January 25, 2023

Director Rohit Chopra
Consumer Financial Protection Bureau
1700 G Street NW
Washington, D.C. 20552

RE: Future of Privacy Forum comments on the CFPB's Outline of Proposals and Alternatives under Consideration related to its Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights

Dear Director Chopra,

The Future of Privacy Forum (FPF) welcomes the opportunity to comment on the CFPB's Outline of Proposals and Alternatives under Consideration related to its Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (Proposal).

The Proposal is a preliminary step in the CFPB's planned rulemaking under the Dodd-Frank Act. Section 1033 of Dodd-Frank provides, subject to CFPB rules, consumer rights to access information about financial products they use. FPF appreciates the thoughtfulness and sophistication of the Proposal's suggestions and questions, and how the CFPB is doing considerable preparatory work, to support rulemaking under the law. Dodd-Frank also requires the CFPB to consult with other banking regulators and the FTC as it develops its rule.

In several respects, the Proposal supports a developing business area, commonly known as open banking, that is dependent on effective financial data access and portability. Open banking involves the sharing of consumer information, at the consumer's direction, to enable financial products and services the consumer wants. A common example is an application that enables peer-to-peer payments. A consumer can sign up for the application and direct their bank to interface with the application so that payments can be authorized from the consumer's accounts to payees of their choosing. Open banking has been subject to various regulatory definitions, approaches, and requirements across the globe. Policymakers have taken action in several jurisdictions to speed adoption, foster competition, and promote consumer options. Some jurisdictions regulate the field extensively, and others provide a more flexible framework that allows businesses and consumers to explore different models. US regulatory frameworks are fragmented between federal and state obligations as well as by business activities. In addition to focusing on compliance with developing legal obligations, industry has been working to develop consumer-oriented practices to support open banking. FPF's comments focus on the Proposal's remit regarding data access, as well as impact to the larger ecosystem of open banking where relevant.

In FPF's view, the Proposal covers two main areas: 1) impacts to businesses, particularly small businesses, in advance of convening its Small Business Review Panel required under SBREFA; and 2) common infrastructure questions that impact all participants: businesses large and small, consumers, and oversight bodies. Examples are the Proposal's recommended approach for standard authorization disclosures; options for when secondary data uses would be permitted; and data deletion requirements.

Below, FPF addresses the Proposal's common infrastructure suggestions and questions. FPF's analysis indicates that the Proposal is on the right directional track and identifies areas of potential improvement that would further clarify obligations and especially roles. There are four main topics, addressed directly or indirectly in the Proposal, where the CFPB could further clarify rules to benefit adoption and consumers. These are:

- Authorized Disclosures and Consent Management
- Roles and Responsibilities
- Secondary Uses of Data
- Retention and Retrieval of Data

FPF's comments include:

- A description of FPF and our work related to topics addressed in the Proposal.
- Sections on the four topics above. Each section describes our understanding of business practices and challenges related to the topic, as well as recommendations. FPF recommendations address the topic generally, and the section header specifies the Proposal questions covered.
- Sections responsive to CFPB questions about industry standards, security programs, and screen scraping as a method of data sharing.

Below, FPF provides recommendations reflecting its expertise in this area and in the interplay of developing business practices and technology. Key recommendations include:

- Phasing-out and eliminating the use of screen scraping—whereby a company uses a consumer's log-in credentials to access a bank or card issuer website;
- Requiring all parties to implement security programs commensurate to their size and scale;
- Encouraging development of shared service platforms to manage notices and consents;

- Establishing clarity about the responsibilities of data providers (banks), data receivers (fintechs), and aggregators, which also improves regulatory oversight models;
- Requiring opt-in consent for secondary uses of data, with a proposed definition for these uses;
- Leveraging other regulatory models like HIPAA for data retention and retrieval; and
- Supporting and strengthening industry governance and technical standards.

1) About the Future of Privacy Forum

FPF is a 501(c)(3) non-profit organization that over the last 13 years has served as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. From immersive technologies to artificial intelligence, FPF has a broad remit and expansive expertise across the field of consumer privacy. We are frequent contributors to ongoing privacy conversations around the world, and we bring together academics, civil society, government officials, and industry to evaluate the societal, policy, and legal implications of data uses, identify the risks, and develop appropriate protections. In the US, we have participated in recent and ongoing efforts by the states and federal agencies to support balanced, informed privacy rules.[1]

FPF has cultivated open banking expertise and made meaningful contributions to the analysis and discussion of these issues. FPF convenes an ongoing Open Banking Working Group with data providers, aggregators, and solution providers to examine key issues. In 2022, we organized an event on open banking with the Organization for Economic Co-Operation and Development (OECD), which was attended by global regulators and key industry experts representing many jurisdictions. At this event, FPF distributed a paper, Data Portability in Open Banking: Privacy and Other Cross-Cutting Issues, detailing how different jurisdictions' laws impacted open banking activities and intersected with data protection law, including issues surrounding consent, security, and data subject portability rights. We have continued to advance conversations surrounding open banking.

[1] The opinions expressed herein do not necessarily reflect the views of FPF's supporters or Advisory Board.

2) Authorization Disclosures and Related Consent Management

FPF appreciates the care and thought the CFPB has given in its Proposal about appropriate disclosures and consents to support data access. FPF offers comments and recommendations about: what activities need consent; duration of consents; consent management; and role of the parties. Recommendations relate to disclosures and consents generally, and are also responsive to CFPB Proposal questions 12-14, 17-19, 76, 91, and 92. FPF addresses consents related to secondary data uses in Section 4 of this comment letter.

A. The Challenge

Under long-standing federal and state financial regulations, consent relates to whether covered institutions can share consumer data with affiliated or unaffiliated third parties. The consents are typically an on/off switch. For sharing with unaffiliated parties, the standard is opt-out under the federal Gramm-Leach-Bliley Act (GLBA) and opt-in under the California Financial Information Privacy Act (SB-1). The purpose of these consents is to give consumers a say in the covered institution's data sharing practices. Historically, data sharing has been primarily designed to align with the institution's business needs – not the consumer's plans – although presumably consumers can benefit too.

More recently, certain modern privacy concepts have been viewed through a lens of individual rights. Under these rights, consumers exercise more autonomy and control about how companies use or share their information. Some examples are rights of access/correction, data portability, and the right to be forgotten. Open banking – with its focus on consumer consent and portability – is on the forefront of this trend regarding individual rights. The consumer directs the parties at a fairly granular level to meet their desired outcomes, not the companies.

In its rulemaking, the CFPB could offer helpful guidance about the main features of consent related to data sharing, such as:

- How consent options are presented to consumers, which party presents them, and how they should be shared with relevant parties.
- Which activities require consumer consent. Examples include:
    1. The parties that should provide data;
    2. The parties that should receive data;
    3. What types of data to share;

4 Uses of the data;
5 Secondary uses of data:
6 Duration and frequency of access; and
7 How long data can be retained.

- Whether all consents must be express (opt-in), or whether some can be opt-out.
- How to revoke consents and the duration of consents.
- Whether there are any exceptions to the consent requirements, such as regarding deidentified data, confidential consumer information, or legal obligations to use or retain data.

Currently, companies engaged in open banking are developing authorization notices and consent models for some of the above issues. However, the solutions are variable, incomplete and voluntary. Where data providers collect consents, they face challenges because they don't offer the open banking service so they may inaccurately describe the data needed and other features of the product. Current approaches also do not reflect common industry infrastructure, like a card network. Each consent that is captured is managed and shared on a case-by-case or party-by-party basis, which creates inefficiencies and frictions.

The CFPB Proposal addresses several of these issues and advances the ball in terms of consistency and completeness. The below recommendations offer suggestions to address any potential gaps as well as some possible larger-scale solutions.

B. Recommendations

- The CFPB should specifically indicate: 1) which of the above seven activities require consent, and 2) which belong in authorization disclosures. It is critical for notice and choice regimes to be clear about what is in scope and what is not. At a minimum, the first four items should be in disclosures. Secondary uses can be presented as those use cases are developed. Access and retention can be provided as a best practice and not necessarily a requirement. The CFPB should clarify that consent to terms of service (ToS) or signing up for a product does not qualify as consent to authorize data sharing. It should be clear to consumers, however, that certain services won't be enabled until the consumer provides needed consents.

- The CFPB should clarify that consumers can consent to all activities at once, or otherwise how consents can be accomplished separately or in groups. A single consent can be effective, and a positive consumer experience, if all activities are presented clearly and objectively, such as via specific lists or descriptions of data types and data uses. This provides a set of boundaries, acting as a kind of limitation principle, on which consent can be based.

- The CFPB, working with other appropriate regulators, should harmonize its GLBA regulations with Dodd-Frank regulations. The harmonization should clarify that opt-in consents received regarding data access satisfy GLBA sharing requirements under Regulation P, 12 CFR 1016.15(a)(1) (e.g., requirements for opt out notice at 1016.10 and for service providers and joint marketing under 1016.13 do not apply when nonpublic personal information is disclosed with the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction). If a consumer has provided a GLBA opt-out to a data provider, and later directs that provider to share data with a recipient for a specific open banking service, the more specific direction should control. The CFPB could facilitate a similar dialogue regarding opt-in directions at the state level.

- The CFPB should provide guidance about which parties should provide authorization disclosures and collect related consents. Generally speaking, the party closest to each aspect of notice and consent should be responsible for related data collection and management. Providers on the one hand, and authorized parties on the other, may each have a role to play given their relationship to the consumer and legal obligations. As an example, data providers could be responsible for activities 1 and 2 regarding who is sending and receiving data. Authorized third parties could be responsible for items 3-7 regarding their data uses and retention. The CFPB should further explore roles relating to types of data. Authorized third parties are responsible for providing the requested service, and so are best placed to specify data elements needed. Data providers want to be sure there has been proper consent regarding data types to be moved, and may have risk oversight obligations for certain data types like account and routing numbers that are used to take money out of accounts. Industry is exploring this issue and the Bureau should keep abreast of progress as it develops its rule.

- To add more value, the Bureau should provide a framework for third party consent management, or consent management platforms, to manage

authorization disclosures and consents. At a minimum, guidance should not inadvertently foreclose this market development. Benefits are manifold. It supports standardized consent rules; a consumer dashboard (versus management by myriads of companies); sharing of consents among appropriate companies; obsolescence of screen scraping; and traceability and accountability for companies and regulators. FPF is agnostic as to which industry or sector could develop or manage this model or platform. FPF notes that this model, given its centralization of consumer information and direction, would need to be supported by clear rules and restrictions regarding secondary data uses (see recommendations in Section 4 below).

- The CFPB should provide guidance about the duration of consents. FPF recommends that consents should be valid for six months or a year after the consumer's last activity. FPF understands that a short duration, like 90 days, frustrates consumers and creates drop-offs from open banking activities. Given that consumers should have a readily accessible mechanism to change or revoke consents, a reasonable time period for lapses seems workable. The Bureaus should include a caveat, however, that data providers can require re-consents sooner if there are objective red flags regarding an authorized third party, such as loss of industry certification or findings of significant compliance violations by a competent authority.

- The CFPB should provide guidance regarding exceptions for business activities that do not require consumer consent. Common examples relate to fraud detection and network security. It is also standard regulatory direction to except deidentified data from privacy rules. A complication is that there is not a deidentification standard applicable to the financial sector like there is, for instance, for health care under HIPAA. The CFPB should encourage a standards-setting body to develop a deidentification standard for the financial sector, and in the meantime allow companies to deidentify data in accordance with internal policies subject to internal or external audit. Some companies have developed sophisticated models for deidentified and anonymized data based on best practices and jurisdictional requirements across the globe. The CFPB guidance to except deidentified data should also specify that authorized third parties cannot use such data to reverse engineer confidential commercial information of data providers, and that industry standards or internal policies must reflect this limitation.

3) Roles and Responsibilities of the Parties

The CFPB can provide considerable benefit to the financial ecosystem by providing some clarifications about roles and responsibilities of the parties. This is an ideal area for guidance, directly in the wheelhouse of policymakers. Given this developing business area and different regulatory structures, the roles and responsibilities of the parties are often unclear, leading to uncertainty among the parties and inconsistent consumer experiences. After laying out the background and key examples of problem areas, FPF provides a number of recommendations. Recommendations relate to roles generally and are also responsive to CFPB Proposal questions 28, 50, 57, 58, 88, 138, 141, and 148.

A. The Challenge

Open Banking involves the interplay of different parties to enable customer-driven and innovative services. Open banking represents a true business case for data portability, as consumers direct data sharing from those parties that have data to those that need it. Data sharing also includes intermediary third parties, such as data access platforms, that support one or more parties and aspects of the ecosystem or transaction. The Proposal calls these parties data providers, data recipients, and, for the intermediary role, data aggregators. For purposes of the Proposal, covered data providers are financial institutions under Regulation E and card issuers under Regulation Z. Data recipients and data aggregators are collectively called authorized third parties. Roles of the parties can also change. For instance, a data provider or data aggregator may serve as a data recipient depending on the service and engagement with the consumer.

Consumers have different relationships and understanding of these different parties. Some of these parties are more known to consumers, like the banks where they hold accounts. Others are apparent, like companies that offer services they'd like to try. Still others, such as data aggregators or service providers, may or may not be known or apparent, depending on how or whether they choose to identify themselves to consumers.

A significant further complication is that these parties are regulated in different ways, both substantively and in the oversight they receive. Consumers are likely unaware of these differences, and the impact these differences have upon them, although they may have a general belief that their data and transactions are strongly protected given the historical safety nets provided for financial interactions.

Financial institutions have been regulated for many years under federal and state (not to mention global) banking laws, most notably by federal law, the Gramm-Leach-Bliley Act (GLBA). The legal obligations are enforced by expert banking regulators, and, in FPF's view, their oversight is arguably the most extensive of any industry. On the other hand, data receivers are only covered by this regime if they are part of the regulated financial sector, like being a financial institution or credit reporting agency. If not, these parties, like other digital services, fall under general FTC protections regarding unfair and deceptive practices and emerging state privacy laws. These state privacy laws often exempt federally regulated institutions. A result is that consumers will receive entirely different privacy disclosures and choices under GLBA and non-GLBA regimes. Intermediaries function in somewhat of a gray area. If operating as a service provider, by law and by contract, they can be regulated under either regime. Parties may also negotiate various obligations and liabilities in their agreements, and FPF has heard from stakeholders these roles and obligations are not always consistent even for similar relationships and services.

Given this developing business area and different regulatory structures, the roles and responsibilities of these parties can be unclear, which creates delays, uncertainties, or problematic consumer experiences.
Some key examples include:

1) Functional Accountability. For certain steps related to data portability, it is unclear which party is meant to perform the necessary steps. An example is management of authorizations and related consents. Open banking has managed to function on an ad hoc basis, with parties able to perform hand-offs of different aspects of consent. However, this has led to inconsistent approaches about who should manage and store consents, and how they should be shared, including with regard to consent changes or revocation.

2) Legal Relationships. The legal relationships between the parties are not well-defined under existing third party models. A common model, especially for financial institutions under GLBA, relates to service provider or vendor management. Although understandable to want to leverage existing structures, the vendor management model does not work for open banking relationships. The main reason, among many others, is that the premise of the vendor relationship is that the vendor has no independent rights to data

collected and is under the complete control and direction of the principal. In open banking services, the data provider and data recipient, and perhaps the aggregator too depending on the model, have independent relationships with the consumer. The data provider simply does not have the authority to control these authorized third parties. Without legal clarity, data providers, which are typically heavily regulated, don't know the limits of their compliance obligations, such as to follow the data, or of their legal liabilities either. Contract negotiations also suffer, resulting in more complex terms and delays, and smaller parties may also simply sign off on obligations and liabilities that they can't meet.

3) Risk Management. Since permission-based sharing involves new intersections of parties and services, risk models are immature. The financial sector relies heavily upon risk management to determine business and compliance objectives. Larger banks have extensive Enterprise Risk functions, supported by risk taxonomies, risk scoring, and risk assessments. Without clarity of functional or legal accountabilities, or appropriate risk models to use, data providers may improperly and untimely assess risk and related mitigation strategies that are meant to marshal resources and reduce consumer harms.

B. Recommendations

- The CFPB should address functional accountabilities, particularly those that directly impact consumer interactions, related to data access and portability. Suggested duties for data providers and data recipients and aggregators are described below.

    - The CFPB should provide guidance on the role of data providers. The lack of clarity on the extent of their obligations inevitably will slow uptake of open banking models, as consumers, policymakers, and industry all expect financial institutions and card issuers to protect consumers' money and data. In particular, the CFPB should clarify that data providers have responsibility to do the following:
        - Authenticate consumers;
        - Provide information about consumer accounts, such as found on periodic statements;[2]

[2] In Q28, the CFPB asks whether data providers should have to produce additional information, including about consumer reports, fees, bonuses, and security breaches. FPF considers that these items should not be required. The items are outside the purview of data access, and providing them will add cost and delay. As an example, notices for security breaches are already required, often tailored by data type, risk of harm, and jurisdiction - would this additional obligation dovetail with those disclosure obligations, including about

- Establish or participate in appropriate portals to enable data sharing;
- Authenticate the party seeking access to data in the portal;
- Follow privacy and security standards regarding data sharing;
- Employ anti-fraud measures to meet safety and soundness obligations; and
- Develop risk models that assess third party risks (see recommendation below).

This balances the provider's expected role as a trusted party, and the independent relationships that consumers establish with authorized third parties that providers do not control.

  - The CFPB should clarify obligations for data recipients and aggregators relating to authorization disclosures, consents, and data management. Data recipients, or data aggregators when acting on their behalf, should be responsible for notice and consents related to the services to be provided, such as regarding primary and secondary uses of data. The CFPB should clarify that these authorized third parties, once they receive data, are responsible for all aspects of data management, including accountability for data security and data breaches.

  - Under transparency principles, data aggregators that are not service providers, and have independent rights to process consumer data, should be required to disclose their identity and role to consumers.

- The CFPB should provide guidance to data providers about third party oversight, consistent with guidance issued by other federal banking agencies or the FTC. Guidance should assign responsibilities between data providers and recipients based on their relationship to consumers and their ability to determine the scope and purpose of data collection and processing. The CFPB should distinguish permission-based data sharing from vendor management models. The joint controller model developed under EU privacy rules is a ripe place to review. It recognizes the independent rights of the parties to process data, yet provides some structure in terms of contracts and legal expectations. FPF has heard from stakeholders that considerable time is spent negotiating the same topics repeatedly, which can cause significant

timing since the breach? What would consumers do with this information when making open banking choices?

delays and hard-to-manage contract variations. Examples of model contracts could help parties minimize variations and delays.

- The CFPB should incentivize data providers to develop risk models specifically for permission-based data sharing or open banking. This approach would drive more accurate risk assessments, better mitigation efforts and controls, and could facilitate improved oversight outcomes as well. As an example, the risk assessment could evaluate whether authorized third parties have received an industry certification, use an industry standard API, or have demonstrated other criteria deemed acceptable by the CFPB to show they can be a trusted participant. The risk assessment could monitor changes to the data receiver's status as well. When a data recipient is known to have failed certain audits, or present red flags, data providers should have the ability to pause sharing data until those risks are sufficiently mitigated to regulatory standards and in order to protect consumers. This type of oversight by data providers has a number of benefits. First, it is more helpful and relevant in managing risk. Second, it is appropriate to roles, rather than, for instance, trying to understand the data receiver's use or secondary use of data, over which the provider has no authority after the consumer has opted-in. Finally, this approach would also allow the CFPB oversight of data receivers via banks' risk assessment models – with some similarity to vendor management but more properly tailored--without the CFPB overstepping authority or providers owning business practices of non-vendor companies.

- The CFPB should establish supervisory authority over data aggregators under a larger participant rule or as service providers. The CFPB should also allocate appropriate supervisory resources according to risks posed to consumers pursuant to Dodd-Frank 12 USC 5514(b)(2). From a consumer and oversight perspective, this authority will be another method to foster consistency of rules and clarity about enforcement responsibility.

4) Secondary Uses of Data

FPF appreciates the Bureau's efforts to address what if any additional uses a data recipient or aggregator can make of consumers' data besides providing the requested service. This issue is an unresolved area of privacy law. To put the issue in a nutshell, a company will use consumer data to provide the requested service, known as the primary purpose, and then also wants to use it for other purposes, such as to perform analytics to develop new services. This question of other uses of data is often referred to as secondary uses of data. For many companies, the focus is on the benefits side of secondary uses, and less on the potential harms. The CFPB asks if additional uses should be prohibited or subject to conditions like additional consents

or notices. FPF offers the following recommendations, which relate to secondary uses generally, and are also responsive to CFPB Proposal questions 98-100, 102, and 145.

A. The Challenge

To date, secondary uses of data is not a well-governed area under federal privacy law. Under financial privacy law, consent relates to data sharing with affiliated or unaffiliated third parties, not data uses. Under health law, certain uses are permitted by covered parties; other uses require authorization. Companies not regulated by either regime are subject to the FTC's authority regarding unfair or deceptive practices.

Various regulators and policy proposals have tried to tackle this problem by defining the scope of primary purpose(s), and then requiring opt-in or opt-out consent for all other purposes, including a fairly long list of exceptions based on customer service or public policy. Under this approach, primary purposes are generally defined to cover the intended service, and also other activities that are compatible to that purpose or that should reasonably be expected by consumers. These are laudatory efforts since the approach needs to cover such a broad range of companies and uses. However, since the approach has to be so high-level and conceptual, it is extremely difficult to apply within a company or consistently across companies. What are compatible purposes and expected uses? Imagine Company A has a primary data use to provide an account aggregation tool. Is it a compatible use to sell data to advertisers who promote other account aggregation services? How about if Company A wants to use the data to develop a product which allows the consumer to better see where financial goals are not being met? As a final matter, consumer expectations, technology, and markets change over time – how or when would that trigger changes to consent management?

Risks related to secondary data uses may be heightened for financial data portability given:

- Data portability is based on consumer direction, so the consumer may be even more surprised about other uses of their data;
- Financial data is typically sensitive and its misuse can cause real harms including financial loss, loss of account access, and disparate impact;
- Unless mitigated, there could an ability to reverse engineer or engage in other anti-competitive behavior (such as based on data mining) that can reduce competition and increase consumer costs; and
- The potential for BigTech to become an emerging player raises risks for market impact and extensive data analytics, up to and including data

externalities and behavioral influences over other consumers whom BigTech can connect to the initial consumer.

The CFPB has an opportunity to simplify this complex question in the specific context of data access. These services are all about consumer direction and control, and secondary uses should be no exception.

B. Recommendations

- The CFPB should not prohibit secondary uses.[3] Consumers should be able to choose them just like they do with the primary service.

- Consumers should have to opt-in to other uses that are not the primary use of the requested service, or customer service related to the primary use and other uses. The primary use should be described in the authorization disclosure so it all ties together. An example could be as follows: A data recipient has a user interface for a particular product. As part of data analytics related to customer service, the company discovers there are pain points in the user experience. The company can use consumer data to fix the user interface flow. It can then make similar changes to user interfaces for other products.

- Consents to secondary uses should be similarly prominent as the initial consents, and should be segregated from the primary use opt-in.

- Exceptions should be prominent and clear in disclosure statements. The CFPB should consider whether the same list of exceptions applicable to primary uses should apply to secondary uses. As an example, as described above, an appropriate exception relates to the use of deidentified data.

- The data recipient, or data aggregator when acting on the recipient's behalf, should collect and manage these consents, perhaps in a consent management tool or platform.

This approach will lead to clearer and more consistent implementation, promote fair market competition, and also substantially reduce the risks of harm in this developing ecosystem. Consumers will be put in informed control of how their data is being used. It can also perhaps set a model for other open data regimes.

[3] As one caveat, the CFPB should clarify that anticompetitive behavior, such as reverse engineering of confidential commercial information or algorithms, is prohibited.

5) Data Retention and Retrieval

FPF applauds the CFPB for tackling the question about when companies should delete consumer data. Consumers may have an expectation that their data will be deleted upon request or upon terminating a service. These expectations may be heightened for open banking services since consumers exercise so much control over data flows and uses. Consumers may also be aware of developing legal requirements, often termed the right-to-forgotten, to delete information when requested. However, data deletion is a complex compliance challenge. Guidance can help set expectations for consumers and clarify requirements for companies. FPF recommendations relate to the topic of retention and retrieval generally and are also responsive to CFPB Proposal questions 37, 103-105, 110, and 119.

A. The Challenge

Historically, regulations related to retention focused on minimum timeframes for keeping information – not on the maximum. Myriad federal and state laws, dealing with a variety of topics, include a retention obligation. Retention requirements are typically couched as records retention. A main purpose is to ensure companies keep records so that regulators can perform oversight or enforcement regarding the law in question. Indeed, per Proposal question 119, the CFPB proposes its own retention requirements. Although the CFPB may limit retention of consumer data, other retention laws don't generally consider personal data minimization.

The countervailing obligation, to delete records, is a fairly new development, championed initially in the EU as a privacy right for data relating to individuals. The obligation now arises in many new privacy laws. Where the obligation appears, there is often a list of exceptions which can be extensive.

Policymakers may have a misimpression that companies desire to keep consumer information indefinitely. There is of course business utility in keeping current or fresh information. However, besides the need to comply with emerging regulatory deletion obligations, companies reduce a number of important risks by deleting consumer records. Stale data is more likely to be inaccurate. The risk of a large data breach rises substantially with over-retention of data. Over-retention also complicates other compliance obligations, such as to retrieve and produce information in response to litigation or consumer access requests. In addition to the sheer volume of data, data may be dispersed in many systems, sometimes legacy systems that are difficult to manage.

Policymakers may also under-appreciate the compliance challenges to destroy records. First, legal obligations to retain data are dispersed in many laws and may be

hard to determine. Large companies typically adopt elaborate record retention schedules developed by law firms. These schedules, given the variations and complexities in the data retention requirements, are difficult to operationalize. Examples of challenges include:

- Retention schedules have complex formulas like life of the relationship + 10 years that must be applied record by record;
- Large amounts of data have been collected and are spread across many disconnected and/or legacy systems;
- Data is typically not date-stamped in databases, at least historically;
- Records are defined terms in retention schedules (including official and unofficial business records) that don't match entirely to definitions for personal information; and
- Companies must not destroy data subject to litigation holds, and penalties for spoliation are considerable.

B. Recommendations

The CFPB should be mindful of these challenges and consumer expectations as it sets rules about deletion and retrieval obligations.

- FPF supports the Proposal to permit deletion exceptions for records that must be kept to meet other legal obligations. To facilitate this exception, guidance should allow companies to rely on their retention schedules as a compliant solution.

- To avoid conflicts of laws with companies' retention schedules, which are based on extensive legal obligations, the CFPB should refrain from issuing inflexible retention time periods.

- FPF suggests the Bureau review other long-standing privacy regulations that offer sensible ways to address storage and retrieval questions relevant to data access and deletion. Under the Privacy Act of 1974, agencies have an obligation to provide information in what's called a 'system of records' (SOR). A SOR is basically records storage that allows retrieval based on the individual's name or other identifier – so reflects records the agency uses to deal with that individual in any capacity. HIPAA has a similar scope requiring access to records in 'designated record sets' (DRSs). DRSs are generally medical, claims and payment information, or other information that the covered entity uses to make decisions about the individual. The CFPB could use a similar model and prioritize deletion of this type information. This approach would address data used by the company, which is the primary risk, and would be faster and more efficient to implement.

- In response to Proposal Q37 regarding an exception for providers to retrieve data based on their ordinary course of business, FPF similarly recommends that the Bureau adopt a principle like system of records or designated records sets. These formulas reflect the ordinary course of business. The data provider accesses information about consumers for its own purposes based on these principles. The data provider should not have to hunt down every reference to a consumer that it does not retrieve itself in its ordinary business course. Information that is currently provided to consumers via periodic statements clearly falls within the ordinary course of business, but as the scope increases beyond what is required by existing law, the relation to the ordinary course of business becomes more tenuous.

- As the CFPB develops implementation timing requirements, given records deletion is an emerging and complex area, the CFPB should consider providing companies a longer lead time for compliance, or a staggered way to achieve compliance as the Proposal suggests for other topics.

- The CFPB should provide certain other alternatives to deletion that mitigate the risk of ongoing data use. Examples include an exception for deidentified data, which is a common privacy exception to privacy requirements, since information is no longer tied to an individual. The CFPB should also consider a safe harbor for companies to archive personal data so it cannot be subject to ongoing use. As examples, the safe harbor could relate to systems under review for data deletion, or that need to be kept for other legal obligations but are no longer needed to provide the requested service.

- Consumer expectations should be addressed. FPF believes consumers should be notified if their information is not deleted upon request or when the open banking service is terminated. The notice should include if any mitigation strategies were deployed, such as personal data has been archived and won't be further used, or has been deidentified.

6) Industry Standards

The CFPB requests information about its role regarding developing industry standards and what steps it can take to support trusted data exchanges. Examples are Proposal questions 57, 58, 72, 73, 80, and 81.

This remains an appropriate area of focus for policymakers. Typically, policymakers provide frameworks and policy requirements for industry implementation. Policymakers often prefer not to set technical standards as they are less close to the technology builds, the consumer relationship, and changes to technological

developments. As an example, if there is a technical fix needed for API implementation, the update can be addressed more efficiently by industry than by the regulatory process. As described in this comment letter, industry can benefit from policymaker guidance about the scope of requirements, consistency of rules, and role clarity. Policymaker prioritization and enforcement can also help incentivize more responsible business activity. The development of industry standards is an ongoing process that policymakers can monitor appropriately.

A nonprofit organization known as the Financial Data Exchange (FDX) has been working on technical requirements for data access portals and APIs. The technical requirements have been developed by consensus across over 200 hundred companies representing data providers, recipients, and aggregators. FPF is a non-profit member of FDX. One of the activities that FDX has undertaken is a certification process for data aggregators and data recipients which requires them to adhere to certain technical practices in order to earn FDX certification. Data providers can have more confidence authenticating FDX-certified parties to receive data and trusting them as an accountable party. FDX also maintains a registry of member organizations which will also list their certification status once that program goes live.

A. Recommendations

- The CFPB should consider how it can build from the FDX third party technical certification process to make the recommended data portal process more secure and trusted. Specifically, the CFPB can:
    - Indicate what factors should be included for an appropriate industry certification process. Part of the process should include that third parties should publicly recognize its certified status and attest to the required business practices required by the certification.
    - For third parties that become certified, provide them a safe harbor as qualified as an authorized third party. For non-certified third parties, the CFPB could require additional criteria or allow data providers to impose processes such as due diligence reviews (which they could charge a reasonable fee for) or contract negotiations before providing data to them.
    - Work with appropriate regulators to provide oversight and enforcement over third parties that have certified and attested to required practices.

These activities will encourage appropriate certification and responsible business practices. They will also aid effective oversight, as a nonprofit does not have this authority or bandwidth.

- The CFPB should consider other areas where it can, as appropriate for respective roles, shape or leverage industry efforts to foster data access. FPF would welcome further dialogue on this topic as an area of our expertise.

7) Security Programs

The CFPB asks if it should establish guidance regarding needed security programs to support data access. The security of data has long been a focus in the financial sector, given the harms that can result from poor security practices. FPF provides the following recommendations which are responsive to CFPB Proposal question 111.

The Bureau indicates that data providers are governed by the safeguards framework under GLBA, and considers that data recipients and aggregators are likely subject to these requirements as well. To make sure security obligations are covered, the CFPB requests feedback as to whether its rule should require authorized third parties:

- To develop, implement, and maintain a security program appropriate to their size and complexity, as well as the volume and sensitivity of the consumer data they manage. The rule would provide that compliance with the Safeguards Rule or Guidance would constitute compliance with the Dodd-Frank rule; or
- To comply directly with the Safeguards Rule or Guidance.

A. Recommendations

- The CFPB should require data recipients and aggregators to establish and follow security programs to protect consumer financial data. Either of the CFPB proposals are workable, and the CFPB should refrain from creating a new security standard given the extensive obligations already in existence. The CFPB could also include a resource component, e.g. that authorized third parties have sufficient resources to employ effective security programs and ensure business viability. It is important for all participants to prioritize security, including via written policies, risk assessments, controls, training, audits, testing, and other elements of an effective program. However, there should be awareness that implementation of a security program based on a company's size and scale will not necessarily result in equivalent security practices across all parties. Some parties, such as innovative start-ups, will be significantly smaller than, for instance, a national bank, so that their

relative security programs will not be comparable even with establishment of this requirement. However, the requirement represents important steps in the right direction, improving security and consumer protection, and should be imposed.

- CFPB guidance should link security programs and related resources of authorized third parties into industry certification processes or data provider due diligence reviews, per Section 6 above.

8) Screen Scraping

The CFPB requests feedback about the practice of screen scraping to enable data sharing. Screen scraping involves the consumer giving a data recipient their log-in credentials to a data provider website, such as chase.com. The data recipient then uses the credentials to access the consumer's account to obtain information, typically in an automated fashion. The CFPB recognized a second method to enable data sharing in its Proposal. Under this other method, data providers, recipients, and aggregators work together to use software, known as APIs, via which the data provider can authenticate the consumer and transmit requested data without the consumer having to give credentials to a third party.

Regarding screen scraping, the Proposal asks, such as in questions 69, 90, 95, and 109, how various proposed requirements could be implemented. As some examples:

- How would data collection be limited to needed data elements only?
- How would data deletion occur?
- How would consumer revocations or service terminations be implemented?

Compliance would certainly be more difficult, if not impossible, to implement across every topic. An additional question is how compliance with any of these requirements could be verified. Parties would not need to work together or enter into contractual arrangements so related controls for consumer protections would not exist. Verification may only be possible via auditing functions by appropriate regulators. Screen scraping is also disruptive to data providers, which have to deal with automated scraping on their websites and distinguish that activity from criminal data entry efforts.

However, beyond compliance, verification, and security challenges, more fundamentally screen scraping involves a consumer providing log-in credentials to financial accounts to a third party. The third party, which the consumer may know little about, can access the account and act as the consumer. Screen scraping continues to pose ongoing risks to consumers. Industry and policymakers need to discourage this activity and provide other options to enable data sharing.

A. Recommendations

- The CFPB should phase out and then prohibit screen scraping as a permissible method for companies to obtain information from data providers. The CFPB could provide a reasonable timeframe for the phase out, given industry's growing maturity regarding the API solution. During the phase-out, and perhaps for a short time period afterwards, a limited exception could be allowed for service outages so that transactions aren't disrupted. For this exception, heavy preference should be given to options that do not expose consumer credentials, such as tokenized access via the data provider. The use of consumer credentials should only be allowed if there are no other options, and only with strong and verifiable mitigation measures such as evidence that credentials were deleted when API service is restored. The CFPB should evaluate the value of this exception during the time period it exists, and eliminate it when it is not truly needed, either because it rarely arose or the preferred solutions have sufficiently matured. The use or maintenance of consumer credentials is a poor solution and should be prohibited as an option as soon as reasonably possible.

- The CFPB should encourage efforts by appropriate bodies, such as FDX, to spread the use of API solutions across all parties in the ecosystem, for the benefit of consumers. CFPB guidance should facilitate appropriate cost sharing for infrastructure commonly used by all parties.

***

FPF thanks the CFPB for the opportunity to comment on its Proposal. The CFPB has considerably advanced many concepts about data access and by extension open banking. Some clarification of roles and certain obligations can help achieve laudable goals and outcomes. Working together, roles and policies can form simpler, more consistent, and better and safer consumer experiences. FPF looks forward to continued progress on these important topics, which can also help inform privacy thought leadership as these principles continue to develop. If you have any questions regarding these comments, please contact Zoe Strickland at zstrickland@fpf.org.

Sincerely,

Zoe Strickland
Senior Fellow

Daniel Berrick
Policy Counsel