Holland & Hart

Open Banking Rules are Finally Here: What's Next for the Financial Services Industry

Timothy Crisp

Partner
303.295.8000
Denver, Salt Lake City, Santa Fe
TSCrisp@hollandhart.com

Tony Arias

Associate
303.295.5115
Boulder
JAArias@hollandhart.com

Insight — 10/28/2024

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) issued its long-anticipated Open Banking Rule (the Open Banking Rule) under Section 1033 of the Dodd-Frank Act, fundamentally reshaping the data-sharing landscape in financial services. This Open Banking Rule empowers consumers to access their financial data and authorize third parties to do the same. Data providers, third parties, and aggregators alike must now prepare for significant compliance demands regarding data access, security, and consent obligations.

Key Takeaways from the Open Banking Rule

- Consumers can now access their account data electronically and authorize third parties to do so on their behalf, provided security and consent requirements are met.
- Third parties must obtain express informed consent from consumers, with clear disclosures regarding data use, collection duration, and revocation rights.
- Third parties are limited in how consumer data can be used, barring unnecessary collection, cross-selling, or monetization efforts by third parties.
- Data providers must develop secure interfaces for third-party data access and comply with Gramm-Leach-Bliley Act (GLBA) or FTC security standards. Interfaces must meet minimum performance thresholds, maintaining at least a 99.5% success rate for data requests each month.
- Data providers cannot charge consumers or third parties for access to covered data.
- The Open Banking Rule introduces a staggered compliance schedule, with larger institutions required to comply by April 2026 and smaller institutions following suit in staggered dates through 2030.

Scope of the Rule: Who It Applies to, What It Covers, and When It Goes Into Effect

Data providers—including banks, credit unions, non-bank payment providers, card issuers, and digital wallet providers—are now required to provide consumers and authorized third parties access to covered data upon request for covered financial products or services. Compliance

timelines, however, vary based on the data provider's size.

Compliance Timeline

- Depository institutions that hold at least $250 billion assets or nondepository institutions that generate $10 billion in total receipts must comply starting on April 1, 2026.
- April 1, 2026: Depository institutions that hold at least $250 billion assets or nondepository institutions that generate $10 billion in total receipts must comply starting on April 1, 2026.
- April 1, 2027: Depository institutions that hold assets between $10 billion to $250 billion or nondepository institutions that generate less than $10 billion in receipts must comply starting April 1, 2027.
- April 1, 2028: Depository institutions that hold assets between $3 to $10 billion must comply starting April 1, 2028.
- April 1, 2029: Depository institutions that hold assets between $1.5 to $3 billion must comply starting April 1, 2029.
- April 1, 2030: Depository institutions that hold assets between $850 million to $1.5 billion must comply starting April 1, 2030.
- Depository institutions with assets of $850 million or less are exempt from the Final Rule's requirements, but if such institutions cross the asset size, then such institutions must comply within five years of crossing the threshold.

Covered financial products and services are:

(1) consumer checking, savings, and other consumer asset accounts, including prepaid accounts;

(2) consumer credit cards (or any single credit device like a credit card that can be used with credit); and

(3) any products or services that facilitate payments from consumer deposit accounts or consumer credit cards, excluding “first party payments,” which are those initiated by a payee or agent acting on behalf of the payee (*e.g.*, loan servicers).

Covered data includes transaction history information (at least 24 months), account balances, agreement terms and conditions, upcoming bill information, basic account verification details, and payment initiation data, such as account and routing numbers necessary for Automated Clearing House (ACH) transactions, with the option for tokenization to enhance security.

Compliance Obligations for Data Providers and Authorized Third Parties

Data Providers

Data providers must establish and maintain both consumer and developer interfaces to facilitate seamless and secure access to covered data. These interfaces must allow consumers and authorized third parties to retrieve

data in machine-readable formats that can be retained and processed in external, third-party systems. Compliance also requires aligning the performance of developer interfaces with commercially reasonable standards, ensuring a minimum response rate of 99.5% for valid requests each month.

To safeguard data access, fees for accessing covered data are prohibited, including any charges for setting up or maintaining the required interfaces. Data providers must also implement robust security protocols under the GLBA or applicable FTC standards, ensuring third-party interactions with developer interfaces meet established data safeguarding requirements. Screen scraping is expressly prohibited, with third-party access limited to secure and approved methods that do not rely on consumer login credentials.

In addition to providing real-time data access, data providers must maintain transparent revocation mechanisms. Consumers must have a straightforward way to revoke third-party access to their data, and data providers must promptly notify the affected third-party upon receiving a revocation request. Finally, data providers are responsible for monthly performance disclosures, reporting key metrics for interface performance and maintaining a 13-month rolling history of such data to promote accountability.

Authorized Third Parties

Authorized third parties must follow strict procedures to obtain, manage, and use consumer data. Before accessing data, they must secure the consumer's express informed consent through a clear, conspicuous, and standalone authorization disclosure. This disclosure must identify the data provider, describe the requested product or service, specify the data categories to be accessed, and include details on the duration of data collection, which cannot exceed one year without reauthorization. Additionally, the third party must provide a certification statement, committing to limit data use strictly to what is necessary for the consumer's requested service.

Third parties are prohibited from using consumer data for targeted advertising, cross-selling, or resale. They must also implement robust security protocols, either in accordance with the GLBA or FTC standards, to ensure the safety and integrity of collected data. Furthermore, third parties must provide consumers with a user-friendly revocation mechanism, free from penalties, and are required to notify data providers, aggregators, and other relevant parties of any revocation requests. Once revoked, the third party must cease data collection and only retain previously collected data if necessary to complete the consumer's requested service.

Finally, if third parties engage data aggregators to facilitate access to consumer data, they must ensure these aggregators comply with the same obligations and provide clear certification statements of compliance to consumers. This framework ensures third parties act transparently,

securely, and solely in the consumer's interest.

Get Proactive: Next Steps for Financial Institutions

Given the staggered compliance deadlines—spanning from April 2026 to 2030—financial institutions can and should proactively prepare to meet new regulatory demands. Below are key recommendations for financial institutions to navigate this compliance transition:

- Conduct a gap analysis to evaluate current data access capabilities and determine what modifications are necessary to align with machine-readable and commercially reasonable interfaces. Early assessments will reduce last-minute compliance risks.
- Establish or update internal governance frameworks to meet the rule's Open Banking Rule's requirements. This includes drafting policies on consent management, data sharing, and revocation processes.
- Monitor qualified industry standards and actively participate in standard-setting initiatives to align with best practices and emerging technologies. This ensures your interfaces remain compliant and competitive.
- Review and update customer agreements, privacy policies, and third-party contracts to reflect the Open Banking Rule's authorization and consent requirements. Incorporating these updates early will prevent disruptions during rollout.
- Design intuitive revocation methods and systems that enable consumers to revoke third-party access easily. Ensure your processes provide timely notification to relevant third parties upon receiving a revocation request.
- Create training programs and audit procedures to ensure ongoing compliance. Develop monitoring systems to track interface performance and prepare monthly disclosures as required.

Conclusion

The CFPB's Open Banking Rule ushers in a new era of open banking, promoting consumer autonomy and competition while safeguarding privacy. The Open Banking Rule introduces significant operational challenges for data providers and third parties. Financial institutions must take proactive steps to align their systems, policies, and governance frameworks with the Open Banking Rule's requirements. Early preparation is essential to avoid potential compliance risks and take advantage of the new competitive environment. Financial institutions that move swiftly can not only meet regulatory expectations but also position themselves as leaders in the open banking space.
