Hashed & Salted | A Privacy and Data Security Update
December 2024

Unlocking Financial Privacy: CFPB Issues Final Rule on Personal Financial Data Rights

The Consumer Financial Protection Bureau (CFPB) in October issued a final rule for personal financial data rights, referred to as the "open banking" rule because it requires banks, credit unions and other financial service providers to make consumer data available upon request to consumers and authorized third parties in a secure and reliable manner. This rule also establishes obligations for third parties accessing this data and promotes an open and inclusive industry standard for the consumer-directed exchange of personal financial data

Following the issuance of the final rule, the Washington, D.C.-based Bank Policy Institute, along with its Kentucky-based counterparts, filed a lawsuit in Kentucky federal court challenging the new rule as overreaching and "fundamentally irrational." The lawsuit complaint alleges that the CFPB lacks statutory authority for its open banking mandate and that imposing it risks undermining emerging private sector efforts to facilitate safer financial data-sharing for consumers.

Who (and what) is covered by the final rule?

The rule requires data providers—the covered banks, credit unions and other financial service providers—to electronically share covered data (e.g., transaction details, account balances, basic account verification and other consumer financial data) related to covered financial products and services, including bank debit accounts, credit card accounts and the facilitation of payments from those accounts, with consumers and authorized third parties. Depository institutions with total assets at or below the U.S. Small Business Administration (SBA) size standard for their North American Industry Classification System (NAICS) code are exempt from this requirement.

What is the CFPB's intended purpose of the final rule?

The rule aims to 1) empower consumers by allowing them to access their account data from data providers and authorize third parties to access their data; 2) promote competition through standardization; 3) prevent the dominance of existing data providers and intermediaries; and 4) protect consumers against unfair, deceptive and abusive practices.

What are the key provisions of the final rule?

Access Requirements: The final rule mandates that data providers must provide access to the covered data in compliance with the following access requirements:

1. **Reliability and Security:** Data providers must provide covered data reliably and securely to promote competition.
2. **Standardization:** Data providers must provide covered data in a standardized, machine-readable format and a commercially reasonable manner.

Attorney Advertising

3. **Frequency of Access:** Data providers cannot unreasonably limit the frequency of data requests.
4. **Prohibition of Screen Scraping:** Data providers cannot use screen scraping (using consumer credentials to log in and retrieve data) to comply with data access requirements.
5. **No Fees:** Data providers may not impose fees or charges for data access.
6. **Public Disclosure:** Data providers must publicly disclose certain information to facilitate data access and promote accountability.

Authorized Third Parties: The final rule mandates that to become an authorized third party, a third party must:

1. **Provide Authorization Disclosure:** Give the consumer a disclosure with key terms of data access.
2. **Certify Obligations:** Include a statement certifying the third party's compliance with specific obligations.
3. **Obtain Consent:** Secure the consumer's express informed consent, either electronically or in writing.
4. **Limit Collection:** Limit data collection, use and retention to what is necessary for the consumer's requested service. Activities like targeted advertising and data selling are excluded.
5. **Annually Renew the Authorization:** The authorization is valid for up to one year, after which a new authorization is needed. If the consumer revokes consent, the third party must stop collecting and using the data unless it's still necessary for the service.
6. **Establish Policies:** Have policies ensuring accurate data handling.
7. **Implement an Information Security Program:** Implement an information security program compliant with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework.
8. **Allow Revocation:** Allow consumers to revoke authorization and notify relevant parties upon revocation.
9. **Ensure Compliance:** Confirm other third parties comply with these obligations through contractual agreements.

Data Aggregators: The final rule mandates that data aggregators are allowed to handle authorization procedures on behalf of authorized third parties seeking consumer authorization. However, the authorized third party remains responsible for compliance. If a data aggregator is used, it must certify to the consumer that it will meet the authorized third party obligations, except for informing consumers and providing the authorization disclosure, contact information and a revocation mechanism. This certification can be included in the authorization disclosure or provided separately. The authorized third party's authorization disclosure must also include the data aggregator's name and a description of its services related to accessing the consumer's data.

Policies, Procedures and Recordkeeping

- **Data Providers:** Must have written policies and procedures to ensure the availability of covered data, proper response to developer interface access requests, accuracy of data transmitted and record retention.
- **Third Parties:** Defined as covered persons or service providers under the Consumer Financial Protection Act; must maintain records proving compliance for at least three years after obtaining the consumer's most recent authorization.
- **Data Aggregators:** Must maintain records proving compliance for at least three years after obtaining the consumer's most recent authorization.

What are the key takeaways from the final rule?

If the final rule withstands the legal challenge, then data providers, authorized third parties and data aggregators should take several steps to prepare for compliance. including, but not limited to:

Business Type	Key Takeaways
Data Providers	1. **Develop and Implement Policies and Procedures** ■ **Data Availability:** Ensure policies are in place to make covered data available to consumers and authorized third parties. ■ **Response Protocols:** Establish procedures for responding to data access requests reliably and securely. ■ **Accuracy and Security:** Implement measures to ensure the accuracy of data transmitted and maintain robust security protocols. 2. **Standardize Data Formats** ■ **Machine-Readable Format:** Ensure that data is available in a standardized, machine-readable format. ■ **Technical Standards:** Align with any technical standards set by the CFPB to facilitate data access and interoperability. 3. **Review and Update Systems** ■ **Developer and Consumer Interfaces:** Develop or update interfaces for third-party and consumer data access. ■ **Compliance Systems:** Ensure systems are capable of handling data requests in a commercially reasonable manner and meeting minimum response rates. 4. **Train Staff** ■ **Compliance Training:** Train staff on the new requirements and procedures for data access. ■ **Security Protocols:** Educate employees on maintaining data security and handling sensitive information. 5. **Prepare for Public Disclosure** ■ **Transparency:** Prepare to publicly disclose information about data access policies and procedures to promote accountability. 6. **Conduct Legal and Compliance Reviews** ■ **Legal Compliance:** Conduct a thorough review to ensure compliance with the final rule and other relevant regulations. ■ **Third-Party Agreements:** Update contracts with third parties to ensure they comply with the new obligations. 7. **Develop Consumer Communication Strategies** ■ **Authorization Disclosures:** Develop clear and comprehensive authorization disclosures for consumers. ■ **Revocation Mechanism:** Implement a method for consumers to easily revoke third-party authorizations. 8. **Establish Record Retention** ■ **Documentation:** Establish and maintain records of compliance for at least three years, as required.

Business Type	Key Takeaways
Authorized Third Parties	1. **Understand Authorization Requirements** ■ **Authorization Disclosure:** Develop clear and comprehensive authorization disclosures that include key terms of data access. ■ **Consumer Consent:** Implement processes to obtain express informed consent from consumers, either electronically or in writing. 2. **Certify Compliance** ■ **Obligations Certification:** Ensure that your organization can certify compliance with the specific obligations set forth in the rule, including limiting data collection, use and retention to what is necessary for the consumer's requested service. 3. **Implement Security Measures** ■ **Information Security Program:** Establish an information security program that complies with the GLBA Safeguards Framework to protect consumer data. ■ **Data Handling Policies:** Develop policies and procedures to ensure accurate data handling and secure data transmission. 4. **Develop Consumer Communication Strategies** ■ **Authorization Disclosure Copies:** Provide consumers with copies of the authorization disclosure and contact information for any questions. ■ **Revocation Mechanism:** Implement a method for consumers to easily revoke authorization and ensure that this process is clearly communicated. 5. **Establish Recordkeeping Practices** ■ **Compliance Records:** Maintain records proving compliance with the final rule for at least three years after obtaining the consumer's most recent authorization. 6. **Prepare for Data Aggregator Collaboration** ■ **Aggregator Certification:** If using data aggregators, ensure they certify to meet third-party obligations, except for informing consumers and providing a revocation mechanism. ■ **Disclosure Updates:** Include the data aggregator's name and a description of its services in the authorization disclosure. 7. **Review and Update Contracts** ■ **Third-Party Agreements:** Update contracts with other third parties to ensure they comply with the new obligations before sharing consumer data with them. 8. **Train Staff** ■ **Compliance Training:** Train staff on the new requirements and procedures for obtaining consumer authorization and handling data securely. ■ **Consumer Interaction:** Educate employees on how to effectively communicate with consumers about their data access rights and the authorization process.

Business Type	Key Takeaways
Data Aggregators	1. **Understand Authorization Requirements** ■ **Certification:** Ensure the ability to certify compliance with third-party obligations, except for informing consumers and providing a revocation mechanism. ■ **Authorization Disclosure:** Coordinate with third parties to include the aggregator's name and a description of services in the authorization disclosure. 2. **Implement Security Measures** ■ **Information Security Program:** Establish a robust information security program that complies with the GLBA Safeguards Framework. ■ **Data Handling Policies:** Develop and enforce policies to ensure accurate and secure data handling. 3. **Develop Consumer Communication Strategies** ■ **Clear Communication:** Work with third parties to ensure consumers receive clear and comprehensive authorization disclosures. ■ **Revocation Process:** Support third parties in implementing a method for consumers to easily revoke authorization. 4. **Establish Recordkeeping Practices** ■ **Compliance Records:** Maintain records proving compliance with the final rule for at least three years after obtaining the consumer's most recent authorization. 5. **Review and Update Contracts** ■ **Third-Party Agreements:** Ensure contracts with third parties reflect the new obligations and compliance requirements. 6. **Train Staff** ■ **Compliance Training:** Train staff on the new requirements and procedures for handling data securely and complying with authorization procedures. ■ **Consumer Interaction:** Educate employees on how to effectively support third parties and consumers in the data access process. 7. **Collaborate With Third Parties** ■ **Coordination:** Work closely with third parties to ensure seamless integration of authorization procedures and compliance measures. ■ **Support:** Provide technical and procedural support to third parties to help them meet their obligations under the final rule.

When does the final rule become effective?

The effective date of the final rule is 60 days after the rule is published in the Federal Register. The CFPB proposed this effective date and did not receive any comments. As set forth in 12 CFR 1033.121, data providers must comply with the requirements of this rule beginning on April 1, 2026. Compliance with the rule will be phased in between April 1, 2026, and April 1, 2030, based on the size of the financial institution. Larger providers must comply by April 1, 2026, while smaller institutions have until April 1, 2030.

Related Professional

Eyvonne Mallett . . . . . emallett@loeb.com