akerman

Practice Update

CFPB Finalizes Open Banking (Section 1033) Rule

October 23, 2024

By Eric I. Goldberg, Thomas J. Kearney, and Lenora ('Mimi') Lynham

On October 22nd, the Consumer Financial Protection Bureau ("CFPB") issued its final open banking rule, which implements section 1033 of the Dodd Frank Act ("Final Rule"). The Final Rule requires data providers, which includes providers of consumer asset accounts and credit cards, among others, to make certain financial data available in electronic form to consumers and to third parties who are authorized by consumers.[1] The CFPB contends the Final Rule moves the United States towards an "open banking system" and seeks to make it easier for consumers to switch between providers. The CFPB anticipates the Final Rule will prompt competition, consumer choice, lower loan prices, and improved customer service.[2] Under the Final Rule, consumers will now be able to access and share data from their bank accounts, credit cards, mobile wallets, and certain payment apps with third parties.

Below, we explain who is subject to the Final Rule, the requirements imposed by the Final Rule, and identify compliance deadlines. We note that a Kentucky bank and two trade associations immediately filed a lawsuit to block the Final Rule.[3] Depending on the outcome of the lawsuit, it may delay or entirely block the Final Rule.

Related People

Eric I. Goldberg
Thomas J. Kearney
Lenora ('Mimi') Lynham

Related Work

Consumer Financial Services, Data and Technology (CFS+)

Related Offices

Dallas
Fort Lauderdale
Washington, D.C.

This alert provides an overview of the Final Rule but does not address any specific compliance scenarios. If you have additional questions about the application of the Final Rule to your institution, please do not hesitate to contact us.

I. Data Providers

A. Data Providers Coverage/Definitions

The Final Rule labels the entities that maintain covered consumer data as "data providers." Data providers who control or possess covered data must make certain data elements available to consumers and certain third parties. The Final Rule applies to:

1. Financial institutions, as defined in Regulation E, 12 C.F.R. § 1005.2(i);
2. Card issuers, as defined in Regulation Z, 12 C.F.R. § 1026.2(a)(7); or
3. Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.[4]

The CFPB explains that buy now pay later (BNPL) providers that are card issuers, pursuant to the CFPB's recent BNPL interpretive rule, are subject to the Final Rule. The CFPB reaches this conclusion even though BNPL providers were not included in the CFPB's 1033 proposal.[5]

The Final Rule does not apply to all consumer financial products and services and also exempts certain small entities. A data provider is exempt if it is a depository institution or credit union with less than $850 million in assets. This number will fluctuate in the future based on SBA size standards referenced in the Final Rule.[6] Once an entity passes this threshold, it will remain subject to the Final Rule's requirements even if its asset size later goes below the threshold.

The following "covered consumer financial product or services" are subject to the Final Rule:

1. Regulation E Accounts (including prepaid accounts and mobile wallets);
2. Regulation Z credit cards; and
3. Payment facilitation from Regulation E accounts or Regulation Z credit cards, excluding products or services that merely facilitate first party payments.[7]

Under the Final Rule, an entity controls or possesses covered data if it is:

1. A data provider initiating a transfer to itself in conjunction with a product that facilitates payments to other payees;
2. A digital wallet provider initiating a transfer from an external bank account to a consumer's digital wallet the provider itself holds;
3. A digital wallet provider initiating a pass-through transfer through a consumer's Regulation E or Regulation Z account to another payee participating in the debit or credit card network; or
4. A credit card provider initiating a credit card payment from the consumer's external bank account to itself.

The Final Rule explains excluded "first party payments" are transfers initiated by the payee or an agent acting on behalf of the payee, including payments initiated by loan servicers.[8] The CFPB discusses this exemption in the Final Rule preamble, explaining that an entity would not be controlling or possessing covered data if it is:

1. A mortgage servicer merely initiating payments to itself to fulfill the consumer's mortgage obligation (because the mortgage servicer is only acting as an agent to the underlying mortgage holder);

2. An online merchant initiating a payment to themselves for goods they sold directly to the consumer; or
3. A utility company initiating payment to satisfy a consumer's bill.[9]

Based on these examples, if a financial institution provides a customer with a financial product or service, and an entity partners with a financial institution to facilitate the customer's payment for that product or service, the transaction might not involve covered data.

B. Data Provider Requirements

The Final Rule generally requires a data provider to make covered data available to consumers and authorized third parties upon request. A data provider must provide the data in a standardized and machine-readable format and in a commercially reasonable manner, including by meeting a minimum response rate with respect to requests for covered data.[10] A data provider must not unreasonably restrict the frequency with which it receives or responds to requests for covered data from an authorized third party and must not charge fees for data and screenscraping.[11] A data provider must also publicly disclose information about itself to facilitate access to covered data and to promote accountability.[12]

Covered data a data provider must make available includes: **(i)** transaction information; **(ii)** account balance information; **(iii)** information to initiate payment to or from a Regulation E account; **(iv)** available terms and conditions; **(v)** upcoming bill information; and **(vi)** basic account verification information – including name, address, email address and phone number, and if applicable, account identifier.[13] Data providers need not share Social Security Numbers.

A data provider is also permitted to make tokenized account numbers available instead of, or in addition

to, a non-tokenized account number.[14] Though, the tokenization may not be used as a pretext to restrict competitive use of payment initiation information. The CFPB explains data providers have legitimate reasons to use tokenized account numbers as "they can protect the security of the relevant payment system and thus benefit" consumers.[15] Tokenized account numbers, the CFPB explains, lower the risk of unauthorized transactions as they limit the potential misuse of payment credentials, help identify the source of data breaches, and cause less disruption when a credential is appropriately replaced.[16] The proposed rule had originally included routing numbers as a required element in this list. The CFPB decided against including routing numbers in the Final Rule because they are not usually tokenized.[17]

A data provider need not provide to a consumer or authorized third party any:

1. Confidential commercial information;
2. Information it collected for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;
3. Information required to be kept confidential by another law (except privacy laws); and
4. Any information not retrievable in the ordinary course of business.[18]

A data provider must provide information a consumer requests only when it can authenticate the consumer's identity and identify the scope of the data request.[19] Third parties may also request data from data providers as authorized by the consumer.[20] A data provider can provide a means to revoke a request for data (*i.e.*, a bank may ask a consumer to revoke a third party's access to data).[21] A data provider is required to maintain a record of when it did not provide data to either a requesting consumer or third party.[22] Data providers must also maintain written policies and procedures designed to achieve

the Final Rule's objectives and maintain evidence of compliance for three years after the date the provider takes an action subject to the rule.[23]

Data providers must establish developer and consumer interfaces by the compliance deadline, subject to narrow exceptions for safety and soundness and other security concerns.[24] There are no requirements for data providers to use specific technology when establishing these interfaces.[25] The developer interface must provide access to covered data upon request in a usable electronic form to third parties that are authorized to access covered data on behalf of consumers. Should a consumer or authorized third party request covered data in a machine-readable file, the data provider must provide the data in such a file that the requesting party can retain and transfer for processing into that party's information system.[26] The CFPB expects that consumer interfaces will need to endure minimal changes from what is provided today via online portals.[27] The data provider is not required to provide the files in a machine readable form for consumer interfaces, but must do so for developer interfaces.

Under the Final Rule, a data provider is prohibited from transferring its legal obligations to a vendor.[28] However, a data provider may retain a vendor to perform activities that satisfy the data provider's compliance obligations under the Final Rule without shifting its legal burden.[29]

In the Final Rule, the CFPB addressed the application of the EFTA and TILA liability provisions to data providers. The CFPB declined to address or adjust data providers' liability for unauthorized transactions, explaining that existing private network rules allow providers to obtain reimbursement for ACH transactions and that the CFPB did not find concerns about a higher risk of credit card fraud to be plausible.[30]

II. Authorized Third Parties

A. Third Party Coverage/Definitions

A third party is defined as "any person that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data."[31] When a third party seeks access to covered data on behalf of a consumer to provide a product or service that the consumer requested from it, the third party must meet three criteria:

1. Provide the consumer with an authorization;
2. Provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to certain obligations set forth in the Final Rule; and
3. Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.[32]

B. Third Party and Data Aggregator Obligations

If a third party meets the above criteria, it is deemed an authorized third party under the Final Rule.[33] Third parties must certify to limit their "collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service."[34] The CFPB has determined that targeted advertising, cross-selling, and the sale of covered data are not part of, or reasonably necessary to provide, any other product or service for purposes of this certification.[35]

Authorized third parties must also certify they will limit the duration of collection of covered data pursuant to a given authorization to a maximum period of one year.[36] To continue collection beyond the one year period, the third party must obtain a new authorization from the consumer no later than the anniversary of the most recent authorization.[37] If a consumer does not provide a

new authorization or if a consumer revokes authorization, the third party must cease its collection.[38] Data may be shared with other third parties in certain cases, such as when required by law, for servicing or processing the requested product or service, or for other reasonably necessary uses.[39] In such circumstances, these other third parties must comply with the requirements of the rule as well.[40]

Third parties must ensure they have written policies and procedures that are designed to ensure covered data is accurately received from the data provider and, if applicable, accurately provided to other third parties.[41] Third parties must also protect covered data with an information security program that satisfies the GLBA Safeguards Rule.[42]

Third parties must provide consumers with a copy of the signed authorization by either delivering the copy directly to the consumer or making it readily available to the consumer.[43] Upon a consumer's request, third parties must provide consumers with information about: **(i)** the categories of the data collected; **(ii)** their reasons for collecting and sharing this data; **(iii)** the names of parties with whom the data was shared; **(iv)** the status of the authorization; and **(v)** how a consumer may revoke this authorization.[44]

Under the Final Rule, third parties are allowed to rely on data aggregators but are not required to do so.[45] Third parties are required to establish and maintain written policies and procedures that are reasonably designed to ensure retention of records for at least three years after the third party has obtained a consumer's authorization.[46] Many commenters raised questions about the application of the Fair Credit Reporting Act (FCRA) to data aggregators. In the preamble to the Final Rule, the CFPB explained that data aggregators are not automatically consumer reporting agencies (CRAs).[47] The CFPB further explained "[t]his is the case even assuming data are provided to a data aggregator that qualifies

as a [CRA]. In these unique circumstances, the consumer, and not the data provider, would be the party that is furnishing data to the consumer reporting agency."[48] The CFPB acknowledged that it has ongoing FCRA rulemakings that may provide further clarification once those rules are finalized.

III. Compliance Dates

The Final Rule is effective sixty days after its publication in the *Federal Register*. However, substantive compliance obligations depend on the data provider's total assets or receipts.[49] Assuming the Final Rule's compliance dates are not changed by litigation or future rulemakings, a data provider's compliance date is as follows:

Data Provider Type			Compliance Deadline
Depository Institutions	>	$250 billion in total assets	April 1, 2026
Nondepository Institutions	>	$10 billion in receipts in either 2023 or 2024	
Depository Institutions	>	$10 billion in total assets	April 1, 2027
but	<	$250 billion in total assets	
Nondepository Institutions	<	$10 billion in total receipts in both 2023 and 2024	
Depository Institutions	>	$ 3 billion in total assets	April 1, 2028
but	<	$10 billion in total assets	
Depository Institutions	>	$1.5 billion in total assets	April 1, 2029
but	<	$3 billion in total assets	
Depository Institutions	>	$850 million in total assets	April 1, 2030
but	<	$1.5 billion in total assets	

The Final Rule does not set explicit compliance dates for third parties. Third parties must be prepared to request covered data in accordance with the Final Rule when requesting it from a data provider after that data provider's compliance date.

---

[1] Dodd-Frank section 1033; 12 U.S.C. § 5533. *See generally* Final Rule, to be codified at 12 C.F.R. part 1033.

[2] Press Release, Consumer Fin. Prot. Bureau, CFPB Finalizes Personal Financial Data Rights Rule to Boost Competition, Protect Privacy, and Give Families More Choice in Financial Services (Oct. 22,

2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/.

[3] Complaint, *Forcht Bank, et al. v. Consumer Fin. Prot. Bureau*, No. 5:24-cv-00304 (E.D. Ky. Oct. 22, 2024).

[4] 12 C.F.R. § 1033.111(c).

[5] CFPB, Required Rulemaking on Personal Financial Data Rights 70 (Oct. 22, 2024), https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights-final-rule_2024-10.pdf.

[6] 12 C.F.R. § 1033.111(d).

[7] 12 C.F.R. § 1033.111(b).

[8] 12 C.F.R. § 1033.111(b)(3).

[9] Final Rule, *supra* note 5, at 68.

[10] 12 C.F.R. § 1033.311(b).

[11] 12 C.F.R. §§ 1033.311(d), 1033.301(c).

[12] 12 C.F.R. § 1033.341(b).

[13] 12 C.F.R. § 1033.211.

[14] 12 C.F.R. § 1033.211(c)(1).

[15] Final Rule, *supra* note 5, at 132.

[16] *Id.*

[17] *Id.*

[18] 12 C.F.R. § 1033.221.

[19] 12 C.F.R. § 1033.331.

[20] *Id.*

[21] 12 C.F.R. § 1033.331(e).

[22] 12 C.F.R. § 1033.351.

[23] *Id.* (such actions include responding to a third party's request for access or information, revoking a third party's access based on a consumer's action, implementing compliant authorization procedures, etc.).

[24] 12 C.F.R. §§ 1033.301, 1033.311, 1033.321.

[25] 12 C.F.R. §§ 1033.301, 1033.311.

[26] 12 C.F.R. § 1033.301(b).

[27] Final Rule, *supra* note 5, at 157-58.

[28] *Id.* at 161.

[29] *Id.*

[30] *Id.* at 39 ("The CFPB has determined it would not be appropriate for this rule to impose a comprehensive approach to assigning liability among commercial entities or safe harbors from the requirements of EFTA and Regulation E or TILA and Regulation Z. The ability of payees to initiate electronic payments has existed for decades and the Regulation E concerns raised by commenters are not specific to CFPA section 1033.").

[31] 12 C.F.R. § 1033.131.

[32] 12 C.F.R. § 1033.401.

[33] *Id.*

[34] 12 C.F.R. § 1033.421(a)(1).

[35] 12 C.F.R. § 1033.421(a)(2).

[36] 12 C.F.R. § 1033.421(b)(2).

[37] 12 C.F.R. § 1033.421(b)(3).

[38] 12 C.F.R. § 1033.421(i).

[39] 12 C.F.R. § 1033.421(c).

[40] 12 C.F.R. § 1033.421(f).

[41] 12 C.F.R. § 1033.421(d).

[42] 12 C.F.R. § 1033.421(e).

[43] 12 C.F.R. § 1033.421(g)(1).

[44] 12 C.F.R. § 1033.421(g)(3).

[45] 12 C.F.R. § 1033.431.

[46] 12 C.F.R. § 1033.441.

[47] Final Rule, *supra* note 5, at 49-50 ("This final rule does not cause data aggregators to incur legal liability under the FCRA that they would not otherwise assume through their ordinary operations.").

[48] *Id.*

[49] 12 C.F.R. § 1033.121.
