COMPLYING WITH THE NEW "OPEN BANKING" REGIME: PRIMER AND FACT SHEET

Date: 9 January 2025

US Policy and Regulatory Alert

By: Joshua L. Durham

The Consumer Financial Protection Bureau (CFPB) finalized its "open banking" rule in late 2024. As required by Section 1033 of the Consumer Financial Protection Act, the CFPB promulgated the rule to require certain financial services entities to provide for the limited sharing of consumer data and to standardize the way in which that data is shared. The CFPB has stated that the open banking rule will "boost competition" by facilitating consumers' ability to switch between banks and other financial service providers.

In general, the open banking rule:

- Provides consumers with control over their data in bank accounts, credit card accounts, and other financial products, including mobile wallets and payment apps;
- Allows consumers to authorize third-party access to consumers' data including transaction information, account balance information, and information needed to initiate payments; and
- Requires financial providers to make this information in accurate, machine-readable format and with no charge to consumers.

For more background on the history and policy of open banking, please review our prior alert.

COMPLIANCE DEADLINES

Numerous comments to the proposed rule urged the CFPB to lengthen the period of time for businesses to comply with the rule. The CFPB responded to those comments by extending the original six month compliance date for the largest affected institutions to provide a 1.5 year implementation period. The table below summarizes the compliance schedule by which different sized entities must operate in compliance with the rule:

Compliance Timeline	Depository Institutions	Nondepository Institutions
1 April 2026 (~1.5 years)	At least US$250b total assets	At least US$10b in total receipts as of either 2023 or 2024
1 April 2027 (~2.5 years)	At least US$10b total assets, but less than US$250b total assets	Less than US$10b in total receipts in both 2023 and 2024 (this is the final compliance date for nondepository institutions)

©2005-2026 K&L Gates LLP. All Rights Reserved.

1 April 2028 (~3.5 years)	At least US$3b total assets, but less than US$10b total assets	-
1 April 2029 (~4.5 years)	At least US$1.5b total assets, but less than US$3b total assets	-
1 April 2030 (~5.5 years)	Less than US$1.5b total assets, but more than US$850m (depositories holding less than US$850m are exempted from compliance)	-

MAKING CONSUMER FINANCIAL DATA AVAILABLE

Under the final rule, a “data provider” must provide, at the request of a consumer or a third party authorized by the consumer, “covered data” concerning a consumer financial product or service that the consumer obtained from the data provider. The rule defines data provider to include depository institutions, electronic payment providers, credit card issuers, and other financial services providers. The rule defines covered data to include transaction information, account balances, and other information to enable payments.

A data provider's obligations regarding covered data arise only when holding data concerning a consumer financial product or service that the consumer actually obtained from that data provider. Notwithstanding third-party obligations, merely possessing data from another data provider does not implicate the rule. The CFPB revised the definition of covered data in a manner that offers some clarity for the consumer reporting agencies (CRAs), which typically gather data for other entities for consumer credit reports.

	Electronic Payments	**Credit Cards**	**Other Products and Services**
Data Provider	A financial institution, as defined in Regulation E.	A card issuer, as defined in Regulation Z.	Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.
Covered Consumer Financial Product or Service	A Regulation E account.	A Regulation Z credit card.	Facilitation of payments from a Regulation E account or Regulation Z credit card.

©2005-2026 K&L Gates LLP. All Rights Reserved.

DATA PROVIDER INTERFACES

As part of the provision of data, data providers must create both consumer and developer interfaces to enable the efficient provision and exchange of consumer data. In addition to various technical requirements, data providers must also establish and maintain written policies and procedures to ensure the efficient, secure, and accurate sharing of consumer data. Data providers are prohibited from charging fees for providing this service.

	Consumer Interface	Developer Interface
When to Provide Data	Data provider receives information sufficient to: (1) authenticate the consumer's identity; and (2) identify the scope of the data requested.	Data provider receives information sufficient to: (1) authenticate the consumer's identity; (2) authenticate the third party's identity; (3) document the third party is properly authorized; and (4) identify the scope of the data requested.
Data Format	Machine-readable file	Standardized and machine-readable file
Interface Performance	Strict requirement to provide data	Minimum 95% success rate
Data Request Denials	Unlawful, insecure, or otherwise unreasonable requests may be denied	Unlawful, insecure, or otherwise unreasonable requests may be denied

AUTHORIZING THIRD PARTIES

To lawfully access covered data, a third party must generally do three things, namely: (1) provide the consumer with an authorization disclosure; (2) certify that the third party complies with various restrictions on the use of the data; and (3) obtain the consumer's express approval to access the covered data.

The rule prohibits three uses of data: (1) targeted advertising; (2) cross-selling of other products or services; and (3) selling covered data. While commenting on the proposed rule, several CRAs requested that the CFPB allow for use of covered data for internal purposes such as research and development of products. The CFPB found this reasonable and permitted “uses that are reasonably necessary to improve the product or service the consumer requested.”

CONCLUSION

The open banking rule establishes a robust framework for the exchange and transmission by certain entities regarding certain types of consumer data and the safeguarding of that data. Although the final rule extends the implementation deadlines beyond those originally proposed, implementation will require careful coordination among various functions of affected data providers' businesses and by entities authorized to receive covered data. Please reach out to a member of our team for further information.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



JOSHUA L. DURHAM
ASSOCIATE

SAN FRANCISCO
+1.415.882.8028
JOSH.DURHAM@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.