Jack E. Hopkins, Chairman
Alice P. Frazier, Chairman-Elect
Michael J. Burke, Jr., Vice Chairman
Quentin Leighty, Treasurer
Douglas E. Parrott, Secretary
Lucas White, Immediate Past Chairman
Rebeca Romero Rainey, President and CEO

October 21, 2025

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: Advance Notice of Proposed Rulemaking – Personal Financial Data Rights Reconsideration [Implementation of Section 1033 of the Dodd-Frank Act]

Dear Acting Director Vought,

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to provide feedback in response to the Consumer Financial Protection Bureau's (CFPB) Advance Notice of Proposed Rulemaking (ANPR) on implementing Section 1033 of the Dodd-Frank Act.[2] The ANPR specifically seeks public input on (1) who can serve as a "representative" making a request on behalf of the consumer; (2) the optimal approach to the assessment of fees to defray the costs incurred by a data providers; (3) the threat and cost-benefit picture for data security and data privacy associated with section 1033 compliance.

Summary of ICBA Position:

1) **Expand the Exemption for Small Data Providers:** The 2024 rule exempted banks with less than $850 million in assets – which are defined as "small businesses" by the Small Business Administration (SBA) – from the requirement to create and maintain a third-party developer interface through which to share customer data. The CFPB should expand this threshold, exempting all community banks with assets $10 billion and under from the rule's requirements.

2) **Limit Mandatory Data Sharing to Third Parties that Act in the Consumer's Best Interest:** The Bureau should adhere to the explicit text of the Section 1033 statute, requiring data sharing only with the customer and third parties that are bona fide

[1] The Independent Community Bankers of America® has one mission: to create and promote an environment where community banks flourish. We power the potential of the nation's community banks through effective advocacy, education, and innovation. As local and trusted sources of credit, America's community banks leverage their relationship-based business model and innovative offerings to channel deposits into the neighborhoods they serve, creating jobs, fostering economic prosperity, and fueling their customers' financial goals and dreams. For more information, visit ICBA's website at https://www.icba.org/.
[2] 90 Fed. Reg. 40986, available at: https://www.govinfo.gov/content/pkg/FR-2025-08-22/pdf/2025-16139.pdf.

agents, trustees, or representatives of the consumer. Data sharing with third parties that retain and use consumer data to refine their own products and services in ways that are not beneficial to the consumer should not be required by the rule.

3) **Allow Banks to Charge a Reasonable Fee for Developer Interface Access**: Banks should be permitted to charge a reasonable fee for providing access to consumer information to third parties. The fees should allow the bank to recover the cost of creating and maintaining the developer interface, ensuring customer data can be shared securely, and to earn a fixed rate of [][return]. In order to prevent large financial institutions from abusing their market power and preventing their customers from sharing access to their information, fees should not be unlimited or excessive.

4) **The Bureau Should Oversee Larger Third-Party Data Recipients to Ensure They Protect Consumers' Private Data:** The Bureau should supervise and examine larger third-party data recipients to ensure they are in compliance with the requirements of the Personal Financial Data Rights (PFDR) rule, including the rule's data security requirements. Data providers should not be required to share customer information with any third-party unless they are regularly supervised and examined by the CFPB or by a federal prudential regulator (the FDIC, the OCC, the Federal Reserve Board, or the NCUA).

Background on Section 1033

Section 1033 of the Dodd-Frank Act mandates that covered financial institutions must provide consumers and authorized third parties with access to financial transaction data upon request, subject to rules established by the CFPB.

On November 18, 2024, the CFPB issued the Personal Financial Data Rights (PFDR) Rule to implement Section 1033. The PFDR Rule required covered data providers—such as banks with more than $850 million in assets and credit card issuers—to share customer transaction history, account fee information, and usage data with consumers upon request through an API-enabled developer interface. Banks would have been prohibited for charging any cost associated with the creation or maintenance of the developer interface. The rule also outlined procedures for data access and third-party authorization.

However, a lawsuit filed in the Eastern District of Kentucky challenged the rule, alleging that several aspects of the rule exceeded the Bureau's statutory authority.[3] On July 29, 2025, the court stayed the proceedings after the CFPB announced plans to reexamine the rule in order to address its shortcomings.

[3] *See Forcht Bank, N.A. v. CFPB,* No. 5:24-cv-00304 (E.D. Ky. 2024).

Expand the Exemption for Small Data Providers

The 2024 PFDR Rule recognized that creating and maintaining a developer interface would be a significant burden for small community banks and therefore exempted all banks defined as small businesses by the SBA (banks below $850 million in assets).[4] Although this ICBA-advocated exemption brought regulatory relief for some community banks, we urge the CFPB to expand its scope to exempt a greater number of small depository institutions. Market forces, rather than top-down regulation, should drive this technological shift.

Community banks will likely depend on their core processors to create and maintain a developer interface and have no meaningful ability to negotiate with their core on the price of the service. Switching core processors is challenging due to the complexity of data management, making it unlikely for banks to undertake costly and time-intensive core conversions—often costing hundreds of thousands of dollars and taking years—just to access a more affordable developer interface. This locks banks into their existing core processor's pricing with limited negotiation power.

Additionally, while community banks could hire third-party vendors to develop and manage a developer portal, this involves extensive due diligence and complex integration with existing systems. For community banks with limited IT budgets and staff, vetting vendors and ensuring compliance with new regulations pose a significant burden, further exacerbating the financial and operational strain of compliance.

Exempting community banks from this rule is consistent with the Bureau's statutory authority. First, when engaging in rulemaking, the Bureau is required to consider the potential benefits and costs to consumers and covered persons, including the potential reduction of access by consumers to consumer financial products or services resulting from such rule; and the impact of proposed rules on [banks and credit unions with less than $10 billion in assets], and the impact on consumers in rural areas."[5]

Second, the Bureau's rulemaking authority gives it the ability to "conditionally or unconditionally exempt any class of covered persons, service providers, or consumer financial products or services, from any provision of [Federal consumer financial law], or from any rule issued under [Federal consumer financial law], as the Bureau determines necessary or appropriate to carry out the purposes and objectives of [Federal consumer financial law]."[6]

Analyzing these considerations, the benefits to consumers of requiring community banks to comply with this rule appear small while the costs are significant. The proposed rule would prohibit banks from passing on the costs of creating a developer portal to customers or third

[4] 12 CFR 1033.111(d)
[5] 12 USC 5512(b)(2).
[6] 12 USC 5512(b)(3).

parties directly, but these costs could have an adverse impact on consumers in the form of higher interest rates, reduced lending capacity, or reduced access to free checking accounts.

These costs are not offset by any substantial benefits. Customers can already access their financial information through online banking portals and there is no evidence of significant consumer demand for sharing this information with third parties among community bank customers. For this reason, the Bureau should expand the exemption for all community banks.

Limit Mandatory Data Sharing to Third Parties that Act in the Consumer's Best Interest

The text of Section 1033 requires a covered bank to "make available to a consumer, upon request, information in the control or possession of the [bank] concerning the consumer financial product or service that the consumer obtained from such [bank], including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[7] The term consumer is defined to mean, "an individual or an agent, trustee, or representative acting on behalf of an individual."[8]

Authorized third parties[9] – as described in the Bureau's PFDR Rule – are not necessarily agents, trustees, or representatives acting on the consumer's behalf. Authorized third parties are not bound by a fiduciary duty to act in the best interest of the consumer, which is typical of agent or trustee relationships. Instead, as the Bureau has recently argued in its motion for summary judgment in Forcht Bank v. CFPB, "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."[10]

Under the PFDR Rule, authorized third parties may retain and use consumer data to refine their own products and services in ways that are not beneficial to the consumer who provides access to the data. Furthermore, authorized third parties are not required to act in the consumer's best interest. In other words, authorized third parties were permitted to act in their own interest and not as a representative of the consumer in any way the term is commonly understood.

The Bureau should limit the use of customer data by authorized third parties to third parties that use the data for the purpose of offering the customer a financial product or service that it is in their interest to receive – for example, for the discrete purpose of underwriting a loan or

[7] 12 USC 5533(a).
[8] 12 USC 5481(4).
[9] An authorized third party is "a third party that has complied with the authorization procedures described in [the 1033 rule]." 12 CFR 1033.131. These procedures include providing consumers with an authorization disclosure and obtaining the consumers consent to access data. 12 CFR 1033.401.
[10] *Forcht Bank, N.A. v. Consumer Fin. Prot. Bureau*, Defendant's Memo in Support of Their Motion for Summary Judgment at p. 15, CV 5:24-304-DCR (E.D. Ky. May 30, 2025).

opening an account. It should not permit the use of customer data for other unrelated commercial purposes.

In contrast to Section 1033, the Gramm-Leach-Bliley Act (GLBA) defines a consumer as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[11] GLBA, which governs financial data privacy, should be instructive to the CFPB as it considers the requirement to share consumer financial data under Section 1033. The GLBA definition requires authorized recipients of consumer information to be legal representatives of the consumer to ensure that consumer data is not misused by third parties that do not work in the best interest of the consumer.

Allow Banks to Charge a Reasonable Fee for Developer Interface Access

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 as required by part 1033. This fee prohibition is not present in the statutory text of the Dodd-Frank Act and imposes an undue burden on smaller covered data providers who must bear the entire cost of creating and maintaining a developer interface and providing valuable consumer information to their own potential competitors.

Most community banks will be dependent on their core processors and other third-party providers to create and maintain a developer interface that complies with the rule. These vendors are permitted to charge fees to covered banks for creating and maintaining the interface – but banks have no way of recouping or offsetting that cost from the third-party data recipients that stand to financially benefit from access to data about their customers. This is patently unfair, and it should be amended by the Bureau as it considers changes to the PFDR Rule.

At the same time, ICBA is not advocating for unlimited fees for data access; instead, ICBA is arguing for banks to be permitted to charge "reasonable fees." We are concerned that unlimited fees would allow the largest banks and other large financial services providers to use their market power to set prohibitively high fees for data access which would limit both the ability of consumers to share their data and the ability of smaller players – including community banks – to compete with larger institutions for the provision of loans and other financial products.

As a solution to this problem, we propose allowing banks to recoup their costs of compliance with this rule and to earn a capped, reasonable rate of return for providing valuable customer

[11] 15 USC 6809(9).

data to third parties. Costs should be calculated by adding any fees banks pay to their vendors for creating and maintaining a third-party developer interface or any costs associated with creating and maintaining a developer interface internally, as well as staff time for complying with this rule, including interface operations and third-party due diligence. Costs should also include any losses due to fraud. We believe a reasonable rate of return would be 10%.

The cost of accessing consumer data through the developer interface should be borne by third party data recipients who profit from access to the data. We do not support charging consumers for data they access through the consumer interface, which will most typically be the online banking portal.

The Bureau Should Oversee Larger Third-Party Data Recipients to Ensure They Protect Consumers' Private Data

In general, we believe that requiring third party data recipients to comply with the Privacy and Safeguards rules of the GLBA is appropriate. Banks rigorously comply with the GLBA standards and have a good record of protecting consumer data. However, the success of this requirement hinges on the actions of third-party data recipients. Community banks should not be responsible for bearing the unrealistic burden of thoroughly evaluating the data security programs of every possible third-party recipient or ensuring these entities adhere to their own policies, maintain updated software, or properly train employees on data security and privacy practices.

To address this, the Bureau should leverage its supervisory authority to confirm that third-party data recipients meet necessary safeguarding standards and take enforcement action against those that fail to comply. Moreover, data providers would be more confident sharing customer information with third parties that are vetted and supervised by the CFPB.

Community banks obligated to share data with third parties are deeply concerned that if a third-party company experiences a data breach, leading to the theft or misuse of customer information, customers will likely hold the bank responsible. Additionally, banks fear they will bear the financial burden of compensating affected customers, even when the breach results from the third party's inadequate data security measures. This pattern is already evident in cases of check fraud and virtual payment fraud, where banks, as payors, reimburse customers for losses caused by third-party fraud or negligence.

To alleviate these concerns, the Bureau should explicitly state that financial liability for data breaches rests with the party who has the breach and mandate that third-party data recipients indemnify data providers when breaches occur at the third party. Furthermore, the Bureau should maintain a publicly accessible list of third-party data recipients that it has examined and certified as compliant with Section 501 of the Gramm-Leach-Bliley Act (GLBA). Banks should be

allowed to reasonably deny data access to third parties not included on this Bureau-maintained "Whitelist."

Screen Scraping

For years, the financial industry has shifted away from screen scraping toward more secure methods of data access. Compared to using APIs, screen scraping raises greater concerns for customer privacy and data security, as it allows third parties with a consumer's login credentials to access data with fewer restrictions.

However, screen scraping enables customers to share their financial information consensually through existing online banking platforms, avoiding the costs and technical challenges of developing a dedicated developer interface. Section 1033 of the Dodd-Frank Act mandates "to the extent appropriate" that any implementing rules "do not require or promote the use of any particular technology in order to develop systems for compliance."[12] By requiring developer interfaces and banning screen scraping, the CFPB may arguably exceed its statutory authority by promoting APIs as the mandated technology for compliance.

While APIs enhance privacy compared to screen scraping, we oppose an outright ban on the latter for exempt institutions. We recommend that the Bureau adopt a technology-neutral stance allowing banks to decide whether to build developer interfaces, permit screen scraping, or restrict all third-party access to customer data based on their assessment of the benefits and risks.

Compliance Dates

ICBA supports tiered compliance dates that give community banks more time to create a developer interface. If the CFPB retains the approach of the PFDR Rule of recognizing a Qualified Standard Setting Organization (QSSO) that issues qualified industry standards, compliance dates should not begin to run until the Bureau finalizes a new rule and recognizes a QSSO.

We believe that the following compliance timelines are appropriate:

- Banks > $250 billion in assets – 1 year from recognition of a QSSO
- Banks > $50 billion and <$250 billion – 2 years from recognition of a QSSO
- Banks > $10 billion and <$50 billion – 3 years from recognition of a QSSO
- Banks <$10 billion –Exempt

[12] 12 USC 5533(e)(3).

Conclusion

In closing, the ICBA urges the CFPB to refine the PFDR Rule to carefully balance consumer access, the business interests of financial technology companies, and the operational and financial realities of community banks. The Bureau should expand the exemption for small banks, restrict data sharing to third parties acting in the consumer's best interest, permit reasonable cost-recovery fees, and strengthen oversight of third-party data recipients. Additionally, addressing liability for data breaches, maintaining a technology-neutral approach, and providing tiered compliance timelines will support community banks while promoting consumer protection.

We appreciate the opportunity to contribute to this rulemaking process and look forward to a revised rule that safeguards consumer data and supports the vital role of community banks in the financial system. Please contact me at Mickey.Marshall@icba.org if you have any questions about the positions stated in this letter.

Sincerely,

Mickey Marshall
Vice President and Regulatory Counsel