Cooley

CFPB Finalizes Section 1033 Rule on Personal Financial Data Rights

October 31, 2024

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) released its long-awaited final rule implementing Section 1033 of the Consumer Financial Protection Act (CFPA) concerning personal financial data rights. The final rule largely tracks the CFPB's October 2023 proposal, although the CFPB did make material changes, for example, with respect to the entities covered and the types of data that must be shared under the rule, as well as the deadlines for compliance with the final rule.

Mere hours after the CFPB issued the final rule, a group of industry participants filed a lawsuit challenging its validity, creating uncertainty with respect to both the rule's scope and ultimate timeline for implementation.

Who is covered and what is required under the final rule?

The final rule governs the practices of data providers, third parties authorized to access consumer data and data aggregators.

Data providers subject to the rule

A "data provider" generally includes any "covered person" under the CFPA that controls or possesses information concerning a "covered consumer financial product or service," which means one of the following:

- Regulation E accounts.
- Regulation Z credit cards.
- The facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first-party payments (transfers initiated by the payee or an agent acting on behalf of the underlying payee, including payments initiated by loan servicers).

Importantly, digital wallet providers are considered data providers subject to the rule, but institutions maintaining electronic benefit(s) transfer (EBT) accounts, for now, are not.

Data required to be provided

Under the final rule, data providers are obligated to provide consumers and authorized third parties with access to "covered data," which includes:

- Transaction information.
- Account balances.
- Information required to initiate a payment to or from an account subject to Regulation E, which can be provided as a tokenized account number (TAN).
- Terms and conditions.
- Upcoming bill information.
- Other basic account verification information.

However, data providers are **not** required to provide access to:

- Confidential commercial information, including algorithms that may be used to derive credit scores or other risk scores or

predictors.
- Information collected for the sole purpose of preventing fraud or money laundering or detecting or reporting other unlawful conduct.
- Information required to be kept confidential by any other provision of law.
- Information that it cannot retrieve in the ordinary course of its business.

Means through which data must be made available

Under the final rule, data providers are required to establish and maintain consumer and developer interfaces to facilitate consumer and third-party access to covered data in a standardized and machine-readable format.

In addition, developer interfaces must:

- Meet specific performance standards.
- Apply an information security program that satisfies the Gramm-Leach-Bliley Act (GLBA) or, if not subject to the GLBA, the Federal Trade Commission (FTC) Safeguards Rule.

Importantly, data providers cannot satisfy their developer interface obligations by merely allowing a third party to engage in "screen scraping," an access method prevalent in the market that uses consumer credentials to log in to consumer accounts to retrieve data.

The final rule also prohibits data providers from interfering with access to consumer data, rendering shared data unusable, discouraging the consumer or an authorized third party from accessing covered data, and charging fees for consumers or authorized third parties to access covered data.

Third-party collection, use and retention of covered data

Under the final rule, in order to access a consumer's covered data, a third party must:

- Provide the consumer with a comprehensive authorization disclosure that:
  - Certifies to the consumer (within the authorization disclosure) that the third party agrees to limit the collection, use and retention of covered data.
  - Obtains the consumer's "express informed consent" signed by the consumer electronically or in writing.
  - Certifies that the entity will limit the duration of the collection of covered data to a maximum of one year.
- Provide the consumer with a method to revoke their authorization that is as easy to access and operate as the initial authorization.

An authorized third party must obtain the authorization to collect data at least once every 12 months. Third parties that fail to obtain the consumer's affirmative reauthorization are prohibited from continuing to collect the consumer's covered data. However, authorized parties are permitted to continue to use covered data beyond one year and without reauthorization for:

- Uses that are specifically required under other provisions of law.
- Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability.
- Servicing or processing the product or service that the consumer requested.
- Uses that are reasonably necessary to improve the product or service that the consumer requested.

In addition to obtaining proper authorization, third parties seeking to access consumer data must:

- Establish and maintain written policies and procedures reasonably designed to ensure that covered data is accurately received from a data provider and accurately provided to another party.
- Apply an information security program to their collection, use, and retention of covered data, which satisfies the GLBA or, if the third party is not subject to the GLBA, the FTC's Safeguards Rule.
- Only collect, use and retain data as reasonably necessary to provide the consumer with the requested product or service.

With respect to the "reasonably necessary" standard, the CFPB is effectively prohibiting third parties from using

covered data obtained from a data provider for targeted advertising, cross-selling products and services, or selling consumer data absent separate authorization from the consumer. In commentary accompanying the final rule, the CFPB also takes an expansive view of what constitutes the "sale" of data, aligning closely to the controversial definition of "sale" under the California Consumer Privacy Act, which defines data sales as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information for monetary or **other valuable consideration**" (emphasis added).

Use of data aggregators

Authorized third parties may use a "data aggregator" to access covered data if:

- The authorization disclosure, which, as referenced above, must be presented by a third party to the consumer to facilitate the third party's access to covered data, identifies the data aggregator.
- The data aggregator certifies to the consumer – either as part of the authorized third party's disclosure or separately – that they agree to comply with the final rule's data access conditions and restrictions.

The authorized third party, however, is ultimately responsible for compliance with the final rule's authorization procedures.

Consensus standards

The final rule reflects that compliance with several of its requirements will be assessed using "consensus standards" established by "standard-setting" bodies that are formally recognized by the CFPB.

Together, this final rule and the industry standard-setting rule finalized in June 2024 identify the attributes that entities must have in order to receive CFPB recognition as a "standard-setting" body, as well as the steps entities must take to receive such recognition.

The CFPB has published two applications of organizations seeking recognition by the CFPB as a standard-setting body, but to date, no entity has been formally recognized as such.

What are the compliance deadlines?

The CFPB's final rule establishes five compliance deadlines for data providers based on asset size, as outlined in the table below.

Compliance deadline	Asset size
April 1, 2026	For depository institutions that hold 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 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** 2023 and 2024.
April 1, 2028	For depository institutions that hold at least $3 billion in total assets but less than $10 billion in total assets.
April 1, 2029	For depository institutions that hold at least $1.5 billion in total assets but less than $3 billion in total assets.
April 1, 2030	For depository institutions that hold less than $1.5 billion in total assets but more than $850 million in total assets.

Depository institutions with less than the size standard set by the US Small Business Administration (SBA), presently $850 million in assets, are excluded from the aspects of the rule that require data providers to make covered data available by providing interfaces and responding to requests for consumer data. This is a notable departure from the proposed rule, which instead would have exempted entities if they did not have a consumer-facing interface.

What's next?

Although the final rule is scheduled to take effect 60 days after publication in the Federal Register, the lawsuit challenging the rule under the Administrative Procedures Act makes its fate uncertain. The plaintiffs in that suit contend that in issuing the final rule, the CFPB:

- Exceeded its authority by requiring banks to broadly provide their customers' financial information to "authorized" third parties.
- Designed the rule in a way that increases security risks to consumer information.
- Inappropriately gave authority to third parties to set compliance standards.
- Unreasonably prohibited data providers from charging reasonable access fees to third parties or data aggregators.
- Incorporated unreasonable deadlines for compliance, in particular given that the third parties who will be responsible for setting compliance (or consensus) standards – and, thus, those compliance standards – have not yet been determined.

The final rule reflects the broader trend, globally and domestically, of requiring companies to provide individuals with increased control over their data, including through data portability. While this final rule represents a marker in the domestic move toward data portability, the pending litigation, the need to designate third parties to set compliance standards, and even the upcoming US election, leave open key implementation questions that will only be resolved with the passage of time.

Register now to join Cooley's financial services and cyber/data/privacy teams on Thursday, November 7, 2024, at 1:00 pm EST for a one-hour webinar discussing the final rule and its potential impacts on your business.

Key Contacts

Michelle L. Rogers **Washington, DC**	**mrogers@cooley.com** **+1 202 776 2227**
Obrea Poindexter Washington, DC	opoindexter@cooley.com +1 202 776 2997
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249