1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 |
fpf.org

October 17, 2025

**Via Electronic Submission**

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

**Re: Comments on Personal Financial Data Rights Reconsideration (Docket No. CFPB–2025–0037)**

Dear Acting Director Vought,

On behalf of the Future of Privacy Forum (FPF), we are pleased to provide comments and recommendations regarding the CFPB's Advance Notice of Proposed Rulemaking (ANPR) for its Personal Financial Data Rights Reconsideration.[1]

FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.[2] FPF focuses on promoting responsible data practices and has deep expertise regarding privacy and data protection, particularly concerning open banking. In addition to its traditional expertise, FPF offers a unique perspective as it hears from stakeholders across the open banking spectrum. FPF has been deeply engaged in the open banking policy process in the United States and abroad. Before the CFPB rulemaking process began, FPF authored a white paper on respective roles of the parties and a consumer infographic highlighting consumer impacts and challenges. FPF submitted comment letters in response to the SBREFA and NPRM filings in 2023. Internationally, FPF co-hosted a conference on open banking with the Organisation for Economic Cooperation and Development (OECD) in 2022, and held a workshop for industry and regulators relating to the EU's suggested Framework for Financial Data Access (FIDA) in 2024.

Earlier this year, FPF testified before the House Financial Services Subcommittee on Financial Institutions regarding financial privacy generally and open banking. For ease of reference, FPF has attached our written testimony, as well as responses to follow-up congressional questions, given the materials are highly relevant to many of the ANPR's topics. Our comments reflect the

[1] Personal Financial Data Rights Reconsideration, 90 Fed. Reg. 40986 (August 22, 2025).

[2] The views expressed in this comment are those of FPF and do not necessarily reflect the views of FPF's supporters or Advisory Board.

belief that privacy and security are foundational to trust in and uptake of open banking products and services.

FPF appreciates that the CFPB in its ANPR is exploring certain significant components of the final rule, with a view to improve the regulation for consumers and industry. FPF supports this goal, and has pointed out key areas for improvement in its comment letters and testimony.[3] We also understand the criticality of having a final rule that industry can implement without further delays in order to benefit consumers. Regulatory certainty will drive open banking adoption forward as industry can build out to meet deadlines. FPF therefore believes that either the final rule should remain as-is, to be amended over time based on implementation experiences and new products coming on board, or that the CFPB can issue targeted amendments per FPF's recommendations that will improve the ecosystem and not cause undue regulatory delay.

FPF offers its analysis of each of the topics raised in the ANPR. At the close of each topic, we offer a synopsis of recommendations where we have them.

## I. Consumers and Representatives

FPF applauds the depth and thoughtfulness of the ANPR questions regarding how to best interpret the meaning of representative under the statute. FPF considers that the meaning is correctly addressed in the final rule, from a plain meaning, best reading, and public policy perspective.

As a gating question, if Section 1033 is interpreted to allow access by only the consumer, and not to allow the consumer to direct access by a third party, the regulation becomes valueless. The consumer will be unable to perform all the open banking operations and updates themselves, and can't use a developer interface. Please see FPF's written congressional responses that describe in detail the consumer challenges and infeasibility of this approach.

FPF considers that representatives should include non-fiduciaries as well as fiduciaries. Again, this is consistent with the plain meaning of the word, which does not include fiduciaries in dictionary definitions, as well as better public policy. Many third parties are non-fiduciaries under the current open banking community, including banks in some circumstances. Limiting representatives to fiduciaries would exclude all these parties, and requiring non-fiduciaries to become fiduciaries would create extraordinary barriers to entry. The goal of open banking is to

[3] In our testimony, we identified five areas that the CFPB could have better addressed in the final rule to make it more palatable to industry and better for consumers. The CFPB asked about four of them in this ANPR: fees, security (see FPF's testimony re pay-by-bank), and privacy (see FPF's testimony re deidentification and secondary uses). FPF's final issue relates to pass-through digital wallets, which we recommend excluding from the definition of data providers and the rule. Consumers need access to accurate data from sources of truth – account issuers – not pass-through digital wallets that don't hold customer accounts. Including them in the final rule adds unnecessary complexity for little benefit, and in our review this was the consensus view across commenters in the rulemaking process.

foster innovation, competition, and more products for consumers, which we have seen play out as open banking has developed in the United States, frankly as a leader across jurisdictions. The ANPR correctly asks, if representatives are interpreted to cover non-fiduciaries, what should be the required elements for an entity to qualify as a representative. FPF again believes that the final rule addresses the question properly.

First, the rule includes a number of required steps and interactions that must be taken between the data provider, consumer, and third party that cover authentication, authorization, and operations. These activities enable the parties to:

- Be certain of the identity of all parties;
- Evaluate safety, soundness, and other risks before providing access; and
- Work together effectively while the consumer relationship is active.

Second, the rule contains privacy requirements for third parties related to their collection, use, and retention of consumer data, and security requirements for all parties. FPF considers it critical that the CFPB does not water down these privacy and security obligations. By definition, to be a representative, the third party needs to represent the consumer for their access request. The third party thus may only use the information to effectuate the consumer's request, not for its own purposes. Please see FPF's comments below relating to privacy provisions, which include the importance of retaining obligations on third parties, with two suggested amendments to make the rule not at odds with modern privacy principles and regimes.

**Synopsis of Recommendations**: The final rule should maintain the ability for consumers to direct access by third parties, if requirements related to account establishment, privacy, and security are retained. Otherwise non-fiduciaries should be excluded.

## II. Fees

FPF considers that from a plain reading of the statute, as well as sound public policy, consumers should not be charged for access to their data. The requirement to provide access is not conditioned on paying fees.

FPF recognizes that an ongoing pain point for industry is whether and how data providers can charge access fees to third parties that are acting on a consumer's request. On the one hand, consumers must be given access. On the other hand, data providers do incur costs to develop and maintain developer interfaces or application programming interfaces (APIs), and data aggregators or third parties can charge fees to downstream users, usually with value-added services. Consistent with our congressional testimony, FPF considers that the typical regulatory course is to be silent about fees between business parties, which can be addressed via contract and the free market. However, FPF recognizes the unique challenges raised in the open banking context since the data provider holds the information needed by the consumer and third party. The CFPB should carefully consider the feedback it receives on this question from industry, including how changes to the rule could impact API adoption.

## III. Data Security

The importance of data security in open banking cannot be over-stated. Consumer data that is accessed, whether via API or screen scraping (discussed in more detail below), is highly personal and sensitive, and enables money movement. As the ANPR points out, the information can reveal a person's wealth, vulnerability, or personal habits that consumers expect to be kept private. Data breaches also place consumers at risk. A consumer's cash is literally at risk too.

### A. The CFPB should move quickly to implement, and strengthen, the rule to move industry from screen scraping to APIs

A central goal of US and global rulemaking is to move open banking from screen scraping to more secure API technology. Screen scraping is a risky privacy and security practice that needs to end. It involves consumers giving their online credentials, such as username and password, to a third party so that it can go onto a data provider's website, like chase.com, and take actions on their behalf. During the rule-making process, the CFPB explored how screen scraping is a poor practice for any good data management. As examples, third parties that screen scrape will have fewer or no controls that limit what data they collect, what they use it for, and how long they retain it. More fundamentally, screen scraping allows the third party to take any action the user could take. The third party thus has full access to information in the account, including the ability to move money. In addition, the practice counteracts efforts to educate consumers never to give out their online credentials and passwords given potential harm to them. Finally, screen scraping is destabilizing to online portals of data providers, where it can be difficult to distinguish real users, screen scrapers, and bad actors trying to access the site maliciously. These major risks to consumers and the ecosystem can be avoided with APIs.

The final rule supports this important public policy goal, so that a data provider can prohibit screen scraping once it offers a compliant API.[4] The approach effectively sunsets screen scraping, as data providers became compliant with the rule via the tiered compliance dates, presumably to include even smaller institutions as the rule and industry standards evolve.

The CFPB should continue to strenuously support the goal to eliminate screen scraping. Per its prior submissions, FPF understands that the process may take time, and a tiered approach can

[4] FPF supports the role of the Financial Data Exchange (FDX), which is recognized by the CFPB as a standard setter for API technical standards. There is a long-standing framework, contained in OMB Circular A-119, for agencies to rely upon industry standards where appropriate. For open banking, per our testimony, an industry standards body is far better placed to develop API technical standards. The CFPB's rule regarding standard setters provides appropriate governance requirements, and FDX has incorporated industry balance at all decision-making levels as well as representation by noncommercial entities (for which FPF currently serves as co-chair on the FDX Board). The CFPB could improve the final rule by providing that adherence to standards is deemed compliance with standardized formatting requirements, rather than an indicia of compliance. This will simplify and clarify the rule, making it easier for the CFPB to implement and oversee. It would also provide more certainty to industry, as companies go to a great deal of effort to comply with API standards. The CFPB included deemed compliance in its proposed rule, and the change in the final rule to 'indicia' creates avoidable and unnecessary complexity.

be appropriate based on entity size. Regulatory deadlines and industry standards will drive the transition forward. In that vein, regulatory certainty, including compliance dates that industry can rely upon, will be very helpful to incentivize the process. In FPF's view, this topic is an example of what the CFPB was designed to do: protect consumers from harmful practices, via a workable process for industry.

FPF recommends that the CFPB place an obligation directly on third parties to refrain from screen scraping once they can access data via an API, rather than put the obligation on data providers to stop them.[5] Many commenters during the rulemaking process raised this point – the rule should place the prohibition on parties that conduct the practice. The rule places many other obligations directly on third parties, so FPF is unsure why it did not do so in this instance. The CFPB has an opportunity to update this obligation as it considers changes to the rule.

### B. The final rule provides appropriate security measures which could be further strengthened

In the ANPR, the CFPB raises a number of questions about the effectiveness of information security standards and relevant regulatory frameworks. FPF considers that the final rule requires appropriate information security for data providers and third parties, recognizing that they do function under different regulatory regimes and oversight. Depending on the party and role, examples of applicable rules involve the GLBA, safety and soundness, Regulation E, anti-money laundering, and the Federal Trade Commission (FTC).[6] In FPF's view, the CFPB conducted a thorough review and devised a rule that provides information security across the ecosystem. Key examples include:

- Authentication and authorization requirements ensure that the consumer and all parties are properly identified and authorized to take requested actions to support the consumer's wishes.
- Data providers and third parties are required to establish security programs under their respective regulatory regimes.
- Data providers are permitted to deny access to their API based on risk management concerns appropriate to their industry and obligations to their customers.

The CFPB should retain existing security obligations in the final rule, particularly if non-fiduciaries can continue to serve as third parties. FPF offers a couple of areas where the CFPB could further strengthen security. These enhancements will benefit consumers, and address pain points for industry identified in the rulemaking process and in FPF's congressional testimony.

---

[5] Data providers should remain accountable to provide compliant APIs in appropriate timeframes, to provide access in accordance with anti-evasion requirements, and even perhaps to block screen scraping once their compliant API is available. In commentary, the CFPB should allow a data provider to block screen scraping for any data for which it provides access via a compliant API, in order to promote API adoption and end screen scraping.

[6] Over time, the agencies have worked together to develop some consistency in approaches, and should continue to do so, like regarding risk management. Strict conformity might require congressional action, and may be undesirable in any event from a public policy perspective given different industry roles.

- First, the CFPB should clarify that, once data is transferred to third parties, they are responsible for proper data management, including privacy, security, breach and records management, etc. Uncertainty about accountability and liability has been a sticking point, and this clarification provides a commonsense approach that will also encourage third parties to put the right resources into data management.

- Second, the CFPB should clarify or permit further industry mitigation to address heightened risks related to requiring access to payment initiation information including bank account and routing numbers. Access to this information, sometimes referred to as pay-by-bank, allows parties to move money out of a consumer's account to a designated recipient. This service is a core value of open banking, and consumers want it. However, as addressed in our congressional testimony, data providers raised warning flags to the CFPB that pay-by-bank not surprisingly raises fraud risk, particularly as the types of third parties may expand beyond initial adopters like landlords and energy companies. FPF is likewise concerned that more controls may be needed to protect consumers' data and money. For access to this data, the CFPB could allow data providers more options to deny access based on risk management or to halt data access quickly if fraud is detected, and conduct its own reviews to evaluate fraud trends and take appropriate action.

**Synopsis of Security Recommendations:**

- The CFPB should retain security standards for all parties and move the final rule forward expeditiously to sunset screen scraping.
- Screen scraping prohibitions should be placed directly on third parties.
- The rule should clarify that third parties are accountable for data management once data is appropriately transferred to them.
- Further controls should be allowed to protect pay-by-bank information.

## IV. Privacy

In the final rule, the CFPB places modern and reasonable privacy rules on third parties relating to their data collection, use and retention of consumer data. The CFPB reasoned that the third party is acting as a representative of the consumer. It is not a purely transactional relationship like purchasing goods off a website. Accordingly, the third party should only use data for the purpose requested by the consumer, collect only what is necessary to perform the activity, and limit how long it keeps the data based on the relationship with the consumer. Moreover, as mentioned above, the CFPB in the ANPR makes special note of the sensitivity of consumer data involved in open banking. Appropriate rules are needed to address privacy risks and concerns.

### A. The CFPB needs to preserve privacy rules for third parties

FPF is concerned that the ANPR seems to focus primarily on risks related to data sale and licensure. These are certainly important topics. The final rule provides that sales of data cannot be considered a primary use of data, and so must be separately authorized by the consumer. In addition, the final rule requires the third party to limit their own use, collection, and retention of consumer information. FPF considers that these requirements are critical to preserve.[7] The privacy rules that the CFPB sets should be reflected in third parties' internal policies as well as privacy policies and other notices available to consumers.

### B. The CFPB can simplify and improve notices for consumers

The CFPB in the ANPR asks about estimates for how many online users read or understand user agreements and privacy notices. FPF appreciates that many consumers are numb to the plethora of privacy notices with which they are presented, and encourages companies to write them simply and directly. However, the rate of readership is not the sole value of privacy notices. Companies are required to comply with their notices, and they are enforceable by regulators. They thus build communications, training, controls, and other compliance features to support the notice. Notices set a public bar that companies cannot go below.

In fact, the open banking context provides an ideal opportunity to offer the best privacy solutions for consumers. Consumers can have:
- A notice that is specific, clear, relevant, and succinct;
- Choices presented to them that are also clear and relevant to reflect their direction; and
- Confidence that regulations require proper privacy and security standards for all parties.

This last feature is sometimes referred to as ethical data management. Consumers can't be 'tricked' into consenting to lower standards.

Open banking can thus marry notice and choice, on topics where consumers need to voice their goals, with ethical data rules that are critical for financial data. The CFPB could improve the rule to better delineate these goals. In many ways, the authorization disclosure serves as a privacy notice. It provides succinct information and enables consumers to make choices based on that information that reflect their desired outcomes. However, the authorization disclosure also includes elements that are more relevant to internal data management. The compliance certification is an example. FPF considers that compliance statements should still be made public, such as on a website, both for regulatory enforceability and for those consumers who do prefer to read deeper information. However, it does not need to be included in every authorization disclosure. FPF believes this will meet all open banking goals. It will increase readability of privacy statements; simplify industry implementation and consumer experiences; and retain ethical standards and enforcement. FPF is grateful that the CFPB raised this

[7] In its comment letters, FPF recommended that the CFPB issue guidance about these rules, since they are new to the financial sector and open banking, although considers the regulatory text to be adequate.

important question that has been vexing industry and consumers. Open banking offers a route to address privacy notices and data management meaningfully.

### C. The CFPB should modify privacy rules for third parties regarding deidentification and secondary uses to be consistent with other privacy regimes and to improve the consumer experience and protections

Consistent with FPF's prior recommendations, the CFPB should make two changes to the rule's privacy provisions to align to good public policy, data management, and modern privacy principles here and abroad.

- First, commentary should clarify that deidentified consumer data is excluded from the rule. FPF is unaware of any other regime in the United States or globally that requires consumers to authorize use of deidentified data. Deidentified data is widely used in every sector including the financial sector. There are strong public policy reasons to incentivize deidentification. First, its use offers consumer benefits for research and innovation. Second, deidentification improves privacy and security, reducing the risk of data misuse or breaches. Reidentification risk is a valid concern, but so is the risk of any regulatory violation that companies need to build effective policies and controls to address. FPF is unsure why this regulatory risk created a poor policy outcome.

- Second, the rule should allow consumers to opt-in to secondary uses of their information. This is also consistent with how other privacy regimes treat sensitive information. FPF is concerned that requiring separate authorizations for secondary uses, as the final rule currently does, will create unintended negative consequences. On the one hand, an aggressive third party could shoehorn broad uses into a primary use (which consumers should rightly know about and approve) to avoid obtaining the authorization. On the other hand, requiring a separate authorization for a related secondary use can create awkward, confusing, and cumbersome consumer experiences, which can quell innovation and products and services they would happily request via opt-in.

**Synopsis of Privacy Recommendations:**

- The CFPB should retain privacy obligations for third parties related to their collection, use, and retention of consumer data. Otherwise permitted representatives should exclude non-fiduciaries.
- The CFPB should review authorization disclosure requirements to move items that are not directly related to notice and choice to effectuate the consumer's direction into another non-transactional public statement. Compliance certifications are an example.
- Secondary uses of data should be permitted via opt-in mechanisms rather than a separate authorization disclosure.
- Deidentified data should be excluded from the rule.

## V. Compliance Dates

The ANPR raises questions about implementation challenges and how changes to the rule could impact compliance deadlines. FPF is unable to comment on how significant changes might impact implementation without knowing what those changes are. However, even if the rule remains similar to the final rule, implementation is impacted during this time period of regulatory uncertainty. The benefits that the open banking rule will bring in terms of privacy, security, consumer expectations, and clarity of respective industry roles and responsibilities will be delayed. Furthermore, as described in FPF's response to congressional inquiries, delay also impacts expansion to other information, like mortgages and loans, that should be part of open banking via appropriate policymaker action.

FPF accordingly recommends that the CFPB retain the final rule, or implement a new rule, as quickly as possible. FPF considers that its recommendations are discrete issues that would be largely welcome across industry, benefit consumers, and not cause significant delay. Indeed, the increased clarity they may bring may even save some implementation time. The CFPF should continue to seek input from data providers, third parties, and consumer groups about reasonable timeframes and impacts of delays.

FPF appreciates the CFPB's efforts to evaluate and improve its rulemaking under Section 1033 of the Dodd-Frank Act and is thankful for the opportunity to comment on these issues. Given the breadth and depth of our expertise, we welcome further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact me at zstrickland@fpf.org.

Sincerely,

Zoe Strickland
Senior Fellow