Written Testimony of Zoe Strickland

Senior Fellow, Future of Privacy Forum

Before the U.S. House of Representatives Financial Services Subcommittee on Financial Institutions

"Framework for the Future: Reviewing Data Privacy in Today's Financial System"

June 5, 2025

On behalf of the Future of Privacy Forum (FPF), I thank you for the opportunity to testify about data privacy in the financial system, with a particular focus on rulemaking under Section 1033 of the Dodd-Frank Act, often referred to as open banking. I offer the following remarks to provide observations about data privacy and financial data privacy, and to focus on open banking. including providing some recommendations on how policymakers can progress this important functionality for consumers.

Privacy expertise

My goal in testifying at this fact-finding hearing is to support congressional efforts to advance financial privacy, and to support innovative services that can support competition and new business opportunities that provide consumer value. To this end, I thought it would be helpful to spend a few minutes on my and FPF's privacy expertise. Over 25 years, I have served as global chief privacy officer, among other roles, at Fortune 20 companies in many verticals, including government, retail, healthcare, and finance. At the USPS, I served as the first CPO, and managed Privacy Act, Freedom of Information Act, and records functions, as well as new areas (at the time) relating to internet privacy. At Walmart, I managed global privacy and records, which included financial privacy requirements for its money service centers under the Gramm-Leach-Bliley Act overseen by the Federal Trade Commission. I also served as global CPO for JPMorganChase, addressing all privacy requirements around the world and building a strong privacy compliance program. I am thus deeply familiar with privacy developments over time – such as addressing new technologies and business developments – in a global context – and how to manage privacy practices under different regulatory regimes, whether in highly regulated areas like finance or

healthcare; broadly regulated like retail; or generally regulated in non-U.S. jurisdictions. My focus has been apolitical and very consumer-focused, a bedrock of privacy.

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship and advancing principled data practices in support of emerging technologies. We are supported by leading foundations, as well as by more than 200 companies and law firms, with an advisory board representing academics, industry, and civil society.[1] We bring together privacy officers, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

We are strong believers in open banking initiatives and growth. Open banking enables consumers to have more control over their data and funds. Properly implemented, it can support numerous consumer benefits and opportunities, enabling better money management, financial health, and privacy. Open banking can be a shining example of modern privacy – consumers should expect to have control over their information – and hopefully this sense of control will permeate other aspects of their lives, leading to better services and competition.

Since initiating our open banking program in 2021, we have:

- Held a joint conference with the Organization for Economic Cooperation & Development and issued a white paper on open banking approaches (2022-23)[2];
- Conducted an industry and policy-maker event in 2024 regarding the EU Open Banking regulatory initiative known as Financial Data Access (FIDA); and
- Focused heavily on the U.S. open banking environment, including creating a consumer infographic, and engaging in the CFPB's Section 1033 rulemaking process via meetings, white papers, and comment letters[3].

This spring, I was elected to serve on the Board of Directors for the Financial Data Exchange (FDX), as a co-chair representing noncommercial entities. FDX is a nonprofit organization, consisting of hundreds of members, that provides technical specifications and other tools to enable consumer-permissioned data sharing within the growing open banking ecosystem of data providers, recipients, and aggregators. We are grateful to CFPB and FDX efforts to include consumer and privacy groups in leadership roles.

---

[1] The views herein do not necessarily reflect those of our supporters or our Advisory Board.
[2] Future of Privacy Forum, "Developments in Open Banking: Key Issues from a Global Perspective" (March, 2022), https://fpf.org/wp-content/uploads/2022/08/FPF-Open-Banking-Report-R2-Singles.pdf.
[3] *See* Future of Privacy Forum, "FPF files comments with the Consumer Financial Protection Bureau regarding personal financial data rights" (Jan. 18, 2024),

Privacy Observations

During my career, I managed privacy and other programs globally. As this committee is aware, most countries have omnibus privacy laws that apply to their residents. These general laws can be supplemented by specific regulations where appropriate. An example for the financial sector is bank secrecy laws that protect consumer records. (At times this can create conflicts of law, for instance making compliance with both that jurisdiction's bank secrecy law and this country's anti-money laundering requirements difficult.) In addition, some national and regional privacy obligations have implications for cross-border data transfers, with companies analyzing whether personal data is flowing to jurisdictions that have adequate privacy protections. Multi-nationals in particular pay considerable attention to cross-border privacy compliance.

In contrast, the privacy environment in the U.S. is largely sectoral. In my view, it is not only sectoral but topical. As examples, Congress has passed laws over time that contain protections for health information (Health Insurance Portability & Accountability Act), financial information (Gramm-Leach-Bliley Act), credit (Fair Credit Reporting Act), and children (Children's Online Privacy Protection Act). Other privacy protection laws relate to topics like marketing, such as the CAN-SPAM Act and do-not-call requirements. U.S. laws can give federal agencies power to issue supporting regulations, such as the Federal Trade Commission for CAN-SPAM or the Consumer Financial Protection Bureau for GLBA privacy requirements. As compared to the omnibus approach, sectoral legislation allows for requirements that are more targeted to goals and risks. At the same time, disparate laws are harder to update and harmonize, both with each other and with other countries' more general laws.

In recent years, Congress has introduced bills to either update privacy laws for certain sectors or create a more broad-based privacy law. I appreciate these initiatives, and recognize the challenges. Privacy is a wide-ranging field that can be difficult to get your figurative and legislative arms around. There can also be inertia with existing regulatory environments and real questions about how existing compliance frameworks would interact with new legislation.

Some recent examples of legislative efforts include H.R. 2977, the Consumer Privacy Protection Act of 2015; H.R. 1165, the Data Privacy Act of 2023; and H.R. 8818, the American Privacy Rights Act of 2024. I commend the growing efforts to introduce modern and substantive obligations relating to privacy, in addition to security and anti-breach requirements. Privacy and security are related yet distinct disciplines. Privacy relates to how companies use consumer information entrusted to them, and respect consumers' rights and control over that information. It's important that a company

secures information from hackers. That's a baseline. Does the company also allow consumers to access, or correct, or delete, data held about them? Many bills grant authority to federal agencies to define and regulate certain obligations, while others rely on statutory text to fully articulate core rights and responsibilities. Based on my experience, some of the thornier legislative issues can often relate to items like state law pre-emption and enforcement mechanisms.

It is helpful for companies, and policymakers too, to take a principles-based approach to privacy. Key examples of modern privacy principles relate to notice, consent or control, individual rights, data minimization, ethical data uses, and security. One of the most significant of these principles, sometimes called data portability, relates to individuals' rights to be able to access and transport information about themselves. Data portability can help individuals more easily use different services and enhance market competition, yet can also introduce security risks if portability frameworks are not thoughtful and well-managed. This principle is central to the Section 1033 rulemaking.

Section 1033 Rulemaking

Under Section 1033 of the Dodd-Frank Act, the CFPB is authorized to issue rules that require covered entities to make information about consumers who use their financial products available to them upon request. As mentioned in the introductory section, the Future of Privacy Forum has deeply analyzed the proposed rules, and has worked with stakeholders to understand their implications on a range of business practices and data protection issues. Below I cover the extensive regulatory process undertaken, some positive aspects of the Rule, and some areas of potential improvement.

Regulatory Process

Last year the CFPB issued two final rules under its Section 1033 authority: a rule relating to Industry Standard-Setting on June 5, 2024, and a rule on Personal Financial Data Rights on October 22, 2024. The data rights rule covers two types of financial products: checking and savings accounts per Regulation E and credit cards per Regulation Z, as well as facilitation of payments from these accounts. The CFPB recognized the Financial Data Exchange (FDX), mentioned above, as a standard setter under the Rule on January 8, 2025.[4]

[4] CFPB Approves Application from Financial Data Exchange to Issue Standards for Open Banking | Consumer Financial Protection Bureau

The CFPB undertook a lengthy and extended process to issue these rules, including the following steps.

- October 2016: the CFPB issued a Request for Information about access to financial records.
- October 2017: the CFPB published a set of Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation, along with a summary of stakeholder insights informing those Principles.
- October 2020: the CFPB released an Advance Notice of Proposed Rulemaking.
- October 2022: the CFPB sought feedback on 1033 from small businesses and others in an Outline of Proposals and Alternatives Under Consideration for the Personal Financial Data Rights Rulemaking.
- February 2023: the CFPB convened a Small Business Review Panel.
- April 2023: the CFPB released the Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights.
- October 19, 2023: the CFPB released the Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights.

As part of this process, the CFPB engaged with numerous stakeholders and closely monitored market developments to promote consumer interests, innovation, and competition. Engagement included meetings with stakeholders, such as FPF. Meetings that occurred during the rulemaking process were captured as ex parte conversations and posted on their rulemaking website. Given the rule's breadth and depth, many stakeholders weighed in. In response to the proposed rule, over 11,000 comments were submitted. In addition to the sheer number of comments, the depth and content of the feedback is noteworthy as well. Many comments delved deeply into several corners of the rule, and were lengthy and detailed. Although there were recommended areas for improvement, including in FPF's comment letters, there was considerable support for the rule across industry sectors and consumer groups. Indeed, many commenters – including consumer and industry groups – recommended that the rule cover more products and move more quickly. Similarly, the recognition of FDX as a

standard setter was a thorough process, including formal submission and approval, with a public comment period.[5]

Positive Aspects of the Rule

There are a number of valuable aspects to the rule, as listed in our NPRM comment letter.

- First and foremost, consumer control and benefits are core to the rule. The consumer and their direction drive industry obligations and activities.

- The rule phases out the practice of screen scraping. Screen scraping is an extremely poor privacy and security practice. Under this practice, a data recipient obtains log-in credentials and passwords from a consumer, and uses these credentials to access a data provider's website (like chase.com) and take actions on the consumer's behalf. Security experts typically advise that consumers should never provide their credentials and passwords to third parties, which then have unrestricted access to the consumer's account. This practice can create serious consumer harms, and promotes risky behavior that undermines consumer protection campaigns. In addition, screen scraping destabilizes website security of data providers, which need to distinguish between actual consumer access, screen scraping, and bad actor intrusions. The Rule's requirement that data sharing occur via developer interfaces, or Application Programming Interfaces (APIs) given current technology, is the right outcome. The transition from screen scraping to APIs should be legally mandated and occur as soon as possible.[6]

- The rule creates privacy and security obligations for data recipients. I applaud the inclusion of modern privacy obligations for data recipients, including data collection, use, and retention requirements. It is critical that recipients, often fintechs that may be new entrants to the financial ecosystem, only use information for purposes that the consumer has requested. Consumers should

[5] https://www.consumerfinance.gov/personal-financial-data-rights/applications-for-open-banking-standard-setter-recognition/

[6] I am sympathetic to the criticism that the rule should place the restriction on the data recipient directly, rather than requiring data providers that offer compliant APIs to prohibit screen scraping. Perhaps the CFPB was concerned about its authority over the full data recipient community. In any event, the rule still accomplishes the same result—data providers need to establish compliant APIs, and then screen scraping can be prevented.

be able to trust that recipients operate this way, rather than having to pore through privacy policies and legalese to (perhaps) understand how their information will be used – and trust me, some policies seek to allow more uses than the consumer requested. Indeed, in some ways, 1033 privacy rules exceed those that apply to data providers. The rule also requires recipients to employ security protections that seek to parallel the highly-regulated data provider environment.

- The rule provides a constructive role for industry standards within a regulatory framework. The CFPB recognized that industry was much better placed to devise technical standards for data sharing. Industry is closer to the technology, business functions, and users, and can also make updates and advances more easily than the government. The CFPB relied on long-standing regulatory guidance, OMB Circular A-119,[7] for how and when to incorporate industry standards. The CFPB provided topical areas for industry standards, particularly related to data sharing interfaces, and also governance requirements to make sure standard setters had transparency, balance in decision making, and oversight. It is one of the strengths of the Rule. One of the areas where the U.S is ahead of other jurisdictions in open banking, despite their sometimes earlier start and coverage of more products, is in development of industry standards. This advantage should be promoted.

Areas for improvement

Unfortunately, the CFPB in its Final Rule did not incorporate some of the comments that it received that would have improved the rule. If the Bureau had made these changes, the rule would have been stronger for consumers and more palatable to industry. I will touch on five topics.

- **Secondary uses of information:** The Final Rule prohibits data recipients from using consumer information for secondary purposes. Data recipients may only use information for primary purposes, and can't cross-sell products, without initiating a new authorization disclosure process. Authorization disclosures are intended to initiate a new product or service. Forcing their use for secondary uses will be awkward and cumbersome to consumers, stifle innovation, and result in inconsistent compliance and experiences. As FPF described in its comment letters, a better outcome for consumers and the ecosystem is to allow

[7] Office of Management and Budget, Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* (Jan. 1, 2016), https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary

consumers to opt-in to secondary uses. To be clear, and as articulated in my testimony, I support regulating uses of information, and believe that data recipients should respect consumers, including their expectations of data uses. Obtaining consumer consent for secondary uses is particularly appropriate for open banking, which is all about consumer direction and permissions. The opt-in mechanisms of course must be clear, prominent, and fair. To the extent that the CFPB wished to exclude uses deemed high risk, that is not a reason to abandon the proper privacy approach; either define prohibited uses, or let consumers choose products that are legal in the marketplace.

- **De-identification:** The Final Rule arguably prohibits the use of de-identified data, unless it is the product or service requested via an authorization disclosure. Per our comment letters, we strongly encourage that de-identified data not be subject to the regulation, consistent with other regulatory regimes in the U.S. and globally. The use of de-identified data is a central aspect of data processing for all industry sectors, including the financial sector, encouraging innovation in a privacy-protective manner. In open banking, examples are quality control and product and service improvements. There are numerous public policy research benefits as well. De-identification is also a valuable privacy and security protective measure, greatly reducing risks relating to data misuse and breaches. Its use should be encouraged, not devalued.[8] I understand there are concerns related to re-identification. As with all risks, appropriate controls should be deployed and monitored. Frankly, as a long-term compliance officer, I know any obligation can be violated, and the risk of data misuse is harder to police for than re-identification risk. In the preamble to the final rule, the CFPB recognized its approach had downsides, and suggested that it may alter its approach in a future rulemaking. That change should happen now.

- **Payment Initiation information:** The Final Rule requires data providers to furnish payment initiation information that allows data recipients to initiate money transfers out of consumers' accounts, often called pay-by-bank. As an initial point, and for consistency with Dodd-Frank language, the rule should instead cover data types (account number and routing number) like it did for the rest of the rule. More broadly, the CFPB should dig deeper into the fraud concerns raised by data providers.[9] To be clear, pay-by-bank exists in today's ecosystem, such as for account openings and for payments to utilities, landlords and other payees. Consumers want this functionality and convenience, and it needs to be part of the rule. However, with the rule opening the door widely to any authorized third party, and with data providers having limited recourse to deny API access via specific risk management concerns, it is critical to examine

[8] *See* Future of Privacy Forum, *A Visual Guide to Practical Data De-identification* (Apr. 25, 2016), https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/.
[9] https://www.regulations.gov/comment/CFPB-2023-0052-11099

any increase in fraud risk. Taking money out of consumer accounts merits higher scrutiny. The CFPB should address these concerns via RFI, enhanced fraud monitoring, more data provider recourses, or shifts in liability.

- **Fees:** The Final Rule prohibits data providers from charging fees related to access to their APIs. Certainly the consumer should not be charged. It is their data and they should be able to direct companies to share it for desired purposes. The rule prohibits data providers from taking actions to evade the rule and discourage access, and should otherwise be silent on fees between companies.

- **Digital Wallets:** The Final Rule covers digital wallets, including pass-through wallets that do not store information. This raises considerable compliance challenges for those providers for no discernable consumer benefit. In my read of comment letters, there appeared to be consensus to exclude pass-through wallet providers.

I consider that the Final Rule unnecessarily stepped back from the NPRM relating to industry standards. The NPRM provided that adherence to a standard issued by a recognized body was deemed compliance for interface obligations. The Final Rule watered this down to an indicia of compliance. In my view, if the CFPB has recognized an industry standard setter, its technical specifications should be considered compliant. This incentivizes industry adoption of consistent standards and good governance. The development of industry standards is a benefit of the U.S. market-led approach, where policymakers can add useful weight.

Finally, in our comment letters, we recommended that the CFPB and other relevant regulators issue guidance relating to risk management and data privacy. The CFPB has issued extensive privacy guidance to data providers under GLBA, and should do the same for data recipients.

Conclusion

I am grateful to this committee for the opportunity to comment on financial privacy and the 1033 Rule. We are hopeful that open banking moves quickly to the future. Rules should incorporate more products and services, so that consumers can truly have a holistic view of their financial picture, and address developing issues like artificial intelligence. We are available to assist in navigating the path forward. It's our mission to progress the intersection of developing technologies, privacy best practices, and consumer interests. Thank you again for this opportunity and I look forward to your questions.