Unpacking The CFPB's Personal Financial Data Final Rule

By **Joel Feinberg, David Teitelbaum and Thomas Ward** (November 19, 2024)

Joel Feinberg

David Teitelbaum

Thomas Ward

On Oct. 22, the Consumer Financial Protection Bureau issued a final rule under Section 1033 of the Consumer Financial Protection Act.[1]

Of note, the final rule includes several important changes from the proposed rule. This analysis focuses on those changes. The final rule also includes hundreds of pages of supplementary information that provide important insights into the manner in which the CFPB will enforce the final rule.

The final rule generally requires depository institutions and certain other companies to make several pieces of a consumer's personal financial data available for free to the consumer and third parties that act with authorization from the consumer. It does not, however, set forth an exclusive means of data sharing by data providers, provided that sharing consistent with the requirements of the rule is also enabled.

The type of information that is within the scope of the final rule relates to asset accounts from which a consumer may initiate electronic fund transfers, e.g., a bank checking account, credit card accounts, and arrangements for the facilitation of payments from such accounts, e.g., digital wallets.

It refers to three types of parties: data providers, authorized third parties and data aggregators. In simple terms, these are respectively the parties that must provide access to the data, that seek access to the data and that transmit the data between the first two parties.

According to the CFPB, this rule "will give consumers greater rights, privacy, and security over their personal financial data" and "moves the United States closer to having a competitive, safe, secure, and reliable 'open banking' system."[2] It remains controversial within the industry, however, and the CFPB has already been sued by banking trade groups — in the case of Forcht Bank v. CFPB in October in the U.S. District Court for the Eastern District of Kentucky — in an effort to block its enforcement.

The following are the key changes from the proposed rule. The compliance dates have been extended.

For depository institution data providers that hold at least $250 billion in total assets and nondepository institution data providers that generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024, the compliance date is April 1, 2026.

For data providers that are depository institutions that hold at least $10 billion in total assets but less than $250 billion in total assets or nondepository institutions that did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024, the compliance date is April 1, 2027.

For depository institution data providers that hold at least $3 billion in total assets but less than $10 billion in total assets, the compliance date is April 1, 2028.

For depository institution data providers that hold at least $1.5 billion in total assets but less than $3 billion in total assets, the compliance date is April 1, 2029.

Lastly, for depository institution data providers that hold less than $1.5 billion in total assets but more than $850 million in total assets, the compliance date is April 1, 2030.[3]

Data providers with assets equal to or less than the Small Business Administration size standard are exempt from the final rule. The current Small Business Administration size standard for commercial banking is $850 million in assets.[4]

Data providers are expressly prohibited, under the final rule, from taking actions to evade the rule's requirements.[5]

The final rule clarifies that if tokenized data — a type of data that data providers must make available for access — is provided as information to initiate a payment, its provision may not be "used as a pretext to restrict competitive use of payment initiation information."[6]

It also clarifies that data providers that do not hold the consumer's asset account, for instance certain types of digital wallets, are not obligated to make available payment initiation information.[7]

In addition, data provider conformity to a developer interface standardized format established as a consensus standard by a CFPB-recognized standard-setting body is indicia of compliance with the final rule's standardized format requirement.[8] In the proposed rule, it was evidence of compliance rather than mere indicia of compliance.

The final rule has changed the required data provider developer interface response time from no more than 3,500 milliseconds to "conformance with an applicable consensus standard" established by a CFPB-recognized standard-setting body.[9]

It also revises and slightly expands the bases upon which a data provider may deny access to an authorized third party or data aggregator.

Access may be denied if granting access would be inconsistent with policies and procedures reasonably designed to comply with safety and soundness standards of a prudential regulator, Gramm-Leach-Bliley Act information security standards, or other applicable laws and regulations regarding risk management. A denial based on those standards is reasonable if it is directly related to a specific risk of which the data provider is aware and is applied in a consistent and nondiscriminatory manner.[10]

Authorization disclosures presented to consumers by authorized third parties must include a statement that the authorized third party will collect, use and retain the consumer's covered data "only as reasonably necessary to provide" the requested product or service.[11] The proposed rule used the phrase "only for the purpose of providing."

The final rule has added a requirement to the authorization disclosures that it provide a brief description of the duration of data collection and a statement that collection will not last longer than one year after the consumer's most recent authorization.[12]

Finally, the final rule clarifies that an authorized third party may use a consumer's data as

"reasonably necessary to improve the product or service the consumer requested" from the authorized third party.[13] An appendix to the rule provides instructions for how a standard-setting organization may apply for CFPB recognition.[14]

Practitioners and industry participants should be aware that the CFPB's final rule cannot be read in isolation.

Rather, the lengthy supplementary information provides important interpretive guidance on topics including access denial standards; access agreement provisions, which are significantly constrained; screen scraping, which is not prohibited under the final rule; Fair Credit Reporting Act compliance; and secondary uses of consumer data.

Indeed, the supplementary information is so detailed and extensive in its elaboration on the content of the final rule that it is not possible to fully understand the rule without also consulting the supplementary information.

This rulemaking has been long in coming. The CFPB is seeking to give consumers greater rights, privacy and security over their personal financial data while at the same time allowing the U.S. to maintain a competitive, safe, secure and reliable banking system. We will know in the coming years whether that balance has been struck.

Joel Feinberg is a partner, co-leader of the banking and financial services practice, and head of the financial institutions group in Washington, D.C., at Sidley Austin LLP.

David Teitelbaum is a partner and leader of the fintech practice area team at the firm.

Thomas Ward is a partner at the firm. He previously served as the CFPB's enforcement director.

Sidley counsel Stanley Boris contributed to this article.

[1] https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/.

[2] https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/.

[3] § 1033.121.

[4] § 1033.111(d).

[5] § 1033.201(a)(2).

[6] § 1033.211(c)(1).

[7] § 1033.211(c)(2).

[8] § 1033.311(b).

[9] § 1033.311(c)(1)(iv)(C).

[10] § 1033.321(a).

[11] § 1033.411(b)(3).

[12] § 1033.411(b)(6).

[13] § 1033.421(c)(4).

[14] Appendix A to Part 1033.