CFPB Releases Final 'Open Banking' Rule on Personal Financial Data Rights

Skadden

December 6, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Ave., NW
Washington, DC 20005
202.371.7000

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) issued a final rule (Rule) on personal financial data rights under Section 1033 of the Dodd-Frank Act.[1] The Rule imposes significant new obligations on financial institutions that maintain consumer account information and affords new rights to consumers, authorized third parties and data aggregators.

The Rule ostensibly seeks to allow consumers to more easily switch financial institutions while maintaining their account history, facilitate comparison shopping by consumers, and better protect data privacy. It may also help resolve some aspects of long-running disputes between banks and data aggregators over security and consumer permission protocols.

The Rule generally mandates that depository institutions and certain other consumer financial services companies provide consumers and authorized third parties with free access to covered consumer personal financial data in a standardized electronic format. It does not establish an exclusive method for data sharing but instead establishes a framework for standard-setting organizations to align on technical standards, which CFPB Director Rohit Chopra indicated will "evolve over time as technology and market needs change."[2] In June 2024, the CFPB issued a final rule outlining the qualifications to become a recognized industry standard-setting organization.[3]

Below we discuss the key requirements under the Rule, including significant changes from the proposed rule, and how we expect the change in administration to impact implementation.

Key Requirements and Features

The personal financial data rights cover consumer data related to Regulation E accounts (*i.e.*, consumer asset accounts such as checking and savings accounts), Regulation Z credit card accounts and payment facilitation arrangements from such accounts (*e.g.*, digital wallets).[4] Differing requirements generally apply to three categories of parties:

- **Data providers**, including financial institutions, card issuers and certain other consumer financial services providers, that must provide access to covered data.
- **Authorized third parties** that obtain the consumer's express informed consent to access covered data from a data provider on behalf of a consumer.
- **Data aggregators** that are retained by and provide services to authorized third parties to facilitate access to covered data.

Data Providers

- **Exemption for small depository institutions**. Depository institutions with assets at or below the Small Business Administration (SBA) size standard are exempt from the Rule. Currently, the SBA threshold for commercial banking is $850 million in assets.

[1] 12 U.S.C. §5533; Required Rulemaking on Personal Financial Data Rights, 89 Fed. Reg. 90,838 (Nov. 18, 2024) (to be codified at 12 C.F.R. Part 1033).

[2] "Prepared Remarks of CFPB Director Rohit Chopra at the Federal Reserve Bank of Philadelphia on the Personal Financial Data Rights Rule" (Oct. 22, 2024).

[3] Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting, 89 Fed. Reg. 49,084 (June 11, 2024).

[4] 12 C.F.R. §1033.111(b).

CFPB Releases Final 'Open Banking' Rule on Personal Financial Data Rights

- **Compliance dates.**
  - April 1, 2026, for depository institutions with at least $250 billion in total assets and nondepository institutions that generated at least $10 billion in total receipts in either 2023 or 2024.
  - April 1, 2027, for depository institutions with total assets between $10 billion and $250 billion, and nondepository institutions that did not generate $10 billion or more in total receipts in both 2023 and 2024.
  - April 1, 2028, for depository institutions with total assets between $3 billion and $10 billion.
  - April 1, 2029, for depository institutions with total assets between $1.5 billion and $3 billion.
  - April 1, 2030, for depository institutions with total assets between $850 million and $1.5 billion.
- **Access to covered data**. Data providers must provide consumers, authorized third parties, and data aggregators with access to "covered data," defined as transaction information, account balance information, payment initiation data, terms and conditions, upcoming bill information and basic account verification information.[5] If tokenized data is provided to initiate a payment and thus made accessible by data providers, this provision of tokenized data cannot be used as a rationale to limit competitive use of payment initiation information. Data providers that do not maintain a consumer's Regulation E account (*e.g.*, certain digital wallets) are not required to provide payment initiation information.
- **Establishment of interfaces**. A data provider must establish a "developer interface" and a "consumer interface" to facilitate data access.[6]
- **No fees**. Data providers cannot impose any fees or charges on a consumer or authorized third party in connection with establishing or maintaining these interfaces or making available covered data in response to requests.[7]
- **Standard-setting process**. The Rule builds on the CFPB's partial finalization in June 2024 of portions of the rule relating to industry standard-setting bodies by outlining a detailed process for those bodies to apply for CFPB recognition.[8] Data providers' adherence to standards established by these recognized bodies, however, serves only as an indicator of compliance with the Rule's format requirement, not full satisfaction of compliance as provided in the proposed rule.[9] The response time for data provider developer interfaces must conform with a consensus standard set by a recognized body.[10]
- **Screen scraping**. The Rule does not expressly prohibit screen scraping, an access method that uses consumer credentials to log in to consumer accounts to retrieve data, despite many industry commenters seeking a ban of the practice. A data provider cannot satisfy the requirement to make data available to authorized third parties by merely allowing the third party to engage in screen scraping. A data provider may satisfy its obligation to maintain the required data access, however, by outsourcing its provision of covered data to a service provider — *i.e.*, by entering into a contract whereby the service provider (*e.g.*, a core processor) screen scrapes covered data from the data provider's consumer interface and makes the covered data available to authorized third parties through a developer interface that the service provider maintains on behalf of the data provider. The CFPB explained that it believes this "self-scraping" approach will reduce the burden of the developer interface requirement through economies of scale.[11]
- **Reasons to deny interface access**. A data provider can deny access if it would conflict with policies and procedures that are reasonably designed to comply with (i) safety and soundness standards of a prudential regulator, (ii) information security requirements under the Gramm-Leach-Bliley Act, or (iii) other relevant laws and regulations related to risk management. Such a denial is considered reasonable if it directly addresses a specific known risk and is applied consistently and without discrimination.[12] The CFPB recognized that data providers have risk management obligations that mandate the protection of consumer data. In response to comments asking for the ability to deny data access based on guidance from prudential regulators, the agency decided that denials must be based on binding legal requirements. When evaluating whether a data provider's policies and procedures are "reasonably designed" to justify a denial of access, the CFPB will assess whether the provider has balanced the need to comply with risk management laws with the goal of minimizing the burden on consumers' access rights under Section 1033. Policies will not be considered "reasonably designed" if they do not explore alternative, less burdensome practices that would still effectively meet legal requirements.[13]

[5] 12 C.F.R. §§1033.201(a), 1033.211.

[6] 12 C.F.R. §1033.301(a).

[7] 12 C.F.R. §1033.301(c).

[8] Appendix A to Part 1033.

[9] 12 C.F.R. §1033.311(b).

[10] 12 C.F.R. §1033.311(c)(1)(iv)(C).

[11] *Id.* at 7, 161-165, 213-215.

[12] 12 C.F.R. §1033.321(a).

[13] Rule, *supra note* 1, at 90,898.

CFPB Releases Final 'Open Banking' Rule on Personal Financial Data Rights

Authorized Third Parties

- **Authorization disclosure**. To become an authorized third party, the third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested.[14] The third party must provide the consumer with an authorization disclosure that conforms to specific content requirements and obtain an authorization disclosure signed by the consumer that represents the consumer's express informed consent to access covered data.[15] The authorization disclosures that third parties provide to consumers must be clear, conspicuous and segregated from other material. They must include a brief description of the data collection duration, along with a statement confirming that the collection will not extend beyond one year after the consumer's most recent authorization.[16]
- **Collection, use and retention of consumer data**. An authorized third party must certify that it will limit the collection, use, and retention of covered data to what is reasonably necessary to provide the product or service requested by the consumer. The Rule does not allow authorized third parties to use de-identified data for purposes that are not reasonably necessary to provide the consumer's requested product or service. The Rule, therefore, limits the availability of covered data for marketing and for the development of new products outside the scope of the original authorization, which may restrict innovation by third parties using de-identified data to train artificial intelligence (AI) models to develop new products and services. The Rule does not prohibit authorized third parties from using de-identified data as reasonably necessary to provide the consumer's requested product or service, or from seeking a separate authorization to use de-identified data for other purposes that the consumer may choose.[17] The Rule clarifies that an authorized third party may use a consumer's covered data as necessary to enhance the product or service requested by the consumer.[18]
- **Lapse or revocation of authorization**. The CFPB explained that the goal of the authorized third party certification is to ensure that third parties access covered data solely for the benefit of the consumer, allowing consumers to retain control over their data when authorizing third party access. If a consumer does not provide a new authorization within one year of the most recent authorization, or if a consumer revokes authorization, the third party immediately must cease its collection, use and retention of covered data unless use or retention of that data remains reasonably necessary to provide the consumer's requested product or service. Specific circumstances may justify continued use or retention of some or all previously collected covered data, including the involuntary collection of more data than reasonably necessary, or the practical infeasibility of extracting de-identified data from models. Authorized third parties, particularly those using covered data for AI training purposes, will need to implement technical capabilities to identify and manage consumers' covered data in a manner similar to what is currently required to comply with the California Consumer Privacy Act and the European Union's General Data Protection Regulation.[19]

Data Aggregators

- **Responsibility for compliance.** Data aggregators may perform the authorization procedures on behalf of the third party seeking authorization, but the third party remains responsible for compliance.
- **Authorization disclosure and certificatio**n. If a data aggregator is used, the name of the data aggregator must be included in the authorization disclosure, and the data aggregator must certify to the consumer, either as part of the authorized third party's disclosure or separately, that it will comply with the Rule's data access conditions and restrictions.

CFPB Goals and Industry Challenge

The stated goal of the Rule is to strengthen consumers' control over their financial data and foster competition in the financial services sector by giving consumers "greater rights, privacy, and security over their personal data," increasing portability of consumer information, and allowing consumers to more easily switch providers and gain access to new products.[20] Fintech trade groups and consumer advocates have generally responded positively to the Rule, while banking trade groups have argued that the CFPB overstepped its authority and ignored their concerns.[21] Some banking trade groups have already challenged the Rule on the grounds that it jeopardizes consumers' privacy, financial data and account security.[22]

[14] 12 C.F.R. §401.

[15] *Id.*

[16] 12 C.F.R. §1033.411(b)(6).

[17] *Id.* at 90,941.

[18] 12 C.F.R. §1033.421(c)(4).

[19] *Id.* at 90,839, 90,930-2, 90, 942, 90,950, 90,973.

[20] Press Release, CFPB, CFPB Finalizes Personal Financial Data Rights Rule to Boost Competition, Protect Privacy, and Give Families More Choice in Financial Services (Oct. 22, 2024).

[21] *See, e.g.*, Press Release, American Bankers Association, ABA Statement on CFPB's Section 1033 Final Rule (Oct. 22, 2024). The American Bankers Association has characterized the Rule as "based on the false premise that consumers lack choices and a misunderstanding of whether Dodd-Frank grants CFPB the authority to radically reshape the financial services marketplace" and noted that "longstanding concerns about scope, liability, and cost remain largely unaddressed."

[22] *See* Complaint, *Forcht Bank et al. v. Consumer Fin. Prot. Bureau*, No. 5:24-cv-00304 (E.D. Ky. Oct. 22, 2024).

CFPB Releases Final 'Open Banking' Rule on Personal Financial Data Rights

The Supreme Court's decision in *Loper Bright* has unquestionably altered the legal landscape in favor of challenges to agency action. The Bank Policy Institute, Kentucky Bankers Association and a Kentucky bank filed suit seeking declaratory and injunctive relief in the United States District Court for the Eastern District of Kentucky.[23] The complaint asserts six claims under the Administrative Procedure Act, including that the Rule misinterprets the term "consumer" in Title X of the Dodd-Frank Act, unacceptably puts consumer data at risk, unlawfully demands the sharing of information necessary to initiate a payment, impermissibly delegates decision-making authority to a private actor, includes unreasonable compliance deadlines, and bans financial institutions from charging reasonable access fees to third parties or data aggregators to access data.[24]

If the challenge is successful, the court could set aside the Rule in its entirety or permanently enjoin enforcement of the Rule against the plaintiffs. The court also could delay the effective date and implementation of the Rule pending the conclusion of the case.[25]

Post-Election Possibilities

Under the incoming Trump administration, the CFPB director is subject to removal at will, so the CFPB's stated priorities are likely to change. But while the CFPB under the Trump administration is broadly expected to be more industry-friendly and will be able to invalidate later Biden administration rules under the Congressional Review Act, reactions to the Rule have not tracked partisan lines. In fact, the chairman of the House Financial Services Committee, Patrick McHenry (R-N.C.), called the Rule "a promising step forward to protect Americans' financial data privacy" and stated that "[a]s Republicans have said for years, Americans should have greater control over their sensitive financial data."[26] During the rulemaking process, Vice Chairman French Hill (R-Ark.), a candidate to replace the retiring committee chairman, indicated that it was important "to make sure we get this right" and noted that "[t]his is something on which the committee wants to collaborate."[27]

The most likely outcome is therefore that the CFPB makes changes to the Rule without rolling it back entirely. Some potential changes to the Rule may include:

- **Formal ban on screen scraping**. Trade groups such as the Bank Policy Institute and The Clearing House Association have called for a prohibition on screen scraping once a data provider has made a developer interface available.[28]
- **Liability allocation for data security breaches**. Trade groups have asked for more clearly defined liability. The Bank Policy Institute and The Clearing House Association have pushed for aggregators and authorized third parties to be liable for unauthorized transactions or failing to protect consumer data once data is within their possession.[29] After the CFPB issued the proposed rule, House committee Vice Chairman Hill questioned CFPB Director Chopra on liability allocation for data security breaches, which suggests that this topic is likely to be revisited.[30]
- **Relief on compliance deadlines**. The Bank Policy Institute has criticized the Rule's compliance deadlines for not aligning with the promulgation of consensus standards issued by standard-setting bodies.[31]
- **Reasonable access fees**. Banking trade groups have requested that the CFPB allow data providers to charge reasonable access fees to defray infrastructure costs and deter unnecessary requests for access,[32] though the introduction of fees would face strong opposition from consumer advocates and fintech trade groups. Such fees would also be in tension with the CFPB's Advisory Opinion issued in October 2023 on Section 1034(c) of the Dodd-Frank Act, which requires large banks and credit unions to comply in a timely manner with consumer requests for account information. The Advisory Opinion states that "requiring a consumer to pay a fee or charge to request account information, through whichever channels the bank uses to provide information to consumers, is likely to unreasonably impede consumers' ability to exercise the right granted by section 1034(c), and thus to violate the provision" because "fees can operate as a significant deterrent to making an information request."[33]

Significant changes would likely delay the Rule's implementation.

[23] *Id.*

[24] *Id.* at 41-52.

[25] *Id.* at 52-54.

[26] Press Release, House Financial Services Committee, McHenry Statement on CFPB's Final 1033 Rule (Oct. 22, 2024).

[27] The Semi-Annual Report of the Bureau of Consumer Financial Protection: Hearing Before the H. Comm. on Financial Services, 118th Cong. 11 (June 14, 2023).

[28] Press Release, The Clearing House, BPI and TCH Call for Stronger Consumer Financial Data Rules for Aggregators and Big Tech (Jan. 1, 2024).

[29] *Id.*

[30] The Semi-Annual Report of the Bureau of Consumer Financial Protection: Hearing Before the H. Comm. on Financial Services, 118th Cong. 9-10 (Nov. 29, 2023).

[31] Press Release, Bank Policy Institute, Banks Challenge CFPB Rule Jeopardizing Security and Privacy of Consumer Financial Data (Oct. 22, 2024).

[32] Press Release, The Clearing House, BPI and TCH Call for Stronger Consumer Financial Data Rules for Aggregators and Big Tech (Jan. 1, 2024).

[33] CFPB, Consumer Information Requests to Large Banks and Credit Unions, at 10.

CFPB Releases Final 'Open Banking' Rule on Personal Financial Data Rights

Next Steps and Takeaways

Companies covered by the Rule — including data providers, authorized third parties and data aggregators — should consider evaluating their data infrastructure, security measures, and compliance processes to assess necessary steps for adopting processes compliant with the Rule. While compliance deadlines appear distant, the CFPB has not yet recognized a setting body, posing challenges for data providers looking to align with standards that do not yet exist. Likewise, third parties seeking to access covered data would be well-advised to assess their data collection, usage and retention policies to ensure compliance with the Rule's purpose limitations and consent requirements.

We will continue to monitor this area as ongoing legal challenges could affect the Rule's implementation and enforcement.

Contacts

Adam J. Cohen
Partner / Washington, D.C.
202.371.7510
adam.cohen@skadden.com

Mark Chorazak
Partner / New York
212.735.3488
mark.chorazak@skadden.com

Darren M. Welch
Partner / Washington, D.C.
202.371.7804
darren.welch@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Nate Balk
Associate / Washington, D.C.
202.371.7295
nate.balk@skadden.com

Melissa L. Dorow
Law Clerk / Washington, D.C.
202.371.7256
melissa.dorow@skadden.com