OpenFinity Oct 28, 2024 4 min read

CFPB Section 1033 Series: Final Rule -Key Takeaways

Updated: Dec 2, 2024

The wait is over! It has been four years since the Consumer Financial Protection Bureau announced its plans to explore the implementation of Section 1033 of the Dodd-Frank Act—more commonly known as open banking.

On Tuesday, October 22, 2024, the Consumer Financial Protection Bureau (CFPB) published its final rule[1], a nearly 600-page regulation highly anticipated by the U.S. financial industry to bring the country on par with global counterparts.

CFPB 1033 Overview

The final CFPB Section 1033 rule establishes robust standards and consumer rights around open banking in the U.S., providing a unified regulatory framework designed to protect consumer data and foster innovation. This rule requires banks to securely share consumer financial data across a broad

spectrum of financial products, including payment apps and mobile wallets (like PayPal, Zelle, and Venmo). The intent is to promote consumer choice, enhance financial inclusion, and mitigate risks associated with outdated data-sharing practices like screen scraping by encouraging secure APIs.

The rule clarifies that when consumers authorize third-party access to their financial data, those third parties operate independently on behalf of the consumer, not as the banks' service providers. This limits banks' discretion to deny data-sharing requests based on risk management considerations. Compliance requirements, such as strong data security standards under the Gramm-Leach-Bliley Act, apply to all institutions handling consumer data, while prohibitions on data harvesting ensure third-party data use aligns strictly with the consumer's needs.

The rule also allows limited secondary uses of data, such as improving the consumer-requested service, but prohibits data retention for purposes like targeted advertising. Additional flexibility in performance targets, such as response time for data requests, acknowledges industry feedback, while tokenization and enhanced consumer control over data (with the right to revoke access) add safeguards.

By banning banks from charging fees for data sharing and enforcing clear privacy standards, the CFPB aligns the U.S. with global open banking practices seen in the U.K., EU, and Australia. With tiered compliance deadlines extending to 2030 for smaller institutions, the rule emphasizes a phased, inclusive approach, particularly for smaller banks and credit unions. Section 1033 is expected to level the competitive landscape, empowering community banks, fintechs, and consumers, and potentially reshaping U.S. banking practices toward a more digital, secure, and consumer-focused model.

> **"The final rule makes clear that when consumers authorize companies to obtain their personal financial data on their behalf, these companies are not acting as service providers to the financial institutions holding the consumer's data — those companies are acting on behalf of the consumer," said CFPB Director Rohit Chopra.**

9 Key Takeaways

1. **Broad Scope of Data Sharing**

   The rule mandates secure data sharing for various financial products, including checking accounts, credit cards, mobile wallets, and payment apps (e.g., PayPal, Venmo, Zelle). This inclusion reflects the growing role of third-party apps in banking and payments.

2. **Consumer-Centric Data Rights**

   Consumers gain strong data rights, including transparency over what data is collected, where it's stored, with whom it's shared, and the ability to revoke access at any time. When access is revoked, data access must end immediately, and the data must be deleted.

3. **Prohibition on Data Harvesting**

   Third parties can use consumer data only for the purpose intended by the consumer. Practices like targeted advertising, cross-selling, or unrelated business uses are banned, ensuring consumer data is used only to fulfill the service requested.

4. **Limited Secondary Data Uses Allowed**

   Third parties are permitted some secondary uses of consumer data, such as improving services (e.g., training underwriting models or developing anti-fraud tools) without needing separate authorization from consumers.

5. **Secure API Standards to Replace Screen Scraping**

   The rule encourages the transition from screen scraping to secure APIs (but does not mandate its removal, (a departure from the CFPB's previous positions), improving data accuracy, security, and consumer control. The Financial Data Exchange (FDX) has applied to set the industry standard, which would further unify data formatting and security protocols.

6. **Enhanced Data Security and Compliance Obligations**

   All entities accessing consumer data, not just banks, must comply with data security standards under the Gramm-Leach-Bliley Act. This requirement promotes a consistent level of data protection across the financial ecosystem.

7. **Ban on Charging Fees for Data Access**

   Similar to international open banking frameworks, the rule prohibits banks from charging consumers for accessing their data, aligning U.S. practices with global standards.

8. **Lack of Clarity and Potential Conflicts with other Reg**

   Some areas of 1033 remain unclear or subject to interpretations. For instance, consumers can authorize third-party providers to access their financial data. This data may pass through aggregators, banks, and fintechs, creating a multi-layered chain where data could be mishandled, misused, or accessed by unauthorized parties. If a data breach or unauthorized transaction occurs, it may be unclear who bears responsibility.

   Will there be a safe harbor provision for banks following all compliance measures?

   1033 may as well intersect with other regulations such as REG E, particularly around issues of consumer rights, liability, and error resolution in electronic transactions.

   The rule may benefit from further guidance or amendments clarifying specific liability boundaries and outlining safe harbor protections for data providers that comply with all prescribed security and consent measures.

9. **Phased Compliance Deadlines**

   Compliance deadlines are staggered by institution size, with the largest banks required to comply by April 1, 2026, and the smallest institutions given until April 1, 2030. Only banks and credit unions with assets over $850 million are subject to the rule.

   Compliance Deadlines:

Compliance Criteria	Compliance Deadlines
Depository institutions with $250B in total assets; and non-depository institutions with at least $10B in total receipts	**APRIL 1, 2026**
Depository institutions with $10B-$250B in total assets; and non-depository institutions with less than $10B in total receipts	**APRIL 1, 2027**
Depository institutions with $3B-$10B in total assets	**APRIL 1, 2028**
Depository institutions with $1.5B-$3B in total assets	**APRIL 1, 2029**
Depository institutions with $850M-$1.5B in total assets	**APRIL 1, 2030**

In summary, CFPB 1033 is expected to transform U.S. banking by strengthening consumer control, promoting secure data-sharing standards, and encouraging innovation across the financial services industry.

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