Deloitte.

# CFPB finalizes Personal Financial Data Rights Rule

Initial perspectives related to the finalized CFPB ruling around section 1033 of the Consumer Financial Protection Act (CFPA)

Center *for* Regulatory Strategy US

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) finalized section 1033 of the CFPA and its highly anticipated ruling around consumer-authorized financial data sharing, which aims to provide consumers with greater rights, privacy, and security over their personal financial data.[1] The final rule looks to improve the consumer experience across the payments, credit, and banking markets by fueling competition and empowering consumer choice. Focusing on flexibility and consumer control, the final rule modified several aspects of the proposed regulation including implementation timelines, in-scope data providers and third parties, adjusted data retention limitations, and shifting to consensus standards. Within hours of the rule's finalization, several bank associations filed a lawsuit claiming that the rule exceeds the authority of the Administrative Procedure Act (APA) under Section 1033.[2] While the outcome of this litigation is uncertain, preparation for implementation should not be delayed. Institutions—if they haven't already—should begin to assess their current consumer data landscape and determine how they will adhere to a secure open banking system.

## 5 summary insights

**Extended compliance timeline**: The final rule provides a more extended timeline compared to the initial proposal. It extends the compliance dates through a tiered approach based on institution asset size. The largest institutions ($250B+) will have until April 1, 2026, to achieve compliance with the final rule, whereas the smallest in scope institutions ($850M - $1.5B) will have until April 1, 2030. Notably, institutions with assets below $850M are now exempt from the rule.

**Expansion of in-scope providers:** Covered participants in the final rule includes digital wallet and payment facilitators, reinforcing the CFPB's mission of consistent data privacy and security protections irrespective of platform. These entities must comply with the same data-sharing requirements as traditional financial institutions and, therefore, will need to act in a timely matter to ensure appropriate infrastructure, processes, controls, and risk management practices are in place to support compliance.

**Data transmission and interface integration:** The final rule continues to encourage the transition from screen scraping to application programming interfaces (APIs), giving data providers the right to block screen scraping mechanisms should the appropriate interface be in place. However, despite industry requests, the rule has not fully prohibited screen scraping. The final rule also distinguishes between developer and consumer interfaces, stating that consumer interfaces need not adopt all developer interface specifications. Consumer interfaces can now provide certain types of data in human-readable or retainable formats rather than machine-readable format.

**Third party authorization and data usage:** The final rule tightens third-party authorization requirements by mandating a more structured process for third-party authorization and revocation. It requires third parties to obtain "express informed consent" from consumers and introduces stricter limitations on the secondary use of data, restricting usage for purposes such as targeted advertising or cross-selling. The final rule mandates that the authorization disclosure explicitly includes a description of the expected duration of data collection, which is one year from the consumer's last reauthorization.

**Information security requirements:** Many within the industry were hopeful that the final rule would include liability protection;[3] however, the rule instead reinforces stringent security requirements, leaving some ambiguity regarding liability in the event of data breaches. Compliance with established security frameworks, such as Gramm-Leach-Bliley Act (GLBA) and Federal Trade Commission (FTC) Standards, is mandated. These frameworks not only enhance data exchange security but also serve as useful benchmarks for determining data breach liability. Developer interfaces must adhere to these standards to ensure reliable performance and response times.



## 5 considerations to evaluate

1 **Formalize open banking strategy:** Institutions should evaluate final rule requirements to identify necessary enhancements and establish a multi-disciplined program management model tailored to the organization's open banking strategy and goals. Given the impact to various program areas such as data security, technology infrastructure, and third-party risk management (TPRM), institutions should seek active stakeholder engagement and support provided across the three lines to effectively adhere to requirements and maintain regulatory compliance.

2 **Assess technology architecture and data availability:** Data providers, as well as third parties, should evaluate their IT architecture to ensure all covered consumer data abides by confidentiality, enhanced consumer authorization, and consent management requirements. As part of the assessment, institutions should confirm that all covered data elements are digitally available in a clean, standardized format to ensure secure and confidential data sharing. To this end, investments in data infrastructure—such as data warehouses and associated data tools—and revisiting data strategy for secure data handling, storage, and transmission are essential to support API connectivity.

3 **Take an offensive stance:** To remain competitive in the era of open banking, institutions should proactively assess their bidirectional data capabilities to allow for effective utilization of increased consumer data availability. As consumer accounts become more portable, leveraging data to identify consumer retention and growth opportunities is paramount for an institution's longevity. Institutions should utilize the extended timeline to proactively address data-out compliance requirements and enhance data-in capabilities for enablement of business development, product and service innovation, and maintaining market position in an increasingly competitive marketplace.

4 **Access management:** The final rule places an emphasis on the consumer's ability to both grant and revoke a third party's access to their financial data. To effectively manage consumer requests and demonstrate compliance, institutions should establish processes, controls, and automation capabilities related to the intake, processing, and oversight of consumer data access requests. Institutions will be required to demonstrate the ability to effectively manage and process authorizations and reauthorizations, including the immediate halting of data sharing should access be revoked by the consumer.

5 **Evaluate TPRM program:** Financial institutions should assess their existing TPRM programs for compliance with the final rule. Potential areas of assessment include enhancing third-party and vendor due diligence, conducting security assessments of third-party systems and data practices, enhancing contractual agreements that bind third parties to the rule's data protection requirements, implementing continuous monitoring, and maintaining audit trail documentation.

## Endnotes

[1] Consumer Financial Protection Bureau (CFPB), "Required Rulemaking on Personal Financial Data Rights," October 22, 2024.

[2] *Bank Policy Institute et al. v. Consumer Financial Protection Bureau*, No. 5:24-cv-00304 (E.D. Ky., Lexington Div.).

[3] *See* Regulations.gov, "Required Rulemaking on Personal Financial Data Rights," as of October 22, 2024.

# Connect with us


### John Graetz
Principal
Deloitte & Touche LLP
jgraetz@deloitte.com

### Tim O'Connor
Principal
Deloitte Consulting LLP
tioconnor@deloitte.com

### Ulrike Guigui
Managing Director
Deloitte Consulting LLP
uguigui@deloitte.com

### Shaun Nabil
Managing Director
Deloitte & Touche LLP
snabil@deloitte.com


## Deloitte Center for Regulatory Strategy, US


### Irena Gecas-McCarthy
*FSI Director, Deloitte Center for Regulatory Strategy, US*
Principal
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

### Aaron Salerno
Manager
Deloitte Services LP
asalerno@deloitte.com

### Kyle Cooke
Manager
Deloitte Services LP
kycooke@deloitte.com