HINSHAW

# CFPB Finalizes Open Banking Rule to Boost Competition, Protect Privacy, and Enhance Consumer Choice

**Privacy, Cyber & AI Decoded Alert | 6 min read**
Dec 3, 2024

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) issued its long-awaited Final Rule implementing Section 1033 of the Dodd-Frank Act ("Final Rule") with the intention of giving consumers greater rights, privacy, and security over their financial data.

Under the Open Banking Rule, consumers will be able to access their financial data and authorize third parties to do the same on their behalf, making it easier for them to shop around and switch financial service providers. The Final Rule is anticipated to stimulate competition, enhance consumer choice, lower loan costs, and improve customer service across payments, credit, and banking markets.

For covered entities, the Final Rule will not come without compliance burdens, both technical and operational in scope. This generally translates to increased compliance costs as well. However, the Rule's fate is uncertain and has garnered the attention of detractors who have voiced concern about the Rule's unintended consequences. Continue reading to explore the key aspects of the Final Rule and discover what people are saying.

## What is Section 1033 of the Dodd-Frank Act?

Section 1033 of the Dodd-Frank Act gives consumers the right to access and share their financial data. Section 1033 requires financial services providers to make certain information they control available to consumers. This can include information like a consumer's transactions or the balance in their financial account.

**Finalizing the Rule was a lengthy process due to several factors, including:**

- extensive public comment periods,
- industry pushback,
- concerns about data security and privacy,
- the need to carefully balance consumer protections with market innovation, and

- legal challenges from industry groups who questioned the CFPB's authority to implement such a rule.

All of these factors led to a lengthy process of revisions and adjustments to the proposed Rule before finalizing it.

# Who is Required to Comply with the Final Rule?

The Final Rule imposes obligations and restrictions on data providers, authorized third parties, and data aggregators.

**Who are Data Providers?**

- Data providers include account-holding financial institutions, credit card issuers, digital wallet providers, and almost any other entity that controls or possesses information concerning a covered consumer's financial product or service (*e.g.*, Regulation E accounts, Regulation Z credit cards, and certain payment facilitators) that the entity provides to the consumer.
- As a result, certain fintech payment platforms and wallet providers will also be subject to the data provider requirements. Small depository institutions with less than $850 million in assets will be exempt. It should also be noted that if permitted, the CFPB will likely continue with further rule-making.

**Who are Authorized Third Parties?**

- A third party is defined as "any person that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data."
- Third parties become authorized after providing the consumer with an authorization disclosure (outlining how their data will be collected, used, and retained) and by obtaining the consumer's express informed consent, thereby permitting them to access covered data on the consumer's behalf in order "to provide a product or service the customer requested."

**Who are Data Aggregators?**

- Data aggregators are entities retained by authorized third parties as service providers to assist consumers with accessing covered data.

# What is "Covered Data" Under the Final Rule?

**Covered data includes the following:**

- Transaction information;
- Account balance information;
- Terms and conditions;
- Payment initiation information;

- Upcoming bill information; and
- Basic account verification information.

**Exceptions apply. For example, data providers are not required to make the following available:**

- Confidential commercial information;
- Information collected for the sole purpose of preventing fraud, money laundering, or other unlawful conduct; and
- Information required to be kept confidential by any other law.

# What Obligations do Covered Entities Have Under the Final Rule?

**What Must Data Providers Do to Comply?**

- Maintain consumer interfaces (which allow consumers to access their data) and establish developer interfaces (which allow third parties to access consumer data) through which the data provider receives and responds to requests from authorized third parties.
- Provide data in a machine-readable format containing covered data suitable for loading into a consumer or authorized third party's own systems. Data providers must also publicly disclose information about themselves to facilitate access to covered data, promote accountability, and retain records of their compliance efforts for up to three years.
- The Final Rule also prohibits screen scraping as a method of granting data access to third parties and charging fees to access interfaces.

**What Must Third Parties Do?**

- To become authorized, third parties must obtain a consumer's "express informed consent," which provides:
  - the name of the third party and the data provider;
  - the identity of the data aggregator, if one is used;
  - a description of the service provided and the categories of data that will be accessed;
  - a certification that the third party will comply with specific obligations related to use, retention, access, accuracy, and security; and
  - a description of the revocation process.

- To that end, third parties may only use and retain covered data in a manner that is reasonably necessary to provide the requested product or service, and they must:
  - maintain policies and procedures to ensure the accurate communication of data;
  - maintain an information security program that satisfies the Gramm-Leach-Bliley Act (GLBA) or the Federal Trade Commission's (FTC) Safeguards Rule;

- ensure that the consumer is informed about the status of their authorization; and
- provide a method by which the consumer can easily revoke third-party access.

**What Must Data Aggregators Do?**

- Agree to comply with the Final Rule's data access conditions and restrictions. Notably, the third party remains responsible for compliance with the Final Rule.

## What are the Compliance Deadlines Under the Final Rule?

**For Depository Institutions:**

- **April 1, 2026:** Holds at least $250 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions;
- **April 1, 2027:** Holds at least $10 billion in total assets but less than $250 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions;
- **April 1, 2028:** Holds at least $3 billion in total assets but less than $10 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions;
- **April 1, 2029:** Holds at least $1.5 billion in total assets but less than $3 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions; and
- **April 1, 2030:** Holds less than $1.5 billion in total assets but more than $850 million in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions.

**For Non-depository Institutions:**

- **April 1, 2026:** Generated at least $10 billion in total receipts in calendar year 2023 or calendar year 2024; and
- **April 1, 2027:** Did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024.

## What Are Fintech Organizations and Others Saying About the Final Rule?

The CFPB believes that implementing the Final Rule will not only close privacy gaps but also spur competition and innovation, thereby benefiting consumers and, ultimately, the entire ecosystem.

However, as indicated above, the Final Rule is not without its detractors. Indeed, on the same day the Rule was announced, two trade groups filed a suit alleging, among other things, that not only did the CFPB exceed its authority in issuing the Rule, but its implementation would increase security risks to consumers.

Meanwhile, fintech organizations and others have raised concerns that:

- many consumers lack financial literacy and/or an understanding of data security, making them vulnerable to exploitation;
- the consent and revocation process is too complicated, and consumers will not be up to the challenge of keeping track of those processes;
- many consumers are still unaware of how their data is used once shared; and
- consumers lack the resources to track and resolve data breach issues and will not know how to manage things like identity restoration or credit monitoring.

Of course, these concerns may all be for naught once U.S. President-elect Donald Trump returns to office. Not only will the incoming Trump Administration likely replace key leadership at the CFPB, but it is equally likely that they will try to curtail the agency's rulemaking activity.

Regardless of your or your organization's stance on the Final Rule, it is important to note that it is slated to go into effect on **January 17, 2025**, just a few days before the presidential inauguration.

---

*Legal intern Elyssa Eisenberg contributed to this post. She is not currently admitted to practice law.*

## Related People

**Jason J. Oliveri**

Partner

**212-471-6237**

**Claire Standish**

Associate

**212-655-3842**

## Related Capabilities

Consumer Financial Services

Data Privacy, AI & Cybersecurity

Financial Services

# Subscribe to receive timely legal insights directly in your inbox.