financial incentive to prioritize data security or protecting consumers or the overall security of the ecosystem, especially where the loss of compromised credentials only impact accounts held elsewhere. Thus, the refusal of third parties to agree to reasonable terms to help ensure the overall security of the ecosystem should serve as a reasonable basis on which the data provider may deny access.

The PFDR Rule further limits data providers' ability to protect their customer data by not explicitly permitting them to obtain data sharing authorization directly from the consumer. Any revised rule should permit data providers to obtain their own consumer authorization to make available some or all of the consumer's data according to the consumer's express informed consent. The manner and

---

[81] *Id*.

[82] *See, e.g.,* Plaid Master Services Agreement (Nov. 27, 2023), https://www.sec.gov/Archives/edgar/data/2069448/000206944825000001/Plaid_msa.htm

circumstances of the authorization would be within the data provider's control, providing consumers additional protection from unfair, deceptive, or abusive third-party authorization procedures. Data providers would gain significant legal protection from the fact that they are then transmitting the consumer's data in accordance with a legal, and properly obtained, data provider authorization.

In addition, data providers must also be able to authenticate a consumer's identity and identify the scope of the data requested as a necessary precondition for data transmission to the consumer, as a data security control measure. Furthermore, a data provider also must be able to authenticate a third party's identity that is requesting data on behalf of a consumer before responding to a request. Similarly, just as data security best practices lead banks and many fintechs to require reauthentication periodically on their own platforms, data providers should be permitted to require periodic reauthentication and reauthorization for consumer data sharing requests. If anything, authentication standards should be stricter when consumers seek to share sensitive data with a third party versus accessing a data provider directly.

d. *The PFDR Rule's failure to ban screen scraping or require third party use of the developer interface puts consumer data at risk.*

While requiring data providers to establish and maintain a developer interface, the PFDR Rule neither requires authorized third parties to use the developer interface nor prohibits them from screen scraping in the consumer interface, the riskiest method of accessing consumer financial data. Screen scraping requires the individual consumer to share their login credentials with a third party that uses those credentials to log in behind the scenes as if they were the individual, and the PFDR Rule repeatedly acknowledged "screen scraping's inherent overcollection, accuracy, and consumer privacy risks;"[83] that "screen scraping creates data security, fraud, and liability risks for data providers,"[84] and that there is "nearly universal consensus that developer interfaces should supplant screen scraping."[85] Yet, rather than prohibit screen scraping, the PFDR Rule assumes "the market [will] move away from screen scraping" based on the onerous obligations put on data providers regarding developer interfaces.[86]

This assumption fundamentally undermines consumer data security. Individual consumers are generally not made adequately aware of the dangerous implications of sharing their credentials for the purposes of screen scraping. For example, because third parties who screen scrape store consumers' login credentials, these entities could move money or make payments without consent and in violation of the terms of the individuals' bank. Screen scraping is an imprecise and brittle technology that has resulted in incidents at banks such as the inadvertent sharing of sensitive data (*e.g.*, plain text account numbers) or the wholesale changing of settings (*e.g.*, language preferences).

While data providers may have the ability to block screen scraping, consistent with prudential risk management practices, blocking it is difficult and costly, even for the largest financial institutions. And it is getting harder. Banks make significant investments in data scanning, analysis, and remediation technologies to protect customers and their data from screen scraping, but scrapers continue to find

[83] PFDR Final Rule at 74,813.

[84] *Id.* at 74,854.

[85] *Id*. at 74,798.

[86] *Id*. at 74,798.

novel workarounds (*e.g.,* data scraping via Interactive Voice Response systems and reverse engineering of banks' APIs), making it nearly impossible for banks to fully protect their customers' data from this activity. The rise of artificial intelligence ("AI") is especially worrisome in this context, as banks anticipate confronting third-party AI agents as autonomous interactors who log into consumer accounts as if they were that consumer with the ability to take actions on that account. A future where undetectable AI agents have proliferated and cannot be trusted to act exactly as consumers intend presents a new and significant threat to the financial security of consumers.

And even when screen scraping is blocked, consumer data continues to be at risk because the third party retains the consumer's credentials. At a minimum, data providers should be able to deny developer interface access to any third party or aggregator that has attempted to screen scrape data available via the provider's consumer interface within a specified time period.

e. *The PFDR Rule's forced sharing of payment initiation information exceeds Section 1033's authority and exposes consumers to fraud and unauthorized transfers of funds.*

Section 1033 requires banks to provide information about a customer's account: "information relating to any transactions, series of transactions, or to the account including costs, charges and usage data." [87] 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.

The PFDR Rule requires data providers to make available to third parties, among other things, "information to initiate payment to or from a Regulation E Account." Requiring disclosure of this fundamentally different piece of information goes beyond the scope of Section 1033. Section 1033, which authorizes only the *sharing* of information about a financial product or service. Yet the PFDR Rule 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 CFPB itself has previously recognized, "[a]uthorized data access . . . is not payment authorization." [88] Section 1033 does not authorize the CFPB 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. Thus, a revised Rule should not require data providers to share payment initiation information because the CFPB has no authority to do so.

Further, requiring the sharing of payment initiation information significantly increases the risk of fraud and unauthorized transactions to consumers, which in turn increases potential liability for banks. Open banking schemes in both the E.U. and the U.K. clearly distinguish between "account information services" and "payment initiation services," and require significantly heightened supervision, liability, and security for "payment initiation services" to appropriately protect consumers. None of these

---

[87] 12 U.S.C. § 5533(a).

[88] Consumer Financial Protection Bureau, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, at 4 (Oct. 8, 2017), cfpb_consumer-protection-principles_data-aggregation.pdf.

.

protections are present in the PFDR Rule. In fact, the PFDR Rule does not even place direct obligations on third parties or data aggregators, much less require that third parties be supervised by the CFPB or be liable if their practices allow fraudulent payments to be initiated from a consumer's account. Requiring sharing of payment information, especially without mandating appropriate obligations on those receiving the information, greatly increases the risk of consumer harm. Indeed, some of our members report that the rate of unauthorized payment claims increased substantially—by *300 percent or more*—for transactions generated as a result of deposit account numbers shared with aggregators and third parties.

While sharing Tokenized Account Numbers ("TANs") rather than actual deposit account numbers reduces some of the potential for fraud, it does not eliminate all forms of fraud or resulting losses or harm from a PFDR rule that requires the sharing of payment initiation. To be sure, banks must have the option to share TANs in cases where they do share account information. TANs grant consumers greater control over their account data because they can limit sharing to specific third parties by disabling individual TANs without needing to close their account. TANs also can be helpful in containing the damage after a breach of account numbers has been definitively identified. But requiring the sharing of account numbers still increases the risk of fraud, and, critically, still exceeds the CFPB's statutory authority.

The PFDR Rule's reliance on Regulation E as mitigating these risks is misplaced, as Regulation E's provisions do not adequately address potential harm to consumers from sharing payment initiation information. Regulation E essentially places all liability for error resolution and making consumers whole for unauthorized transactions on banks. While this policy decision may have been appropriate when Regulation E's enabling legislation was first enacted in 1978, it is patently inadequate in the modern consumer data ecosystem, particularly when the PFDR Rule requires banks to share sensitive payment initiation data with commercial third parties.

The liability and consumer protection provisions of Regulation E were not drafted in consideration of data aggregators and third parties originating transactions from consumer accounts, and important questions remain unaddressed about the application of Regulation E's provisions regarding service providers, access device restrictions, error resolution, and various required consumer notices. Without properly addressing these concerns and establishing clear liability and indemnification rules that place responsibility on data aggregators or third parties for the payments they initiate, consumers will not be sufficiently protected. Further, the requirement to make payment initiation information available will expose data providers to costly regulatory and external risks that they cannot measure, mitigate, or control. The PFDR Rule should not have required data providers to share payment initiation information, nor should any revised Rule do so.

f. ***The PFDR Rule's failure to allocate liability for security breaches will cause consumer harm***.

Despite the PFDR Rule's establishment of a mass-dating sharing mandate, it does not prescribe liability rules for when consumer data is inevitably misused or compromised. As the preamble to the PFDR Rule acknowledged, "commenters, academic researchers, and research institute[s] . . . predicted that the final rule would increase the volume of sensitive financial data accessed by third parties, particularly sensitive information to initiate a payment," which would "increas[e] the risk of

unauthorized transactions or other harms."[89] Existing liability regimes generally hold banks responsible for investigating and compensating for unauthorized transfers.[90] But these frameworks were not designed for the CFPB's mandatory open-banking regime, where massive amounts of data are transmitted to "aggregators and third parties that . . . may not have the same liability or responsibilities [as banks] . . . even where they are at fault."[91] Because of these dynamics, many commenters urged the CFPB to "mandat[e] a comprehensive approach to assigning liability or safe harbors for [banks]."[92]

The foundation of any such framework should have liability "follow the data," which means once a bank shares customer-permissioned data with a fintech or other third-party provider, liability for fraud, data breaches, or other issues and errors involving that data should sit with the fintech or other third-party provider where an incident happens. This is the approach being adopted in Canada following a series of working groups dedicated to considering how that country should manage liability issues in the open banking context.[93]

The PFDR Rule attempted to explain this failure by asserting that "[a]pplicable payment authorization requirements continue to separately apply," existing liability frameworks under "private network rules, contracts, and other laws" were sufficient to address any increased liability.[94] This assertion is wrong. Data aggregators and fintechs have ***no incentive to bargain for liability allocation when the PFDR Rule requires banks to share data for free subject to traditional liability arrangements***.[95] And "other laws" do not fairly allocate liability to the actor responsible for breaches: they largely constrain banks' ability to pursue indemnity and contribution from the parties actually at fault.[96] Indeed, as discussed above, one of the "other laws" on which the Rule relies is Regulation E, which essentially places on banks all responsibility for error resolution and making consumers whole for unauthorized transactions.

Moreover, the PFDR Rule's reasoning as to unauthorized payments fails to address the key problem: that in a regime that forces banks to share "information to initiate payment" with *thousands* of unregulated third-party companies with very limited ability to control that sharing, adherence to the "applicable payment authorization requirements" is orders of magnitude more costly and complex.

---

[89] PFDR Final Rule at 90,846; *see* Bank Policy Institute and The Clearing House Comment Letter on PFDR Proposed Rule at 7, 49, 51-52, 78-79; JPMorganChase, Comment Letter on PFDR Proposed Rule at 10, 54; Consumer Bankers Association, Comment Letter on PFDR Proposed Rule at 3, 26-27, 48.

[90] *See* 12 C.F.R. 1005.6, 1026.13.

[91] JPMorganChase, Comment Letter on PFDR Proposed Rule, at 9.

[92] PFDR Final Rule at 90,846-47.

[93] *See* https://www.canada.ca/en/department-finance/programs/financial-sector-policy/open-banking-implementation/2024-fall-economic-statement-canadas-complete-framework-consumer-driven-banking.html.

[94] PFDR Final Rule at 90,847.

[95] *See, e.g.*, Consumer Bankers Association, Comment Letter on PFDR Proposed Rule at 48-50; JPMorganChase, Comment Letter on PFDR Proposed Rule at 9; Bank Policy Institute & The Clearing House, Comment Letter on PFDR Proposed Rule at 10, 80.

[96] *See, e.g.*, *Mich. First Credit Union* v. *T-Mobile USA, Inc.*, 108 F.4th 421, 430 (6th Cir. 2024) (holding that financial institutions lack a right of action to seek indemnification under the Electronic Funds Transfer Act, and that the Act simultaneously bars banks from seeking indemnification under state law).

However, the PFDR Rule did not address or even dispute that the natural and inevitable consequence of its unlawful mass data sharing regime would be more unauthorized or fraudulent payments.[97] Neither existing liability principles nor private network rules were designed—or are suited—for the Rule's mass data sharing mandate. Furthermore, fair apportionment of liability would serve as incentive for fintechs, data aggregators, and other third parties to ensure that they implement and maintain robust data security protections.

The PFDR Rule's reliance on its other features "to mitigate unauthorized transfer and privacy risks to data providers and consumers" increases risk of consumer data breaches.[98] It is indisputable that substantially more consumer data will be transferred pursuant to the Rule, resulting in more data compromise. The PFDR Rule requires this data transfer without adequately protecting consumers or data providers from the costly consequences or requiring third parties to appropriately safeguard the data they receive. Liability should "follow the data" and require the party responsible for a data breach bear liability for any negative consequences to the consumer. Indeed, as noted previously, data providers should be able to require third parties seeking access to consumer data to meet obligations reasonably designed to enable data providers to manage the risks associated with sharing consumer's data with third parties, including requiring third parties to accept liability for unauthorized transfers or data breaches, indemnify data providers for harm resulting from these incidents, obtain insurance as a backstop to liability, and undergo routine audits.

g. ***The CFPB agrees that the PFDR Rule's overall framework places consumer data at significant risk.***

Individually, any one of the failings described above is likely to cause substantial harm to consumers: forced sharing of data with third parties, including highly sensitive payment initiation information; declining to impose any direct obligations on third parties or data aggregators; allowing screen scraping of the consumer interface to continue; and relying on existing liability regimes for data breach that were not designed for mass data sharing.

The CFPB now agrees with the assessment that Rule unlawfully puts consumers' data at risk, highlighting that the PFDR Rule greatly expanded the scope of Section 1033 to encompass a vast data sharing framework, inviting greater risk to consumer privacy and data security.[99] The CFPB further agrees that the aggregate effect of the PFDR Rule "led to a data sharing framework that poses unacceptable risk to the security of consumer data . . ."[100] Taken as a whole, the PFDR Rule is not only unlawful, but indefensible from a policy perspective.

V. <u>Privacy Concerns in the Exercise of Section 1033 Rights</u>.

a. ***The PFDR Rule's failure to address the role of data aggregators in the data sharing ecosystem unjustifiably poses risks to consumer privacy.***

---

[97] PFDR Final Rule at 90,847-48.

[98] *Id.* at 90,848.

[99] CFPB Summary Judgment Memorandum, *supra* n. 4 at sections I.A. and I.C.

[100] *Id*. at 16.

As we have consistently articulated, consumers must have control over their data, and their data should be subject to the same robust protections when a consumer authorizes a third party to access their data as it is when the data resides with a bank.

Unfortunately, while there have been many benefits to consumers from the expansion of consumer data sharing, there are still significant data security and privacy risks to consumers that result from the mass transfer of consumer data among banks and other entities, and consumers may not fully appreciate these risks. For example, consumers generally lack an understanding of how their financial information is being collected, shared, and stored. A 2021 survey conducted by The Clearing House found that more than 80% of financial app users are not aware that apps may use third parties to access consumers' personal and financial information, 78% didn't know aggregators regularly access personal data even when the app is closed or deleted, and 73% of financial app users are not fully aware that apps or third parties may store their bank account username and password.[101]

The PFDR Rule does not sufficiently protect consumer data privacy. While the rule requires third parties to obtain "authorization" from a consumer to seek access to his or her sensitive financial data, the Rule effectively requires only that a consumer click "accept" on a disclosure form that recites the third party's obligations under the Rule, which are insufficient to protect consumer data privacy. The Rule's disclosure framework can also be cumbersome for consumers to process or fully understand. It seems likely that consumers would treat the current authorization disclosures as "legalese" that they do not read or fully understand. This is especially true if the fintech or other third-party provider is seeking permission for multiple use cases, since this would likely involve many screens that may overwhelm the consumer with information. The consumer authorization process should be seamless, intuitive, and easily digestible to ensure that consumers give appropriate informed consent for data sharing. This should include the use of clear and conspicuous language to explain what data will be accessed, how often, by whom, for how long, and in what manner. This framework should also include a clear and simple process for withdrawing consent for any or all use cases.

Furthermore, consumers have no insight into or choice over whether the authorized third party involves a fourth-party data aggregator to access their information. Many data aggregators not only enable access to data, but they also collect the data and manipulate the format or other aspects of data to suit the needs of their customers. Data aggregators typically retain the data that is collected, and, in some cases, use it for their own purposes without consumers' express informed consent.[102]

---

[101] The Clearing House, Consumer Survey: Data Privacy and Financial App Usage, December 2021, available at: 2021-tch-consumersurveyreport_final.pdf.

[102] Indeed, all the large data aggregators in the U.S. have been sued for unauthorized collection, use, and sale of consumer data. *See* "Judge approves settlement ordering Plaid to pay $58 million for selling consumer data," Courthouse News Service (July 20, 2022), available at https://www.courthousenews.com/judge-approves-settlement-ordering-plaid-to-pay-58-million-for-selling-consumer-data/; "MX Technologies Hit With Lawsuit Accusing Fintech Firm of 'Screen Scraping' and Selling User Bank Account Data," Law.com (Apr. 28, 2023), available at https://www.law.com/therecorder/2023/04/28/mx-technologies-hit-with-lawsuit-accusing-fintech-firm-of-screen-scraping-and-selling-user-bank-account-data/; "Consumer Advances Info-Broker Suit Against Mastercard's Finicity," Bloomberg Law (Feb. 14 ,2024), available at https://news.bloomberglaw.com/litigation/consumer-advances-info-broker-suit-against-mastercards-finicity; "Envestnet and Yodlee Sued In Data Privacy Class-Action," Law Street Media (Aug. 31, 2020), available at https://lawstreetmedia.com/news/tech/envestnet-and-yodlee-sued-in-data-privacy-class-action/.

Given the proliferation of fintechs and their resulting use of data aggregators to provide quick and easy access to multiple data sources, data aggregators have been able to accumulate massive amounts of consumer financial data. Banks have legal obligations to safeguard customer data and comply with strict regulatory requirements related to privacy and security and have put decades of effort into protecting their customers and institutions. In comparison, neither data aggregators nor fintechs are required to apply to their systems an information security program that satisfies the standards set forth in the FFIEC Information Technology Examination Handbook on Information Security.

Relatedly, the PFDR Rule permits data aggregators to share a consumer's data with *other third parties* without the consumer's permission or even knowledge.[103] And data aggregators have virtually unchecked ability under the Rule to use consumer data "to improve the product or service the consumer requested," even if using consumer data in this way entails "provision of covered data . . . to other third parties."[104] Therefore, data aggregators can unilaterally choose to use the data they are purportedly obtaining "on behalf of consumers" in these ways, without any ability of consumers to control those actions. Data aggregators under the PFDR Rule also do not share the record retention or reporting requirements of data providers, so determining the extent to which consumer data has been shared to additional less-regulated third parties may not be possible in the event of a data breach.

The PFDR Rule's defines a data aggregator as a "person that is retained by and provides services to the authorized third party to enable access to covered data."[105] This definition significantly understates the role of the data aggregator in the data sharing ecosystem. Data aggregators do not merely enable access to covered data, they often retain that data, manipulate it and sell it to third parties for various commercial purposes. In light of many data aggregators' access to, use, and storage of a substantial volume of sensitive data, the PFDR Rule should have directly required them to implement and maintain robust data security, privacy, and consumer protections, as well as ensured fintechs and aggregators are directly supervised by federal regulators. Additionally, the PFDR Rule should have prohibited data aggregators from using consumer data for their own purposes (*i.e.*, *anything* beyond what is needed to enable data sharing with the third party to provide the consumer's desired product or service) and required that the aggregator delete the data after passing it along to a fintech or other third-party provider. Requiring deletion as the baseline expectation for aggregators would help mitigate the privacy and data security risks consumers face from these entities. As it stands, the PFDR Rule would permit data aggregators to collect, use, and monetize consumer data for a myriad of purposes. Any revised rule should directly cover data aggregators and impose all of the obligations described above.

b. *The PFDR Rule's failure to ban screen scraping exacerbates consumer privacy concerns that exist in the market today.*

As explained in part V.b above, the PFDR Rule neither prohibits third parties from screen scraping the consumer interface nor requires third parties to use the developer interface when one is available. Any rule that permits screen scraping to continue necessarily poses significant risk to consumer privacy, particularly by data aggregators who store and monetize consumer data for myriad purposes. These data aggregators work in the background, often unbeknownst to consumers. As a

[103] *See* 12 C.F.R. 1033.421(f).

[104] *Id*. at 1033.421(c).

[105] *Id.* at 1033.131.

result, consumers may be unaware that (1) they are providing their credentials to a third-party data aggregator, rather than directly to a bank; (2) their credentials or data could be further shared and/or used beyond their initial authorized access; and (3) through screen-scraping, data aggregators can gain access to data attributes beyond those needed to provide the product or service requested by the customer.

In order to protect consumer privacy, the rule should have ensured that the consumer data shared is limited to what is absolutely necessary for the product or service the consumer requested, including by prohibiting screen scraping by third parties or data aggregators and requiring them to use the developer interface.

VI. Compliance Dates.

a. *The PFDR Rule did not provide sufficient time for data providers to come into compliance with its requirements given its reliance on standard setting bodies and consensus standards.*

As noted in Part I, banks currently face an untenable situation regarding the existing compliance deadlines. It is imperative that the CFPB act as expeditiously as possible to suspend those compliance deadlines in the PFDR Rule.

In addition, the compliance timelines established in the PFDR Rule were much too short given the PFDR Rule's reliance on standard setting bodies and consensus standards. First, the CFPB's decision to set fixed deadlines for banks to come into compliance with a Rule that (under the CFPB's design) was not even fully articulated is unreasonable. The PFDR Rule in numerous places purports to define substantive compliance by reference to "consensus standards" set by private organizations. Those standards naturally would be afforded great weight by industry participants trying to understand what the PFDR Rule would require of them.[106] It therefore makes little sense to require banks to begin spending resources to come into compliance by a date certain before any such standards have been issued. That approach would penalize banks who undertake compliance measures earliest, because once standards are announced, they may be forced to incur substantial time and expense to redo their work to conform to those standards. Despite these concerns, the PFDR Rule set fixed and rapidly approaching compliance dates that were not tied to the issuance of consensus standards.

Second, when the PFDR Rule was issued, the CFPB had not recognized any standard setters. Since that time, it has recognized only one, and that organization applied only to issue standards concerning technical data formatting issues, not the standards regarding substantive regulatory mandates.[107] Now that the CFPB has reopened the PFDR Rule, it is highly unlikely that any substantive consensus standards will be issued in the foreseeable future.

The PFDR Rule acknowledged that "[m]ost commenters" requested "that compliance dates account for the timeline for development of consensus standards."[108] And in its preliminary final rule about how it would select standard-setting organizations, the CFPB explained that "waiting to finalize the

---

[106] *Ass'n of Am. R.R.*, 721 F.3d at 672.

[107] *See Financial Data Exchange, Inc.*, CFPB No. 2024-CFPB-PFDR-0001 (Jan. 8, 2025).

[108] PFDR Final Rule at 90,859.

provisions" governing selection of standard setters would "increase[] costs to industry of complying with any substantive compliance requirements" those organizations set.[109] Yet the Rule inexplicably prescribed a compliance timeline where the clock is ticking regardless of when standards are set.

The PFDR Rule's existing compliance timeline is unreasonable because it is not tied to the promulgation of the consensus standards that the PFDR Rule made fundamental to compliance with that rule. But banks cannot build toward compliance with standards that do not exist. And if a revised PFDR Rule also relies on consensus standards, any steps data providers take toward compliance without final consensus standards come with the substantial risk of being wasted in the event that they must unwind and redo that work to adapt to subsequently issued standards.

b. ***Any final rule should allow for at least a 24-month implementation period*.**

As articulated in multiple comment letters and elsewhere, at a minimum, the CFPB should allow large data providers at least a 24-month implementation period from either the final rule or, if relevant, the establishment of final consensus standards. Implementation will be a time-consuming endeavor, which likely will require, among other things, the development of new technical capabilities, the enhancement of certain public-facing products and websites, and the establishment of appropriate policies and procedures on a range of subjects. All of those changes take even longer when they must be developed and rolled out while ensuring that existing developer interfaces remain fully operable. Though data providers have already begun their compliance efforts for the PFDR Rule, they do not yet know whether or how those efforts will be useful for a revised Rule.

Indeed, complying with the Rule may require banks to:

- Update public-facing websites to meet the final rule's public disclosure requirements;
- Generate and publish performance metrics to align with the CFPB's new definitions;
- Ensure data is provided in a (currently unknown) standardized format;
- Enable support for required data elements not currently shared (such as, for example, bill payment data, certain terms and conditions);
- Develop and operationalize the policies, procedures and processes required under the Rule;
- Upgrade underlying technology infrastructure to meet API performance standards;
- Build new functionality pertaining to "machine readable" files accessible by consumers;
- Manage new maximum access duration requirements;
- Build and operationalize processes to notify third parties of developer interface denials and consumer access revocations;
- Update customer service operations to account for the new scope of activities and functionality;
- Perform robust testing to ensure safe and resilient implementation of new functionality; and
- Adapt current data access agreements and third-party oversight processes.

Further, a revised Rule could include more or different obligations that may require additional compliance investments by data providers. Importantly, depending on the scope of the revised Rule, implementation may require extensive work and coordination between different private entities to

[109] Consumer Financial Protection Bureau, *Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting, Final Rule*, 89 Fed. Reg. 49084, 49,089 (June 11, 2024).

amend existing agreements or put in place new or revised technology protocols. This process, too, will take time.

* * *

We appreciate the CFPB's recognition that the PFDR Rule exceeds the CFPB's authority and should be substantially revised. Section 1033 neither requires nor authorizes the CFPB to regulate the innovative consumer permissioned data sharing ecosystem in the United States. Furthermore, the PFDR Rule would interfere with the robust and competitive consumer permissioned data sharing ecosystem and place consumers and their data at significant risk.

We support the CFPB's substantial narrowing of the Rule, consistent with the authority Congress granted the agency. Revising the PFDR Rule in line with a faithful reading of Section 1033 would allow individuals to continue to have access to their financial information as they do today, and to continue to grant third parties access to their data in a way that protects the security and privacy of that data.

We would welcome the opportunity to discuss this request with you further. Please contact me at (703) 887-5229 or paige.paridon@bpi.com to schedule time to discuss or with any questions.

Respectfully submitted,

/s/ Paige Pidano Paridon

Paige Pidano Paridon
EVP, Senior Associate General Counsel &
Co-Head of Regulatory Affairs
Bank Policy Institute