Consumer Data Rights

Cite
Small Business Advisory Review Panel
for Required Rulemaking on Personal Financial Data Rights

Recommended Distribution:
Retail Finance, Privacy, Digital Finance, Policy, Legal, Government Relations

Website
https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf

Impact Assessment

- If personal data are a new form of capital as many academics have come to believe, then the CFPB's decisions about which firms have access to consumer data under what circumstances will have far-reaching strategic consequence.
- Open data exchange would reduce legacy-provider competitive advantage, likely enhancing innovation and lowering some prices but also encouraging reliance on unregulated providers not only for core services, but also advice possibly based on conflicting business interests or unreliable/inaccurate protocols.
- Third-party portals would become a new form of critical financial infrastructure under an uncertain regulatory framework not only when it comes to data integrity, but also security, operational resilience, and conflicts of interest.
- Minimizing consumer and systemic risk in concert with expanded data rights appears to require a highly complex set of CFPB rules that will need a careful design to avoid regulatory arbitrage opportunities, identify areas where standards are needed outside the CFPB's jurisdiction, address burdens that may undermine both innovation and market-entry providers, and give consumers the data and product-selection power intended by the CFPB.

Overview

Beginning a long-awaited rulemaking process on the extent to which consumers have rights to their own data and how these rights may be exercised, the CFPB is seeking views on an array of ideas and questions to guide future action. This outline is essentially an advance notice of proposed rulemaking (ANPR) in which the Bureau outlines its initial thinking on key questions such as the extent to which screen-scraping should be allowed, whether new security standards are needed, and when consumers are at risk and the rights and remedies they have following a decision to open their personal data to parties other than the entity that holds key accounts. Although limited to only a few

transaction-account offerings, the CFPB's framework is also intended as the base from which consumers would gain rights to their data across the full range of retail deposit, loan, payment, and related financial services. "Open" banking along these lines would increase account portability as well as ease access to advisory services (e.g., budgeting, investment, funds transfer) but raise numerous consumer-protection and even systemic concerns based on the extent to which consumers understand the risks attendant to new providers as well as those embedded in the portals that either provide these services or identify those suitable for an individual consumer. Complex questions also arise because of the interplay between a consumer's data in a specific account he or she may have chosen and the way transactions and thus personal data flow through the financial system via payments or other interactions. The CFPB appears intent on governing these interconnections under numerous data-privacy and -protection standards, but how this is actually to be accomplished and then enforced is a complex challenge as evident not only from the questions posed in this outline, but also the description of the options initially favored by the Bureau.

Impact

The CFPB has been struggling with the issue of consumer data rights since the Dodd-Frank Act of 2010 first gave it the power to establish them.[1] Although it issued an ANPR in 2020,[2] the CFPB since has focused on other priorities despite this statutory requirement. Now, the Bureau has not only turned to this question, but also taken a very different approach than the Trump Administration's agency because it and the Biden Administration are focusing on the extent to which the network effects derived by bigtechs and/or large financial companies from personally identifiable information give them undue market power that adversely affects consumer privacy, product choice, and even market integrity. Indeed, President Biden's executive order on market competition urged the CFPB to enact new rules granting consumer data rights.[3]

The Bureau has thus touched on this competition concern in many recent actions, including a recent policy edict on digital marketing,[4] but it is now going to the heart of the issue to set the terms and conditions on which the U.S. would have a system akin in at least some ways to the "open banking" construct found in the European Union, Britain, China, and some other jurisdictions. The paper includes a detailed description of the Bureau's views and research supporting them to validate the importance of increasing consumer data rights. It also lays out an array of implementation challenges, resolving only a very few with concrete proposals.

The agency notes that the Dodd-Frank Act describes a consumer for purposes of data rights as the consumer him- or herself and/or agents or certain other parties acting on the consumer's behalf. This is read as requiring the agency to craft standards allowing certain third parties access to data based on the consumer's authorization. Among the many complex questions this definition

[1] See **CONSUMER14**, *Financial Services Management,* July 19, 2010.

[2] See **DATA**, *Financial Services Management*, November 4, 2020.

[3] See **MERGER6**, *Financial Services Management,* July 9, 2021.

[4] See **FINTECH30**, *Financial Services Management,* August 15, 2022.

engenders is the role of payment networks in providing consumers with relevant data. Although the proposal initially appears to cover only "direct and indirect" account providers for covered services (see below), it also notes in detail how payment-system providers have information that could be of considerable value to consumers in areas such as judging which transactions have the highest interchange fees or learning who participated in unauthorized transactions. These payment providers would, like covered account providers, need to provide covered information to authorized third parties. The Bureau has yet to detail how it will otherwise govern payment-service providers, although it has sought extensive information from bigtechs in general and nonbank payment providers (e.g., PayPal) in particular.

The outline does not deal with how the Bureau would approach any mandatory data access requirements when the Federal Reserve is the consumer's payment network. The issue of personal privacy related to the Fed has so far come up principally with regard to CBDC,[5] which could prove even thornier when it comes both to gathering sensitive personal information and transmitting it to third parties outside the Fed's regulatory or supervisory reach.

The Bureau also seeks comment on ideas such as allowing third parties to access provider information germane to an account such as the incentives paid to staff or others related to generating, servicing, or cross-selling the account holder or transactions related to the account. The Bureau suggests that these data would have considerable value to the consumer in evaluating providers and thus enhancing market competition, but these have long been considered confidential business information. As with the fraud-related payment-system noted above, these data points could be considered proprietary business information and thus included in the list of data related to a consumer expressly exempted from personal rights in the Dodd-Frank Act. These proposed rights will be among the most controversial in concert with consideration of the extent to which the outlined CFPB approaches may go beyond its express authority.

Another controversial question is the use of screen-scraping aggregators. The outline expresses significant concerns about their use but does not propose a specific ban, instead laying out numerous restrictions that might be imposed with regard to data availability and accuracy that would then be backed by strict standards ensuring compliance and accountability. It is unclear if screen-scrapers could comply with what is likely to be required and, even were they capable of doing so, if many would choose to adhere to standards that significantly change their business model.

The Bureau's intent is, as noted, to increase market competition. As a result, it takes an expansive view of the data legacy providers now maintaining instead of setting broad standards within the boundaries of the exemptions noted above to which account-providing institutions would then be expected to comply. The Bureau instead suggests it will not only take control of data rights by defining open data in a very detailed fashion, but also limiting exceptions with additional express

[5] See **CBDC10**, *Financial Services Management,* January 27, 2022.

standards because, it notes, legacy providers may use these statutory exemptions to hoard consumer data that would undermine market dominance. The balance among the Bureau's open objective, consumer rights, data sensitivity, and provider business models will prove among the most challenging aspects of the agency's final rule.

Ambiguities over the security of provider data transmitted to third parties is another structural challenge the outline does not fully address. At some points, it suggests that all providers and third parties are adequately governed under current banking agency and FTC data-safeguard standards. At other points, it seeks views on the extent to which third parties should come under express new data-security standards. Even were the agency to mandate these, the extent to which it could examine or enforce them is uncertain. The same considerations would also apply if Bureau decides to limit third-party secondary uses of consumer data, impose accuracy standards, and/or give consumers certain disclosure and revocation rights. No express liability for any misuse, loss, or theft of consumer data provided to an authorized third party appears to apply to that third party absent or even in concert with regulatory noncompliance, perhaps making the initial data provider at risk if a consumer's data once in its hands goes astray or awry.

The CFPB appears to believe that covered products (see below) come largely from regulated institutions, but this is less and less the case as the agency's own bigtech/fintech actions make clear. To the extent the agency enforces open-banking at regulated companies but fails in practice also to provide like kind consumer rights and remedies in unregulated entities, significant market asymmetries could result that not only fail to reduce market-power concentrations, but also increase consumer or systemic risk.

What's Next

Although framed as required by CFPB procedure, the request is similar to another advance notice of proposed rulemaking and will serve as the base from which the Bureau expects to issue a formal proposal in 2023 and then to finalize rules effective early the following year. The Bureau issued this request on October 27; comments from those not directly engaged in the small-business review are due by January 25. Although the rule addresses third-party portals in often-technical detail, it does not directly address the extent to which these portals could become a form of critical financial infrastructure. CFPB Director Chopra has, however, indicated that he plans to address this without saying how to do so or whether this would be done in the context of final data-privacy rights and/or some form of systemic designation by the FSOC.

As noted below, the Bureau is seeking comment on how best to implement its final rules, planning now to implement and mandate them even if suitable third-party data portals are in early stages of construction in compliance with the final rule.

Analysis

The analysis below summarizes strategic issues raised by the agency's analysis and questions on possible policies. The outline is complex, including 149 questions and various, sometimes contradictory regulatory options. It also

includes a detailed discussion of small-business considerations largely omitted from the analysis below.

A. General Questions

Those on which views are sought include:

- any law or rule that may be adversely affected by the CFPB's approach;
- small-business costs and opportunities;
- enforcement or supervisory challenges; and
- the subset of covered data providers and how best to proceed in future.

B. Data Providers

Data providers are the institutions now holding customer accounts that would be opened to third parties. The CFPB approach here would:

- initially cover only depository and non-depository institutions that are considered financial institutions under applicable law which provide consumer fund-holding accounts– i.e., banks, credit unions, prepaid account providers, and those providing mobile accounts, digital wallets, and similar products regardless of the extent to which an account is held at another institution. Data providers would also include banks and nonbanks providing credit card or otherwise issuing cards (i.e., those acting as agents for the card issuer for open-end plans even if the account is held by another institution);
- exempt accounts other than those noted above at covered institutions (e.g., mortgages) at this time; and
- possibly exempt some providers of accounts based on burden, size or other considerations detailed in the release.

C. Third-Party Access

Here, the Bureau is considering:

- requirements governing issues such as the terms of access, disclosures related to access, and certifications to ensure that these terms are met. Detailed requirements and related consent procedures are explored in this outline in areas such as limits on data collection, use, and retention;
- standards differentiating aggregators from other third-party recipients (e.g., with regard to disclosures and certifications);
- how best to implement statutory requirements to exempt provider data in areas such as fraud, AML compliance, and proprietary algorithms. The law also states that information that must be kept confidential is expected, but the Bureau is considering limiting this exemption only to information that by law must be kept confidential from the consumer. Limiting the "confidential" exemption in this way might for example force depository institutions to disclose to the consumer the company's judgment about his or her creditworthiness;

- whether to impose restrictions on the extent to which an account holder may use exemptions to block data transfer; and
- the categories of data that would have to be provided (e.g., periodic statement information, prior transactions, prospective online transactions, account-identity information, and other information such as the fees or bonuses associated with the providers' account policy).

Account-identity data are described along with the Bureau's concerns that requiring these to be shared by an account provider beyond those expressly authorized by the account holder (e.g., in connection with a loan application) may create significant privacy and fraud risks even if "confirm/deny" formats are used. The Bureau notes that payment networks often have additional information that would be useful to consumers (e.g., with regard to fraudulent transaction participants).

D. Information Availability

1. Consumers

This section of the outline deals with when and how information must be made available directly to the consumer. The law suggests development of standardized approaches to information release and the outline thus discusses various ways to mandate this and poses numerous questions about how best to do so, including with regard to inaccurate information and resulting costs or burden.

2. Third Parties

This section of the outline describes different ways third parties now access consumer data, noting that screen-scraping is particularly problematic. The Bureau is considering requiring third parties to establish a portal that does not require the third party to possess or retain consumer credentials, asking numerous questions about how best to do so with particular regard to matters such as fees, data availability, security, customer authorization/revocation protocols, and accuracy. The nature of these questions suggests that final rules will include numerous regulatory, supervisory, and enforcement requirements. The Bureau is also considering whether to require account providers to notify consumers when a third party seeks access to their information under a purported authorization and perhaps after submitting information to the provider sufficient to ensure the third party's identity and the account-provider authenticates it. It is, though, unclear if the account provider would need to honor a third-party authorization while a disclosure is pending with a consumer who may come to dispute access or otherwise experience fraud or other risks.

In addition to these standards, the Bureau is also considering whether third parties should have express obligations to consumers. These could include:

- limiting the collection, retention, and use of authorized data;
- curtailing the duration and frequency of data access;
- requiring express revocation rights and processes;
- restricting secondary uses of authorized data by flatly prohibiting it, defining high-risk uses, or requiring opt-outs or -ins;

- imposing new data-security standards even though the Bureau believes that most third parties fall under current data-safeguards standards;
- setting rules for data accuracy and dispute resolution;
- mandating disclosures of factors such as data-access terms (e.g., revocation); and
- mandating record-retention requirements.

E. Implementation

The Bureau is also seeking comments on how best quickly to implement new standards, noting that it will provide "plain-language" compliance guides in addition to final rules. The agency recognizes that it may take time to establish standardized data portals for communications between covered-account providers and third parties but believes its other standards could go into effect quickly to ensure consumer protection.

Federal Financial Analytics, Inc.
2101 L Street, N.W., Suite 300, Washington, D.C. 20037
Phone: (202) 589-0880
E-mail: info@fedfin.com Website: www.fedfin.com