Consumer Data Rights/Open Banking

Cite

CFPB, Notice of Proposed Rulemaking, Required Rulemaking on Personal Financial Data Rights

Recommended Distribution

Retail Finance, Payments, Privacy, Digital Finance, Policy, Legal Government Relations

Website

https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf

Impact Assessment

- Open banking could increase competition for what are now sticky bank customers reluctant to select alternative providers due to the high transactional cost of identifying more attractive options, marshalling personal data, and safely transferring to a new provider.
- Consumers may also more easily find third parties providing budgeting, bill-payment, wealth-management, and other value-added services not provided by their bank, perhaps leaving IDIs with low-return functions and a largely operational role.
- Third-party portals could 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.
- However, data-integrity, -security, and -privacy challenges are formidable obstacles to sound implementation of open banking. The Bureau's proposed framework addresses this with many complex standards intended also to reduce data-provider liability in the event a third party does not properly adhere to its representations. Third parties are also subject to extensive authorization procedures, CFPB supervision, and consumer transparency and obligation requirements. How well the Bureau implements and then enforces these complex standards will determine how well competition and consumer data protection are balanced.
- Given the challenges of identifying all authorized third parties and CFPB supervisory/enforcement limitations, it seems likely that data providers will bear the brunt of both direct and indirect compliance and enforcement.
- The extent to which standard-setters are able to meet CFPB requirements and thus facilitate open banking will prove critical to program success for providers, third parties, competitors, and consumers. Similarly, the CFPB contemplates technological solutions that may facilitate compliance; if these are developed, then the complex new regime may be more easily implemented and robustly deployed.
- It is also unclear if the open-banking regime will promote the Bureau's goal of increasing the market power of "relationship-banking" entities at the expense of giant banks or if the cumulative effect of pending rules, broader market conditions, and heightened account portability will advance the migration of more profitable financial services outside the regulatory perimeter, contributing to the realignment of regulated banking as a sector providing portals and infrastructure, not core financial intermediation and community-access financial services.

Overview

Following a request for information that was a de facto advance notice of proposed rulemaking,[1] the CFPB has now proposed a preliminary, but binding framework for consumer data rights covering consumer "transaction" accounts offered by banks, credit unions, and – a departure from the initial outline – nonbanks/fintechs. The proposal is sweeping with regard to data-rights and -sharing standards for covered accounts and providers, but still preliminary in that the Bureau has yet to turn as it plans to in in subsequent actions to loan products such as mortgages and student loans. Although details of the open-banking standards for these products and covered providers will vary, the overall construct the Bureau finalizes would apply with particular regard to matters such as consumer rights and data standards. As a result, this proposal is, for all the issues it leaves for later, a sweeping rewrite of the manner in which consumer-finance companies could make use of one of their most valued assets: personally-identifiable digital data. The combination of the importance of this new regime to commercial success and consumer rights combined with the complexity necessary even to begin to balance these objectives under rapidly-changing digital-finance technological developments will have profound implications for the future configuration of consumer finance, its integration with commercial service providers such as tech-platform companies, and financial stability. The speed with which the Bureau plans to finalize and then implement its open-banking construct would likely lead to rapid change without the ability necessary to also alter direction or introduce new controls should these prove necessary to ensure consumer protection, sound finance, and effective competition.

Impact

This proposal implements what the Bureau calls "dormant" authority in its authorizing statute to grant consumers the right to control the data maintained on them by financial-services firms, to set technical standards by which this may be done, and to give consumers additional financial-data privacy rights.[2] The proposal also builds on additional federal statutes the CFPB believes authorize its provisions and the Bureau's recent advisory prohibiting what the Bureau calls "junk fees" when consumers seek account data.[3] This initiative is also consistent with the Bureau's use of its consumer-finance authority to advance the President's executive order pressing heightened competition.[4] As a result, the Bureau's approach to data rights is designed to create a broader open-banking agenda very different than the approach initially espoused by the Trump Administration's CFPB in 2020.[5]

The Bureau in part builds its new approach on the rapid pace at which it finds consumers to have sought to distribute their financial data to access other financial product providers or obtain financial services not offered by dominant providers – the large banks and credit unions considered "data providers" for purposes of this proposal along with nonbank entities offering covered financial products and services. At least 100 million Americans are found by the CFPB to have allowed third parties to access their account data, with this done billions of times in 2022 via "screen scraping" and other technologies regardless of the data-integrity and privacy rights this creates to the data holder and consumer. Third-party access is said to be most often allowed without full

[1] See **DATA3**, *Financial Services Management*, November 4, 2022.

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

[3] See **CONSUMER52**, *Financial Services Management*, October 13, 2023.

[4] See *Client Report* **MERGER6**, July 9, 2021.

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

consumer understanding of these risks in order to achieve functionality (e.g., budgeting) or better rates and services than believed possible from the account holder. The extent to which the Bureau now mandates third-party data access along with consumer data rights and access thus has significant implications for competition, privacy, data-security, market-integrity, and payment-system functionality.

Reflecting this, banks strongly objected to the Bureau's initial outline on the grounds that it created significant competitive inequity between regulated institutions with severe liability for consumer and market risk and fintechs or other nonbanks that could still more easily obtain consumer data without like-kind safety, soundness, and privacy obligations. Applying the new framework to banks and nonbanks as proposed broadly addresses these competitive concerns, but still has asymmetric soundness challenges because federal data-integrity and privacy standards apply only to banking organizations and, to a certain extent, credit unions. As detailed below, the Bureau attempts to address this with standards that cover all data transfers from covered companies related to covered data, but significant supervisory and enforcement asymmetries remain due to the Bureau's more limited enforcement power and reach over nonbanks in contrast to its coverage and that of the federal banking agencies over depository institutions.

The Bureau also proposes standards that prevent reliance on screen-scraping (the most problematic form of third-party access according to both data providers and the Bureau). This would pose significant franchise-value problems not only for entities that provide screen-scraping services, but also for the nonbanks that rely on screen-scraping to identify new customer prospects. Firms in this arena fear that the Bureau's standards will make business growth slower and more costly, undermining competition; the Bureau preliminarily concludes that these potential problems are warranted due to the need to ensure robust rights and numerous consumer protections.

The data-integrity standards to be set by this rule are also said by the CFPB to prevent "rent extraction" by data gatherers that put consumers at risk. However, the Bureau is also keen to prevent banks and other data providers from similar anti-competitive actions. As a result, information data providers would need to transfer is that related to product or service price. This will facilitate comparison shopping and provider switching, but is in practice complicated by many factors in most covered products and services. For example, transaction- and savings-account pricing depends on factors such as a consumer's initial balance, transaction frequency, related fees, and minimum maturity. Credit cards are often complex trade-offs between fees, interest rates, and reward features. The standard-setting process the Bureau outlines to define how data are to be transferred will surely address these challenges, but the manner in which it is done will determine both competitive impact and consumer understanding. Complexities could obscure key features and lead consumers to select what might turn out to be higher-priced products, particularly if the consumer is looking for a new provider under different financial circumstances not reflected in his or her current data used by data recipients for product underwriting, pricing, and other key offer factors.

Data to be provided also would have to include those needed to initiate a transaction on a consumer's behalf. This would be of significant value to payment entities such as PayPal or Plaid and even nominally backroom payment-service providers who could develop interfaces with consumers that ensure bill-payment and other transactions that press banks still farther to the margin of value-added consumer-financial products. Tech-platform companies could also create seamless interfaces between their payment products and underlying bank accounts, with the proposal seeking to limit the network effect and market power resulting from this knowledge by limiting its use only to providing financial services. Given the scope of tech-platform offerings and the wide variety of eligible financial products, these firms could still gain considerable market clout.

What's Next

The CFPB proposed this rule on October 19; comments are due by December 29.

The proposal sets compliance dates for covered providers (see below) for tiers based on provider size and whether the entity is a bank. The compliance dates would run from six months after issuance of the final rule for depository institutions with over $500 billion in assets and nonbanks generating or likely to generate at least $10 billion in revenue in the preceding calendar year. Smaller IDIs and nonbanks would then go into a more delayed transition, but all nonbanks would need to comply within one year of the rule's release. The smallest banks (i.e., those with less than $850 million in assets) would need to comply four years after the rule's issuance. Comment is sought on these tiers and coverage as well as on providing additional time for compliance if needed to ensure third-party compliance meets necessary risk-management criteria.

Analysis

I. Scope

A. Key Definitions

1. Covered Products

These would be:

- depository-institution transaction and savings accounts;
- prepaid payroll cards;
- credit-card accounts, considered transaction accounts for purposes of this rule because the Bureau says that they are increasingly used as payment instruments;
- digital wallets; and
- products of services facilitating payments from these accounts.

The Bureau is seeking comment on whether government electronic-benefits transactions (EBTs) should be covered in the final rule or to do so going forward in subsequent standards. Comment is also solicited on the Bureau's decision to exempt mortgage and other consumer-loan products on grounds that that they do not support transaction-account underwriting or payments even though information about them is often shared. However, future rulemakings would address these products.

2. Data Providers

These are generally banks and credit unions, credit-card issuers, and any person who controls or possesses information related to covered accounts with a consumer interface unless the entity is a bank or credit union that does not offer an interface on the rule's effective date. Comment is sought on whether the proposal's definition fully covers neobanks and other nontraditional entities, with views also sought on whether nonbanks that possess or control data without consumer interfaces should also be exempted.

3. Third Parties

Third parties gaining access to consumer data following consumer consent would be defined as any person or entity, including a data aggregator, that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data. Authorized third parties are those that meet conditions noted below. The proposal also sets authorization procedures including disclosures to consumers regarding how a request will be handled by the third party. "Informed consent" by the consumer to the third party is required prior to data access or transfer. Specific requirements apply to third parties to ensure that they act in consumer interest and when the third party is an aggregator and numerous record-keeping requirements are also proposed governing data providers. These would among other things need to ensure ongoing third-party adherence to CFPB requirements. Comment is sought on whether these standards should apply to some third parties (e.g., small ones).

The proposal also imposes an array of restrictions on third-party data recipients, including mandatory consumer disclosures, consumer rights to revoke authorization, record-retention standards, a one-year duration period for data retention and access services, a defined set of third-party obligations, and stringent limits on the use of data only for the purposes stipulated by the consumer. Data received via these authorizations also could not be otherwise monetized, but comment is sought on whether third parties could offer consumers and opt out from these restrictions on secondary use of their personal data. Third parties would also have to certify that they comply with the Gramm-Leach-Bliley privacy requirements governing banks.[6] Third parties that contract with others to handle consumer data must ensure that their out-sourced providers comply with all the requirements that directly apply to the authorized third party.

As in numerous sections of the NPR, comment is also sought here on whether there are technology solutions that would automatically ensure compliance.

B. Industry Standards

Indicators of compliance with certain provisions include conformance to an applicable industry standard issued by a fair, open, and inclusive standard-setting body, defining the attributes (e.g., participation by public-interest groups, not just industry) that would lead to eligibility. Data providers would need to use standardized formats unless these do not apply (where other procedures are stipulated). The CFPB is otherwise technology/standard-agnostic.

Comment is sought on proposed attributes, with the proposal making clear that data providers could also rely on standards set by government entities. The agency plans to issue standard-setting guidance and also seeks views on how best to do so.

II. Open-Banking Construct

6 See **PRIVACY83**, *Financial Services Management*, November 5, 2007.

A. Data-Provider Obligations

A provider's most recently-updated data would need to be provided to authorized third parties in an electronic format accessible to consumers detailed in the NPR. Consumers could also receive historic data if requested. Comment is sought on whether this requirement should be more clearly set to prevent data-provider evasion.

B. Covered Data

These would include data on any actual, past, or pending transaction, series of transactions (with terms here further defined), balances, costs, terms and conditions, interest rates, upcoming bill information, basic account-verification information, charges, usage data, and information needed to initiate a transaction (including those via ACH). The NPR omits suggestions in the RFI that data would also need to include factors such as consumer demographics. Comment is sought on whether the data fields are clear and flexible enough to handle emerging standards.

C. Exceptions

These would include:

- confidential commercial information, including algorithms but not inputs or outputs to these models;
- information collected to prevent fraud, money laundering, or other unlawful behavior;
- information that must be kept confidential under other laws; and
- information that cannot be retrieved in the orderly course of the provider's business.

D. Data Access

The proposal also sets the terms on which data are provided, along with setting data-access mechanics with particular regard to operational, performance, and security standards. As noted, the proposal would end screen-scraping, instead establishing requirements for developer interfaces.

A "bright-line" ban on fees for providing third-party access is also set, more definitively codifying the "junk fee" advisory on consumer data access noted above and applying them also to consumers request with authorized third parties. This fee prohibition does not bar fees for services related to access (e.g., a subsequent request for an international remittance).

Comment is sought on matters including:

- how to provide human interfaces with natural persons serving as authorized third parties;
- the relationship of these standards to data housed on mobile-banking applications not accessible via online banking;
- whether compliance deadlines should be extended if there are no applicable data standards;
- the extent to which data providers can limit access to problematic developer interfaces;
- the requirement that developers adhere to the privacy standards required of banks;
- the impact of subjecting nonbank data providers to the FTC's safeguards rule;

- the terms on which a data provider may deny access based on security or risk-management considerations. When this is done, it must be "reasonable," with the Bureau seeking comment on how it defines this standard and the role certifications or accreditations may place in provider determinations. The Bureau also encouraged the development of inclusive accreditation standards, describing how this could be done and seeking comment on it; and
- the terms on which a data provider can reject consumer data-access requests.

E. Disclosures

Data providers would need to publish extensive readily-identifiable information about their data-access programs and also provide consumers with disclosures on matters such as the reason why a data-access request was denied and release data on matters such as developer-interface contacts and performance. Comment is sought on these disclosures as well as on the need for additional reporting to the Bureau on matters such as how many requests were addressed through which developer interfaces, compliance with machine- and human-readability standards, and other matters detailed in the proposal's record-retention requirements.

F. Governance

The rule would also require extensive "current", "accurate", and "reasonable" written policies and procedures to ensure compliance and accountability. Additional record-keeping requirements are also specified. Among other things, these procedures and records must demonstrate that data providers substantiate decisions not to honor consumer requests and properly disclose these decisions to affected consumers. Comment is sought on how to make these disclosures.

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