Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

October 22, 2024

Executive Summary of the Personal Financial Data Rights Rule

On October 19, 2023, the Consumer Financial Protection Bureau (CFPB) issued a notice of proposed rulemaking regarding personal financial data rights to implement section 1033 of the Consumer Financial Protection Act (*i.e.*, the Dodd-Frank Act). On June 5, 2024, the CFPB finalized the provisions of the proposed rule regarding the attributes a standard-setting body must demonstrate in order to be recognized by the CFPB. That final rule and a guide for applying for recognition are available at https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights-industry-standard-setting.

On October 22, 2024, the CFPB finalized the remainder of the proposed rule. The October 22, 2024 final rule (final rule) requires data providers to make covered data regarding covered financial products and services available to consumers and authorized third parties in an electronic form, subject to a number of requirements. The final rule also sets forth criteria a third party must satisfy in order to be an authorized third party, including certifying it will satisfy certain obligations regarding the collection, use, and retention of covered data. The final rule is available at https://consumerfinance.gov/personal-financial-data-rights/.

.

This is a Compliance Aid issued by the Consumer Financial Protection Bureau. The CFPB published a Policy Statement on Compliance Aids, available at http://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/policy-statement-compliance-aids/, that explains the CFPB's approach to Compliance Aids.

Covered Entities: Data Providers

The final rule applies to data providers that control or possess covered data concerning a covered consumer financial product or service that a consumer obtained from the data provider. For this purpose, a "data provider" is a covered person pursuant to the Consumer Financial Protection Act (as defined in 12 U.S.C. 5481(6)) that is also:

- A financial institution, as defined in Regulation E, 12 CFR 1005.2(i);
- A card issuer, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or
- Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.

However, a depository institution that holds total assets at or below the specified Small Business Administration (SBA) size standard is not required to comply with the final rule as long as its total assets remain at or below the SBA size standard.[2] Beginning on the final rule's effective date, a depository institution calculates its total assets pursuant to the final rule by averaging the assets reported on its four preceding quarterly call report data submissions to the Federal Financial Institutions Examination Council (FFIEC) or National Credit Union Association (NCUA), as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the FFIEC or NCUA.[3] Information about when a depository institution must begin to comply if its total assets exceed the specified SBA size standard is available in the effective and compliance dates section below.

Covered Consumer Financial Products and Services

For purposes of the final rule, a "covered consumer financial product or service" is a consumer financial product or service pursuant to the Consumer Financial Protection Act (as defined in 12 U.S.C. 5481(5)) that is also one or more of the following:

- An account for purposes of Regulation E, 12 CFR 1005.2(b) (a Regulation E account);
- A credit card for purposes of Regulation Z, 12 CFR 1026.2(a)(15)(i) (a Regulation Z credit card); or

[2] The SBA size standard is the appropriate SBA size standard for commercial banking, credit unions, savings institutions and other depository credit intermediation, or credit card issuing, as codified in 13 CFR 121.201. Currently, the size standard is $850 million.

[3] If, as a result of a merger or acquisition, a depository institution does not have the named four quarterly call report submissions, the depository institution data provider shall use the process set out in 12 CFR § 1033.111(d)(3) to determine total assets.

- The facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments.

Making Covered Data Available

The final rule requires a data provider to make available to a consumer or an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. As discussed below, the data provider must make the covered data available in an electronic form usable by consumers and authorized third parties.

Pursuant to the final rule, "covered data" is:

- *Transaction information,* including historical transaction information in the control or possession of the data provider. A data provider is deemed to make available sufficient historical transaction information for this purpose if it makes available at least 24 months of such information.
- *Account balance information*.
- *Information to initiate payment to or from a Regulation E account*. This category applies only if the data provider directly or indirectly holds the Regulation E account, and does not apply to a data provider that merely facilitates pass-through payments. A data provider may make available a tokenized account number instead of, or in addition to, a non-tokenized account number as long as the tokenization is not used as a pretext to restrict competitive use of payment initiation information.
- *Terms and conditions*. These are data in the agreements evidencing the terms of the legal obligation between a data provider and a consumer, such as data in the account opening agreement and any amendments or additions to that agreement, including pricing information.
- *Upcoming bill payment information*, including information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.
- *Basic account verification information*. This is the name, address, email address, and phone number associated with the covered consumer financial product or service. For Regulation E and Regulation Z accounts, the data provider must also make available a truncated account number or other identifier for that account.

However, a data provider is not required to make the following available:

- Confidential commercial information;

- Information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting or making any report regarding other unlawful or potentially unlawful conduct;
- Information required to be kept confidential by any other provision of law; or
- Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

The final rule also prohibits a data provider from taking actions to evade the requirements of the final rule, including actions that are likely to make covered data it provides unusable or are likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data pursuant to the final rule.

Data Access Requirements

The final rule requires a data provider to receive requests for covered data in electronic form from consumers and authorized third parties and to make covered data available in electronic form in response to the requests. The final rule does not require that a data provider use any particular technology to satisfy these requirements.

With respect to requests for covered data in electronic form from authorized third parties, the final rule imposes the following requirements regarding how a data provider must be able to receive such requests and make covered data available in response to them:

- *Standardized format*. The data provider must make covered data available to authorized third parties in a standardized and machine-readable format, including through standardized protocols for communicating requests and responses for covered data. Indicia that the format is standardized and machine-readable include that the format conforms to a consensus standard.
- *Commercially reasonable performance*. A data provider's interface for receiving requests from and making covered data available to authorized third parties must perform at a commercially reasonable level. Performance cannot be commercially reasonable if it does not meet a minimum response rate of 99.5 percent. Indicia that performance is commercially reasonable include whether performance conforms to an applicable consensus standard, how performance compares to the performance levels achieved by similarly situated data providers, and how performance compares to the performance levels achieved by the data provider's interface for direct consumer data access.
- *Access caps*. A data provider must not unreasonably restrict the frequency with which it receives or responds to requests for covered data through its data interface. Any frequency

restrictions must be applied in a manner that is non-discriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to the final rule. Indicia that frequency restrictions are reasonable include that they conform to a consensus standard.

- *Access credentials*. A data provider must not allow a third party to access covered data using credentials that a consumer uses to access data electronically.
- *Security program*. In making covered data available to authorized third parties, a data provider must apply an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, except if the data provider is not subject to section 501 of the Gramm-Leach-Bliley Act. In that case, the program must satisfy the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

With respect to requests for covered data in electronic form received directly from a consumer, if a consumer requests covered data in a machine-readable file, the data provider must make covered data available in a file that is machine-readable and that the consumer can retain and transfer for processing into a separate information system that is reasonably available to and in the control of the consumer. These requirements do not apply to payment initiation information or account verification information, and terms and conditions do not need to be available directly to consumers in a file that is machine readable.

The final rule prohibits a data provider from imposing any fees or charges on a consumer or an authorized third party in connection with receiving electronic requests to access covered data or making covered data available pursuant to the final rule.

Denial of Data Access

A data provider does not violate the general obligation to make covered data available by denying a consumer or third party access to its data interface if the following two conditions are met:

- Granting access would be inconsistent with policies and procedures reasonably designed to comply with: (i) safety and soundness standards of the data provider's prudential regulator, as defined at 12 U.S.C. 5481(24); (ii) information security standards required by the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or (iii) other applicable laws and regulations regarding risk management.
- The denial is reasonable, meaning it must be directly related to a specific risk of which the data provider is aware and must be applied in a consistent and non-discriminatory manner.

Indicia that a denial is reasonable under the second condition include whether:

- A denial adheres to a consensus standard related to risk management;
- The denial proceeds from standardized risk management criteria that are available to the third party upon request;
- The third party has a certification or other identification of fitness to access covered data that is issued or recognized by a recognized standard setter or the CFPB.

Additionally, a data provider can deny access to a third party if:

- The third party does not present any evidence that its data security practices are adequate to safeguard the covered data; or
- The third party does not make the following information available to the data provider and readily identifiable to members of the public: its legal name; any assumed name it is using while doing business with the consumer; a link to its website; its Legal Entity Identifier (LEI); and contact information a data provider can use to inquire about the third party's data security and compliance practices.

Responding to Requests

The final rule requires a data provider to make covered data available through its interface to a consumer when it receives information sufficient to authenticate the identity of the consumer and identify the scope of the data requested.

The final rule requires a data provider to make covered data available through its interface to a third party when it receives information sufficient to authenticate the identity of the consumer who authorized the third party to access covered data, authenticate the third party's identity, document that the third party has followed the authorization procedures set forth in the final rule, and identify the scope of the data requested. Information on the final rule's authorization procedures is provided below. Before responding to a request from a third party, the data provider may confirm the scope of a third party's authorization by asking the consumer to confirm the account(s) the third party may access and the categories of covered data the third party may collect.

The final rule does not require a data provider to make covered data available in response to a request when:

- The data are withheld because an exception set forth in the final rule applies (see the discussion on making covered data available above);

- The data are not in the data provider's control or possession;
- The data provider receives the request when its data interface is not available;
- The request is from a third party and the consumer's authorization is no longer valid (e.g., it has been revoked or has expired); or
- The data provider has not received information sufficient to trigger the obligation to make covered data available in response to the request.

A data provider may provide a reasonable method for a consumer to revoke a third party's authorization to access the consumer's covered data, provided that method does not violate the prohibition against evasion. Indicia that the data provider's revocation method is reasonable include whether it conforms to a consensus standard. If a consumer requests revocation using this method, the data provider must revoke the authorized third party's access and notify the authorized third party of the request in a timely manner.

Making Information About the Data Provider Readily Identifiable

The final rule requires a data provider to make certain information readily identifiable to members of the public and available in both human-readable and machine-readable formats. This information includes the data provider's legal name, any assumed name it is using while doing business with the consumer, a link to its website, its LEI, contact information that enables a consumer or third party to receive answers to questions about accessing covered data pursuant to the final rule, and documentation sufficient for a third party to electronically access covered data pursuant to the final rule. Additionally, each month, a data provider must disclose to the public certain information about its data interface's response rate to authorized third party requests for covered data in the previous calendar month.

Policies, Procedures, and Recordkeeping for Data Providers

The final rule requires a data provider to have written policies and procedures that are reasonably designed to achieve the objectives set forth in the final rule. Among other things, the policies and procedures must be reasonably designed to ensure that the data provider:

- Creates a record of the data fields of covered data in its control or possession, what covered data are not made available to authorized third parties through the data provider's interface pursuant to an exception, and the reasons the exception applies. Indicia that a record of such data fields complies include listing data fields that conform to a consensus standard.

- Creates certain records when it denies an authorized third party's request for access to the data provider's interface or a request for information and provides certain information regarding the denial.
- Accurately makes covered data available to an authorized third party through its data interface. Indicia that policies and procedures regarding accuracy are reasonable include whether they conform to a consensus standard regarding accuracy.
- Retains records to reflect compliance with the final rule.

A data provider must periodically review these policies and procedures and update them as appropriate. Policies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities. A data provider has flexibility to design policies and procedures to avoid acting inconsistently with its other legal obligations, or in a way that could reasonably hinder enforcement against unlawful or potentially unlawful conduct.

Authorized Third Parties, Authorization Procedures, and Authorization Disclosures

As discussed above, the final rule requires a data provider to make covered data available to the consumer about whom the data pertains or to an authorized third party. For this purpose, an authorized third party is a third party[4] that has complied with the authorization procedures set forth in the final rule.

To become an authorized third party, a third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service that the consumer requested and must follow the authorization procedures set out in the final rule. Specifically, the third party must:

- Provide the consumer with an authorization disclosure as described in the final rule;
- 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 (see the discussion regarding third party obligations below); and
- 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.

[4] For purposes of the final rule, 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 is a third party.

The authorization disclosure must be provided to the consumer electronically or in writing, and it must be clear, conspicuous, and segregated from other material. It must be in the same language as the communication in which the authorization disclosure is provided to the consumer. Any translation of the authorization disclosure provided to the consumer must be complete and accurate. If the authorization disclosure is in a language other than English, it must include a link to an English-language translation.

The authorization disclosure must include all of the following:

- The name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures;
- The name of the data provider that controls or possesses the covered data that the third party seeks to access;
- A brief description of the product or service the consumer has requested from the third party and a statement that the third party will collect, use, and retain the consumer's data only as reasonably necessary to provide that product or service to the consumer;
- The categories of data that will be accessed;
- A statement certifying that the third party agrees to certain obligations set forth in the final rule (see the discussion of third party obligations below);
- A brief description of the expected duration of data collection and a statement that collection will not last longer than one year after the consumer's most recent reauthorization; and
- A description of the method that the consumer may use to revoke the authorization.

Third Party Obligations

As noted above, to satisfy the final rule's authorization procedures, a third party must provide a statement to a consumer certifying that the third party will satisfy certain obligations. These obligations are summarized below.

The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. For purposes of this limitation, targeted advertising, cross-selling, and the sale of covered data are not part of, or reasonably necessary to provide, any other product or service. Examples of uses of covered data that are permitted under the reasonably necessary limitation include: servicing or processing the product or service the consumer requested; uses that are specifically required under other provisions of law; uses that are reasonably necessary to improve the consumer's requested product or service;

and uses that are reasonably necessary to protect against or prevent fraud, unauthorized transactions, claims, or other liability.

The third party will also limit the duration of collection of covered data pursuant to a given authorization to a maximum period of one year. To continue collection, the third party must obtain a new authorization from the consumer no later than the anniversary of the most recent authorization. The third party is permitted to ask the consumer for a new authorization in a reasonable manner. Indicia that a new authorization request is reasonable include its conformance to a consensus standard. If a consumer does not provide a new authorization or if a consumer revokes authorization, a third party will cease its collection of covered data and cease its use and retention of covered data that was previously collected unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

A third party will have written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable. Indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy. The third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

A third party will apply an information security program to its systems for the collection, use, and retention of covered data. Generally, the program will satisfy the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801). If the third party is not subject to the rules issued pursuant section 501 to the Gramm-Leach-Bliley Act, the program will satisfy Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

The third party will ensure that consumers are informed about the third party's access to covered data. Specifically, the third party will provide the consumer with a copy of the authorization disclosure that the consumer has signed electronically or in writing and that reflects the date of the consumer's electronic or written signature. The third party will also provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The third party will have reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, information about the third party's access to the consumer's covered data as set forth in the final rule. The third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

The third party will provide the consumer with a method to revoke the third party's authorization. The method to revoke must be as easy to access and operate as the method for providing the initial authorization. The third party will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization. Additionally, the third party will notify the data provider, any data aggregator, and other third parties to which it has provided the consumer's covered data when the third party receives a consumer's revocation request.

A third party will require other third parties by contract to comply with specified third party obligations before providing covered data to them, unless otherwise permitted pursuant to the final rule.

Policies and Procedures for Third Party Record Retention

A third party that is a covered person or service provider as defined in the Consumer Financial Protection Act (12 U.S.C. 5481(6) and (26)), must have written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the final rule for a reasonable period of time.[5] A third party must periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

Use of Data Aggregators

The final rule permits data aggregators to perform the authorization procedures described in the final rule on behalf of the third party seeking the consumer's authorization. The third party seeking the authorization remains responsible for compliance with the authorization procedures even if it uses a data aggregator to perform the authorization procedures.

If the third party will use a data aggregator to assist with accessing covered data, the data aggregator must certify to the consumer that it will satisfy specified third party obligations as set forth in the final rule. This certification must be provided to the consumer. Either the third party may include this certification in its authorization disclosure or the data aggregator may provide it separately (in which case additional requirements set forth in the final rule apply). Additionally, the third party's authorization disclosure must include the data aggregator's name and a description of the services that the data aggregator will provide in connection with accessing the consumer's covered data.

[5] The period for which records are retained may not be less than three years after the third party obtains the consumer's most recent authorization.

Effective and Compliance Dates

The final rule is effective 60 days after its publication in the *Federal Register*. However, compliance with the final rule is not required at that time. In order to determine when it must begin complying with the final rule,[6] a data provider must determine which compliance date applies to it based on its status as a depository or nondepository institution and its size, which is either measured by total assets (for depository institutions) or by total receipts (for nondepository institutions). The dates on which data providers must begin complying with the final rule are set forth in the following chart.

Compliance Date	Depository Institution	Nondepository Institution
April 1, 2026	Holds at least $250 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions	Generated at least $10 billion in total receipts in calendar year 2023 or calendar year 2024
April 1, 2027	Holds at least $10 billion in total assets but less than $250 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions	Did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024
April 1, 2028	Holds at least $3 billion in total assets but less than $10 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions	Not applicable
April 1, 2029	Holds at least $1.5 billion in total assets but less than $3 billion in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions	Not applicable
April 1, 2030	Holds less than $1.5 billion in total assets but more than $850 million in total assets based on an average of its Q3 2023 through Q2 2024 call report submissions	Not applicable

When calculating its compliance date tier, a depository institution uses an average of its 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter call report data

[6] By the applicable compliance date, a data provider must have the functional ability to respond to requests in accordance with the final rule. A data provider may need time after the applicable compliance date to onboard third parties to its data interface, as permitted by the final rule.

submissions. If, as a result of a merger or acquisition, a depository institution does not have the named four quarterly call report submissions, the depository institution data provider shall use the process set out in 12 CFR § 1033.111(d)(3) to determine total assets. A nondepository institution calculates total receipts based on the SBA definition of receipts, as codified in 13 CFR § 121.104(a).

As noted above, a depository institution that holds total assets below the specified SBA size standard is not required to comply with the final rule as long as its total assets remain below the SBA size standard. If such a depository institution subsequently holds total assets (based on an average of its four preceding quarterly call report data submissions) that exceed that SBA size standard, it must comply with the final rule within a reasonable amount of time after exceeding the size standard. A reasonable amount of time shall not exceed five years.