CONSUMER FINANCIAL PROTECTION BUREAU | DECEMBER 2024

Personal Financial Data Rights Rule

Small Entity Compliance Guide

This document reflects the final rule as issued on October 22, 2024.

It does not include any legal developments occurring after this date. The Bureau has announced it is reconsidering the final rule. For updates, visit the Personal Financial Data Rights Compliance Resources page, which is available here.

Consumer Financial Protection Bureau

Table of Contents

1. Introduction

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act)[1] provides that, subject to rules issued by the Consumer Financial Protection Bureau (CFPB), certain persons must make information regarding consumer financial products and services available to individuals and their agents, trustees, and representatives acting on their behalf. It also provides that the information must be made available in a useable electronic form and mandates that the CFPB prescribe rules to promote the development and use of standardized formats for providing the information.

On October 19, 2023, the CFPB issued a proposal regarding personal financial data rights to implement section 1033 of the Act. On June 5, 2024, the CFPB finalized the provisions of the proposal regarding the attributes a standard-setting body must demonstrate in order to be recognized by the CFPB.[2] 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. The provisions regarding standard-setting bodies are also discussed in Section 5 of this guide.

On October 22, 2024, the CFPB finalized the remainder of the proposal. 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 and to have one or more interfaces that make that covered data available to consumers and authorized third parties in a useable electronic form. The final rule has requirements for interfaces, how data providers provide access to interfaces, and how data providers respond to requests for covered data. 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://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/.

[1] 89 *Fed Reg* 49084, 49084-091 (June 11, 2024).

[2] 89 *Fed Reg 90838,* 90838-998 (Nov. 18, 2024).

1.1 Scope of This Guide

This guide includes a detailed summary of the final rule's requirements.[3] Except when specifically needed to explain the final rule, this guide does not discuss other laws, regulations, or regulatory guidance that may apply. The content of this guide does not include any rules, bulletins, guidance, or other interpretations issued or released after the date on the guide's cover page. Users of this guide should review the final rule as well as this guide. The final rule is available on the CFPB's website at http://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/.

1.2 Use of Examples

This guide has examples to illustrate some portions of the final rule. The examples do not include all possible factual situations that could illustrate a particular provision, trigger a particular obligation, or satisfy a particular requirement.

1.3 Additional Resources

Additional resources to help industry understand and comply with the final rule are available on the CFPB's website at http://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/personal-financial-data-rights/. There is a link on this website to sign up for an email distribution list that the CFPB will use to announce additional resources as they become available.

If you have a specific regulatory interpretation question about the final rule after reviewing these resources, you can submit the question to the CFPB on its website at http://reginquiries.consumerfinance.gov. You may also leave your question in a voicemail at 202-435-7700. CFPB staff provides only informal responses to regulatory inquiries, and the responses are not official interpretations or legal advice. CFPB staff is not able to respond to specific inquiries within a particular requested timeframe. Actual response times will vary based on the number of questions that staff is handling and the amount of research needed to respond to a specific question.

[3] This guide meets the requirements of section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996 with regard to the final rule and is a Compliance Aid issued by the Consumer Financial Protection Bureau. The CFPB published a Policy Statement on Compliance Aids, available at https://www.consumerfinance.gov/rules-policy/final-rules/policy-statement-compliance-aids/, that explains the CFPB's approach to Compliance Aids.

2. Coverage

2.1 Covered Entities

Generally, data providers are required to comply with the final rule. However, the final rule includes a coverage threshold for data providers that are depository institutions. If a data provider is a depository institution and its total assets do not exceed the coverage threshold, the data provider is not required to comply with the final rule for as long as its total assets do not exceed the coverage threshold. The final rule specifies the calculation method that depository institutions must use when determining if they exceed the coverage threshold. 12 CFR 1033.111.

The final rule's definition of data provider is discussed in Section 2.1.1, the coverage threshold for data providers that are depository institutions is discussed in Section 2.1.2, and the method for determining total assets for purposes of the coverage threshold is discussed in Section 2.1.3.

2.1.1 Data Providers

A "data provider" is a covered person, as defined in 12 U.S.C. 5481(6), that is:

- A financial institution, as defined in Regulation E, 12 CFR 1005.2(i);[4]
- A card issuer, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or [5]
- 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 products and services are discussed in Section 2.2.

12 CFR 1033.111(c).

Data providers include banks, credit unions, and other persons that issue consumer purpose credit cards, that directly or indirectly hold consumer purpose demand deposit accounts or prepaid accounts, that issue access devices and agree to provide electronic fund transfer

[4] For this purpose, a "financial institution" is a bank, savings association, credit union, or any other person that directly or indirectly holds an account (as defined in 12 CFR 1005.2(b)) belonging to a consumer, or that issues an access device (as defined in 12 CFR 1005.2(a)(1)) and agrees to provide electronic fund transfer services (see 12 CFR 1005.3), other than a person excluded from coverage by section 1029 of the Act.

[5] For this purpose, a "card issuer" is a person that issues a credit card (as defined in 12 CFR 1026.2(a)(15)(i)) or that person's agent with respect to the card. Card issuers who only issue business purpose credit cards do not have data provider obligations under the final rule.

services, or otherwise facilitate payments to or from a Regulation E account. Digital wallet providers are data providers.

Data providers only have obligations under the final rule if they control or possess covered data concerning a covered consumer financial product or service that a consumer obtained from that entity. 12 CFR 1033.111(a). Covered financial products and services are discussed in Section 2.2. The information that constitutes covered data under the final rule is discussed in Section 3.1.2. Additionally, the final rule's definition of consumer is discussed in Section 3.1.3.

2.1.2 Coverage Threshold

The final rule includes a coverage threshold for data providers that are depository institutions. A depository institution that holds total assets that are equal to or less than the Small Business Administration (SBA) size standard applicable to the depository institution is not required to comply with the final rule as long as its total assets remain equal to or less than the SBA size standard. 12 CFR 1033.111(d).

Depository institutions that are data providers under the final rule must calculate their total assets (in the manner described in Section 2.1.3) as of January 17, 2025 (i.e., the final rule's effective date) to determine if their total assets are equal to or less than the specified SBA size standard. If the total assets are equal to or less than the SBA size standard, the depository institution is not covered under the final rule, but must recalculate its total assets on a quarterly basis (in the manner described in Section 2.1.3) until it either exceeds the coverage threshold or no longer satisfies the definition of a data provider under the final rule. If the total assets exceed the SBA size standard, the depository institution data provider exceeds the coverage threshold. Once a depository institution data provider exceeds the coverage threshold, it does not recalculate its total assets. The final rule does not allow depository institution data providers to fall out of coverage if their total assets subsequently decrease.

For purposes of the final rule, a depository institution is any depository institution as defined by the Federal Deposit Insurance Act, 12 U.S.C. 1813(c)(1), or any credit union as defined by 12 CFR 700.2. 12 CFR 1033.131.

The SBA size standard used to determine coverage under the final rule is the SBA size standard for the appropriate NAICS code for commercial banking, credit unions, savings institutions and other depository credit intermediation, or credit card issuing, as codified in 13 CFR 121.201. 12 CFR 1033.111(d)(1). As of the date on the cover of this guide, the size standard for each of the named NAICS codes is $850 million. The SBA reevaluates this size standard at least once every five years.

Example 1: Bank A is a depository institution and a data provider pursuant to the final rule. On January 17, 2025 (i.e., the final rule's effective date), Bank A calculates its total assets pursuant to the final rule and determines that it holds total assets of $3 billion. Bank A exceeds the final rule's coverage threshold. As long as Bank A is a data provider and controls or possesses covered data concerning a covered consumer financial product or service that a consumer obtained from it, Bank A will be covered under the final rule. This is true even if Bank A's total assets subsequently decrease to an amount that is equal to or below the applicable SBA size standard.

Example 2: Bank B is a depository institution and a data provider pursuant to the final rule. On January 17, 2025, Bank calculates its total assets pursuant to the final rule and determines that it holds total assets of $750 million. Bank B does not initially exceed the coverage threshold and is not covered under the final rule. Bank B recalculates its total assets every quarter pursuant to the final rule. In the first quarter of 2026, Bank B determines that, based on its four prior call report submissions, it holds total assets that exceed the applicable SBA size standard. Bank B exceeds the final rule's coverage threshold. As long as Bank B is a data provider and controls or possesses covered data concerning a covered consumer financial product or service that a consumer obtained from it, Bank B will be covered under the final rule. This is true even if Bank B's total assets subsequently decrease to an amount that is equal to or less than the applicable SBA size standard.

2.1.3 Calculating Total Assets

As noted above, the final rule has a coverage threshold for data providers that are depository institutions. The final rule provides a specific method for calculating total assets when determining whether a depository institution exceeds that coverage threshold.

Total assets held by a depository institution are determined by averaging the assets reported on the institution's four preceding quarterly call report 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. 12 CFR 1033.111(d)(2).

When determining whether it exceeds the coverage threshold as of the final rule's effective date, a depository institution determines its total assets by averaging the assets reported on its four quarterly submissions preceding January 17, 2025. Thus, if the depository institution submitted its call report for the fourth quarter of 2024 before January 17, 2025, it averages the assets

reported on its four quarterly reports for 2024. If it did not submit its call report for the fourth quarter of 2024 before January 17, 2025, it averages the assets reported on its fourth quarter report for 2023 and its first three quarterly reports for 2024.

Example 1: Bank is a data provider. Bank reports assets on its quarterly call reports for 2024 as follows: (Q1) - $850 million; (Q2) $855 million; (Q3) $850 million; and (Q4) $850 million. Bank submits its Q4 call report for 2024 before January 17. Bank's total assets exceed the coverage threshold because it must average the total assets reported on its four quarterly submissions preceding January 17, 2025.

Example 2: Assume the same facts as above, except Bank submits its Q4 2024 call report after January 17, 2025. Bank reported total assets of $840 million on its Q4 2023 call report. Bank's total assets do not exceed the SBA size standard as of the final rule's effective date. However, Bank must recalculate its total assets each quarter for as long as it is a data provider. When Bank recalculates its total assets using its Q4 2024 call report, its total assets will exceed the coverage threshold.

Example 3: Credit Union is a data provider. Credit Union reports assets on its quarterly call reports for 2024 as follows: (Q1) $700 million; (Q2) $755 million; (Q3) $750 million; and (Q4) $750 million. Additionally, Credit Union reported assets of $755 million on its report for Q4 of 2023. Regardless of when Credit Union submits its report for Q4 of 2024, its total assets do not exceed the SBA size standard as of the final rule's effective date. However, Credit Union must recalculate its total assets each quarter for as long as it is a data provider.

The final rule includes a separate provision for determining coverage of a data provider that is a surviving depository institution after a merger or acquisition. After a merger or acquisition, the surviving depository institution still determines total assets based on quarterly submissions. However, for quarters prior to the merger or acquisition, the surviving depository institution uses the combined assets reported on the quarterly call report submissions by all predecessor depository institutions. For quarters after the merger or acquisition, the surviving depository institution determines total assets by using the assets reported on the quarterly call report submissions by the surviving depository institution. The surviving depository institution shall determine total assets by using the average of the total assets reported for the four preceding quarters, whether the total assets are the combined assets of the predecessor depository institutions or from the surviving depository institution. 12 CFR 1033.111(d)(3).

Example 1: Bank A acquires Bank B effective June 1, 2025. Bank A reports assets of $750 million for each of its quarterly reports for 2024 and for its first two quarterly reports of 2025. Bank B reports assets of $500 million for each of its quarterly reports for 2024 and for its first two quarterly reports of 2025. Neither Bank A nor Bank B has total assets that exceed the SBA size standard. Thus, neither Bank A nor Bank B is covered under the final rule prior to the date that the merger is effective. However, pursuant to the final rule, Bank A must recalculate its total assets on June 1, 2025. Bank A must calculate total assets based on the combined assets reported by both Bank A and Bank B on the four quarterly reports submitted prior to June 1, 2025. Bank A's total assets based on the combined assets exceed the SBA threshold. Assuming Bank A is a data provider, it is covered under the final rule.

2.2 Covered Consumer Financial Products and Services

Generally, the final rule applies to a covered consumer financial product or service that a consumer obtained from a data provider. For this purpose, a covered consumer financial product or service is a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is one of more of the following:

- An account, as defined in Regulation E, 12 CFR 1005.2(b) (Regulation E account). This category includes consumer purpose checking accounts, saving accounts, and prepaid accounts.
- A credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i) (Regulation Z credit card).
- Facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments. A first party payment is a transfer initiated by the payee or an agent acting on behalf of the underlying payee. First party payments include payments initiated by loan servicers.

- A data provider's obligations under the final rule are limited to covered consumer financial product or services that a consumer obtained from the data provider. The final rule's definition of consumer is discussed in Section 3.1.3.
- Given the foreign applicability provisions in Regulation E and Regulation Z , covered consumer financial products and services for purposes of the final rule are limited to products and services obtained by consumers who reside in the United States. See Regulation E comment 3(a)-3 and Regulation Z comment 1(c)-1.

Situations where an entity, such as a merchant or mortgage loan servicer, is merely initiating a payment to itself for a product or service it provided to the consumer would not be enough to qualify as a covered consumer financial product or service. However, some first party payments satisfy the definition of covered consumer financial product or service, such as where the data provider is initiating a transfer to itself in conjunction with a product that facilitates payments to other payees, or the data provider is otherwise providing a Regulation E or Regulation Z account.

12 CFR 1033.111(b).

3. Data Provider Requirements and the Prohibition on Evasion

3.1 Requirement to Make Covered Data Available to Consumers and Authorized Third Parties

3.1.1 General Discussion

The final rule requires a data provider, upon request, to make covered data available to consumers and authorized third parties in an electronic form that the consumers and authorized third parties can use. This requirement applies to covered data that is in the data provider's control or possession and that concerns a covered consumer financial product or service that the consumer obtained from the data provider.
12 CFR 1033.201(a)(1). A data provider must make available the most recently updated covered data that it has in its control or possession at the time of a request, including information concerning authorized but not yet settled transactions. 12 CFR 1033.201(b). Section 3.1.2 discusses the covered data that the data provider must make available, and Section 3.1.3 discusses the consumers and authorized third parties to whom the covered data must be made available.

> Some elements of covered data are non-numeric—that is, they include natural language. When a data provider controls or possesses covered data that includes natural language, the data provider must make available the data in the language in which the data provider controls or possesses the covered data (whether that language is Spanish, English, or any other language).

The final rule also requires a data provider to have one or more interfaces to make covered data available to consumers and authorized third parties in an electronic form that they can use. Section 3.2 discusses the requirements related to interfaces, and Section 3.3 discusses the circumstances in which data providers are permitted under the final rule to deny access to an interface.

The final rule requires a data provider to make covered data available to a consumer or authorized third party upon request. Section 3.5 discusses the requests from consumers and authorized third parties that trigger the final rule's requirement to provide covered data.

As discussed in Section 3.6, a data provider must maintain certain policies and procedures that are reasonably designed to ensure that the data provider is satisfying the final rule's objectives, including this requirement to make covered data available.

Finally, the final rule includes an anti-evasion provision. Among other things, it prohibits any action that the data provider knows or should know is likely to render covered data unusable or that the data provider knows or should know is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data consistent with the final rule. The anti-evasion provision is discussed in Section 3.7.

3.1.2 Covered Data

For purposes of the final rule's requirements to make covered data concerning a covered financial product or service available to consumers and authorized third parties, covered data is:

1. *Transaction information*. This category includes historical transaction information that is in the control or possession of the data provider, such as amount, transaction date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges. A data provider is deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information.

2. *Account balance information*. This category includes available funds in an asset account and any credit card balance. However, a variety of account balances can apply to a product, such as cash advance balance, statement balance, or current balance, and the information a data provide must make available depends on the information in the data provider's control or possession.

3. *Payment initiation information*. This is information to initiate payment to or from a Regulation E account directly or indirectly held by the data provider. This category includes an account and routing number that can be used to initiate an Automated

- The final rule does not require data providers to grant access to, or facilitate payments on, any particular payment network.
- The final rule does not affect other requirements for initiating payments or accessing payment networks. Other payment authorization requirements continue to apply.
- Nothing in the final rule gives a third party authority to initiate or "push" payments from a consumer's account or requires a data provider to allow a third party to initiate a payment.

Clearing House (ACH) transaction. A data provider is permitted to make available a tokenized account number (TAN) 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. Data providers who do not directly or indirectly hold the underlying Regulation E account are not required to provide payment initiation information. For example, a data provider that merely facilitates pass-through payments would not be required to make available account and routing number for the underlying Regulation E account.

4. *Terms and conditions*. Terms and conditions are limited to data in agreements evidencing the terms of the legal obligation between a data provider and a consumer for a covered consumer financial product or service, such data in the account opening agreement and any amendments or additions to that agreement, including pricing information. This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, credit limit, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

5. *Upcoming bill information*. This category includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider. If upcoming bill payment information scheduled outside of the data provider's bill payment platform is not in the data provider's control or possession, it is not covered data. For example, when a consumer uses a cell phone company's website to schedule a bill payment from the consumer's bank account, the consumer's bank may not control or possess that information unless the cell phone company is sharing that preauthorization information with the bank. In contrast, a bank does control or possess information about a cell phone payment a consumer scheduled through the bank's consumer interface.

6. *Basic account verification information*. This category is limited to the name, address, email address, and phone number associated with the covered consumer financial product or service. If a data provider directly or indirectly holds a Regulation E account or Regulation Z account belonging to the consumer, the data provider must also make available a truncated account number or other identifier for that account.

12 CFR 1033.211.

A data provider is not required to make the following covered data available to a consumer or authorized third party:

1. *Confidential commercial information*. This category includes an algorithm used to derive credit scores or other risk scores or predictors. However, covered data does not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. For example, annual percentage rate and other pricing terms are sometimes determined by an internal algorithm or predictor but do not fall within this exception. Similarly, rewards programs terms, rewards credits, and rewards terms and conditions are not confidential commercial information.

2. *Information collected to prevent, detect, or report unlawful conduct*. A data provider is not required to make available any 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. Covered data collected for other purposes does not fall within this exception. For example, name and other basic account verification information do not fall within this exception.

3. *Other confidential information*. A data provider is not required to make available information it is required to keep confidential by any other provision of law. Information does not qualify for this exception merely because the data provider must protect it for the consumer. For example, the data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections.

4. *Information that is not retrievable in the ordinary course*. A data provider is not required to make available any information that it cannot retrieve in the ordinary course of its business. Generally, a data provider is not permitted to categorically refuse access to data included in the definition of covered data under this exception, absent some additional showing that the specific data were not retrievable in the ordinary course of its business. Additionally, a data provider that takes any action with the intent of evading the final rule's requirements, or that the data provider knows or should know is likely to render unusable covered data, or that is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data would violate the final rule's anti-evasion provision. Nonetheless, there may be situations where a data provider cannot retrieve information in the ordinary course of its business. For example, if historical terms and conditions information is stored as image files and it would require extraordinary, manual effort to translate this information into an electronic form, that information may not be retrievable in a data provider's ordinary course of business.

12 CFR 1033.221.

3.1.3 Consumers and Authorized Third Parties

As discussed above, the final rule requires data providers to make covered data available to consumers and authorized third parties upon request. This section discusses who is a consumer and who is an authorized third party under the final rule. Additional information regarding third parties and authorized third parties is in Section 4.

Consumers

For purposes of the final rule, the term consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of the final rule and, as a result, are included in the final rule's definition of consumer. 12 CFR 1033.131.

For the purposes of the final rule, the term consumer also includes guardians, trustees, custodians, and similar natural persons acting on behalf of a consumer pursuant to state law. In these circumstances, natural persons who manage consumer accounts through legal processes, like guardians and custodians, function through existing legal processes that establish rights for a natural person to manage the assets and income for another natural person. It would be appropriate for these natural persons that are duly authorized to manage another natural person's covered financial products or services to also authorize third parties to access the covered data related to those products or services pursuant to the final rule.

However, circumstances where corporate terms and conditions contain provisions by which consumers purportedly appear to consent, upon acceptance, to corporate entities' limited powers of attorney to act as agents for the consumers, would not position such corporate entities as consumers under the final rule because they are factually and legally different from those circumstances addressed by the final rule's definition of consumer.

Authorized Third Parties

An authorized third party is a third party that seeks to access covered data on behalf of a consumer to provide a product or service that the consumer requested and that has satisfied the final rule's authorization procedures. To satisfy those authorization procedures, a third party must:

- Provide the consumer with an authorization disclosure that satisfies requirements set forth in the final rule. These requirements for the authorization disclosure are discussed in Section 4.2.

> Under the final rule, a third party is 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. 12 CFR 1033.131.

- Provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to the third party obligations described in the final rule. These third party obligations are discussed in Section 4.3.
- 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.

12 CFR 1033.131 and 1033.401.

3.2 Requirements for Data Providers' Interfaces

A data provider must maintain one or more interfaces to receive requests for covered data from consumers and authorized third parties, and to make covered data available to consumers and authorized third parties in response to those requests. 12 CFR 1033.301.

> Under the final rule, not every interface that a data provider maintains to make covered data available to consumers must satisfy the final rule's requirements, as long as collectively the data provider's consumer interfaces satisfy the requirements. For example, a data provider may maintain both a mobile application and an online banking portal that consumers can use to request and receive covered data. The mobile application does not need to satisfy the final rule's requirements as long as the online banking portal does.

The final rule uses the term "consumer interface" to refer to the mechanism a data provider uses to receive requests from and provide covered data to consumers. It uses the term "developer interface" to refer to the mechanism a data provider uses to receive requests from and provide covered data to authorized third parties. 12 CFR 1033.131. While the final rule uses the terms "consumer interface" and "developer interface," it does not require a data provider to maintain interface functionality that is exclusively accessible by authorized third parties and a separate interface functionality that is exclusively accessible by consumers. Instead, the final rule permits (but does not require) data providers to grant developer interface access to consumers and to grant consumer interface access to authorized third parties. It also permits (but does not require) a data provider to provide its developer interface and its consumer interface through the same mechanism (or set of mechanisms), provided that the mechanism otherwise satisfies the final rule's requirements.

A data provider must maintain interface(s) that satisfy the requirements set forth in the final rule. 12 CFR 1033.301(a). Its consumer interface must satisfy the requirements for interfaces

that are discussed in Section 3.2.1. A data provider's developer interface must satisfy the requirements discussed in Section 3.2.1 and the additional requirements discussed in Section 3.2.2.

The final rule prohibits a data provider from imposing any fees or charges on a consumer or an authorized third party in connection with establishing or maintaining the interfaces. 12 CFR 1033.301(c).

3.2.1 Machine-Readable Files Upon Request

Generally, if a consumer or authorized third party requests covered data in a machine-readable file, the final rule requires that a data provider's interface must make covered data available in a file that is machine readable and that the consumer or authorized third party can retain and transfer for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party. 12 CFR 1033.301(b).

- The final rule does not require a data provider to make all covered data available to a consumer in a single file.
- A data provider should not require a consumer to specifically use the words "machine-readable file" when making a request. For example, if a consumer requests "a spreadsheet" of transactions, the data provider should consider the consumer to have requested a machine-readable file.

This requirement to make covered data available in a file that is machine readable and that can be retained and transferred for processing into a separate information system does not apply to payment initiation information or basic account verification information made available to consumers. 12 CFR 1033.301(b)(1)(i). A data provider need only make that information available to consumers in an electronic form that consumers can use, such as a human-readable form. Additionally, the final rule does not require data providers to make the account terms and conditions available to consumers in machine-readable form. 12 CFR 1033.301(b)(1)(ii). Instead, that information need only be made available in an electronic form that consumers can use, retain, and transfer for processing.

For consumers, the covered data that remains subject to the requirement to provide a machine-readable file that can be retained and transferred to for processing is the following: transaction information, account balance information, and upcoming bill information. 12 CFR 1033.301(b)(1). The following chart sets forth the form in which a data provider must make each category of covered data available to consumers.

Category of Covered Data Made Available to Consumers	Must be in a machine-readable file?	Must be in a form that the consumer can retain?	Must be in a form that the consumer can transfer for processing?
Transaction information	Yes	Yes	Yes
Account balance information	Yes	Yes	Yes
Upcoming bill information	Yes	Yes	Yes
Terms and conditions	No, but must be in an electronic form that consumers can use	Yes	Yes
Payment initiation information	No, but must be in an electronic form that consumers can use	No	No
Basic account verification information	No, but must be in an electronic form that consumers can use	No	No

All covered data made available to authorized third parties is subject to the requirement to provide a machine-readable file that can be retained and transferred for processing into the information systems of the third parties. 12 CFR 1033.301(b). A data provider may satisfy this requirement by making covered data available in a form that satisfies the final rule's standardized format requirement in 12 CFR 1033.311(b). The final rule's standardized format requirement is discussed in Section 3.2.2 immediately below. 12 CFR 1033.301(b)(2).

3.2.2 Additional Requirements for Developer Interfaces

A data provider's developer interface must satisfy the requirements discussed above in Section 3.2.1 and the requirements discussed in this Section 3.2.2. See 12 CFR 1033.311(a).

Standardized Format

A developer interface must make covered data available in a standardized and machine-readable format. Indicia that the format satisfies this requirement include that it conforms to a consensus standard. 12 CFR 1033.311(b).

For purposes of this requirement, "format" includes structures and definitions of covered data and requirements and protocols for communicating requests and responses for covered data.

"Standardized" means conforms to a format widely used by other data providers and designed to be readily usable by authorized third parties.

- A data provider's developer interface would not necessarily need to make each specific term of its account terms and conditions available as a discrete "callable" data field. Instead, it could make the full account opening agreement available or a broad section of such an agreement available as "text" data fields, subject to the final rule's standardized and machine-readable format requirements.

Commercially Reasonable Performance

A developer interface's performance must be commercially reasonable. 12 CFR 1033.311(c). The developer interface's performance cannot be commercially reasonable if it does not meet the response rate described below. Additionally, the final rule includes indicia of whether a developer interface's performance is commercially reasonable. These indicia are also discussed below.

The developer interface's performance cannot be commercially reasonable if its response rate is not equal to or greater than 99.5 percent in each calendar month. To calculate the response rate, the data provider divides the number of proper responses by the total number of requests for covered data to the interface. For purposes of making this calculation, all of the following apply:

- Any responses by and requests to the interface during scheduled downtime for the interface must be excluded respectively from the numerator and the denominator of the calculation.
- In order for any downtime of the interface to qualify as scheduled downtime, the data provider must have provided reasonable notice of the downtime to all third parties to which the data provider has granted access to the interface. Indicia that the data

provider's notice of the downtime may be reasonable include that the notice conforms to a consensus standard.

- The total amount of scheduled downtime for the interface in a calendar month must be reasonable. Indicia that the total amount of scheduled downtime may be reasonable include that the amount conforms to a consensus standard.

- A proper response is a response, other than any message provided during unscheduled downtime of the interface, that meets all of the following criteria:

  - The response either fulfills the request or explains why the request was not fulfilled;

  - The response is consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to 12 CFR 1033.351(a). These policy and procedures are discussed in Section 3.6; and

  - The response is provided by the interface within a commercially reasonable amount of time. Indicia that a response is provided in a commercially reasonable amount of time include conformance to an applicable consensus standard.

  - The final rule's "proper response" definition does not require that covered data be returned in every case. For example, if a data provider has reasonable frequency restrictions in place that comply with 12 CFR 1033.311(d) and has written policies and procedures that comply with 12 CFR 1033.351(a), a proper response to a request that is in excess of the reasonable frequency restrictions described in the data provider's policies and procedures may explain why the request was not fulfilled (provided the response is timely and otherwise complies with the final rule).

12 CFR 1033.311(c)(1).

Indicia that an interface's performance is commercially reasonable as required by the final rule include:

- Whether the interface's performance conforms to a consensus standard that is applicable to the data provider;

- How the interface's performance compares to the performance levels achieved by the developer interfaces of similarly situated data providers; and

- How the interface's performance compares to the performance levels achieved by the data provider's consumer interface.

12 CFR 1033.311(c)(2)(i).

For each of the above indicia, relevant performance specifications include: (1) the interface's response rate as discussed above; (2) the interface's total amount of scheduled downtime; (3) the amount of time in advance of any scheduled downtime by which notice of the downtime is provided; (4) the interface's total amount of unscheduled downtime; and (5) the interface's response time. 12 CFR 1033.311(c)(2)(ii).

Access Caps

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 through its developer 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. These policy and procedures are discussed in Section 3.6. Indicia that any frequency restrictions applied are reasonable include that they conform to a consensus standard. 12 CFR 1033.331(d).

Security Specifications

ACCESS CREDENTIALS

A data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface. However, a data provider does not violate the final rule if it contracts with a service provider to establish or maintain the data provider's developer interface if the contract provides that the service provider will make covered data available, in a form and manner that satisfies the final rule, to authorized third parties through the developer interface by means of the service provider using a consumer's credentials to access the data from the data provider's consumer interface. 12 CFR 1033.331(e)(1).

SECURITY PROGRAM

A data provider must apply an information security program to its developer interface. Generally, if the data provider is subject to section 501 of the Gramm-Leach-Bliley Act (GLBA), it must apply an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA, 15 U.S.C. 6801. If the data provider is not subject to section 501 of the GLBA, it applies the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314. 12 CFR 1033.331(e)(2).

3.3 Denials of Interface Access

A data provider does not violate the general access obligation discussed in Section 3.1 if it denies a consumer or third party access to all elements of the data provider's interface and the following two conditions are met:

1. Granting access would be inconsistent with policies and procedures reasonably designed to comply with:

    a. Safety and soundness standards of a prudential regulator, as defined at 12 U.S.C. 5481(24), of the data provider;

    b. Information security standards required by the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

    c. Other applicable laws and regulations regarding risk management. A denial based on "other applicable laws and regulations regarding risk management" might include a denial of a third party on a list released by the Office of Foreign Assets Control (OFAC), such as the Specially Designated Nationals and Blocked Persons list, or a denial made to avoid inconsistency with requirements to prevent money laundering and terrorist financing under the Bank Secrecy Act or the Corporate Transparency Act. 12 CFR 1033.321(a).

2. 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. 12 CFR 1033.321(a) and (b). Indicia that a denial is reasonable under this second condition include whether:

    a. The denial adheres to a consensus standard related to risk management;

- A denial would not be appropriate under the final rule's denial of access provision if it applied only to certain aspects of the developer interface or only to certain data fields, because it would not affect "all elements" of the interface.
- A data provider may deny access any time the requirements for denial in the final rule are met, even if it has previously granted access.
- The final rule provides data providers with flexibility to deny access to third parties that are not domiciled in the United States based on risk management obligations.

- In general, a denial is directly related to a risk if it is appropriately tailored to that risk. For example, if a data provider denies access to a third party during the onboarding process because it is missing information about that third party's information security practices, then it should grant access once it receives information that establishes the sufficiency of those practices. Under these circumstances, an indefinite denial would not be directly related to the risk justifying the denial.

b. The denial proceeds from standardized risk management criteria that are available to the third party upon request; and

c. 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. 12 CFR 1033.321(c).

If a data provider identifies a risk that might call for denying access to a third party, the data provider should effectively consider how its policies and procedures can tailor any restriction on data access to the risk presented. In analyzing the extent of the risks presented by the third party, the data provider should take into account the fact that a consumer will have authorized the third party to access data, or that certain risks are mitigated by operation of the final rule. Policies and procedures would not be reasonably designed, for instance, if, they do not account for the protections in the final rule that address a third party's potential use of consumer-authorized data.

Denials would be unjustified if they are based solely on a data provider's policies and procedures that override the substantive protections found in the final rule, such as asserting that the authorization procedures and obligations for third parties seeking to access covered data on consumers' behalf are insufficient. For example, denying access because a third party intends to follow the final rule's protections rather than a data provider's alternative protections would infringe consumer's data access rights.

Additionally, a data provider can deny a third party access to the data provider's interface 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.

12 CFR 1033.321(d).

> Attempts to seek or demand particular terms in an onboarding arrangement, including wholesale indemnification or hold-harmless terms or other terms that would effectively relieve data providers of their own obligations to follow applicable law, may violate the final rule's anti-evasion provision, and raise concerns about the permissibility of a denial.

A data provider could rely on the final rule's denial of access provision to deny a third party access to the developer interface temporarily, consistent with policies and procedures

reasonably designed to comply with safety and soundness standards of a prudential regulator (among other legal obligations), and if the denial otherwise complies with the final rule. A data provider could not rely on the final rule's "denial of access" provision to justify a developer interface's technical inability to satisfy the final rule. For example, it generally would be impermissible for a data provider to deny a third party access temporarily, in connection with onboarding, solely because the data provider's developer interface could not scale to achieve the 99.5 percent response rate required under the final rule.

As discussed in Section 3.8 regarding the compliance dates, data providers may need to onboard third parties in a staggered manner. Denying access to a third party until it can be properly onboarded may be necessary to comply with a data provider's legal obligations regarding risk management. When the third party has been properly onboarded, the data provider may impose reasonable access caps pursuant to the final rule.

3.4 Requirement to Make Covered Data Available in Response to Requests

Once a data provider has granted interface access to a consumer or authorized third party, the data provider generally must provide covered data through the interface in response to the consumer's or authorized third party's request. However, a data provider is not required to make covered data available in response to all requests. First, a data provider is only required to make covered data available in response to a request under the final rule if the information provided is sufficient to trigger a response as discussed in Section 3.4.1. Second, there are circumstances in which covered data need not be made available in response to a request under the final rule. These circumstances are discussed in Section 3.4.2. See 12 CFR 1033.331.

> 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 requests or making available covered data in response to requests pursuant to the final rule.
> 12 CFR 1033.301(c)(3).

Information on responding to requests for covered data for joint accounts is discussed in Section 3.4.3.

3.4.1 Sufficient Information to Trigger Obligation to Make Covered Data Available in Response to a Request

A data provider must make covered data available in response to a consumer's request when the data provider receives information sufficient to authenticate the consumer's identity and identify the scope of the data requested. 12 CFR 1033.331(a).

A data provider must make a consumer's covered data available in response to an authorized third party's request when that data provider receives information sufficient to:

- Authenticate the consumer's identity;
- Authenticate the third party's identity;
- Document that the third party has followed the final rule's authorization procedures (see Section 4.1 for information on these authorization procedures); and
- Identify the scope of the data requested.

12 CFR 1033.331(b)(1).

- Receipt of a copy of the signed authorization disclosure constitutes information sufficient to document the third party has followed the rule's authorization procedures, absent facts to the contrary.
- A data provider should consider applicable Standards for Safeguarding Customer Information and any other applicable legal obligations when determining whether it has information sufficient to authenticate a consumer's or third party's identity.

The data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm the account(s) to which the third party is seeking access and the categories of covered data the third party is requesting to access. 12 CFR 1003.331(b)(2). However, the data provider cannot do so in manner that violates the final rule's anti-evasion provision.

3.4.2 Circumstances in Which a Data Provider is not Required to Make Covered Data Available

A data provider is not required to make covered data available in response to a request when:

- The data are withheld because they are covered data that the data provider is not required to make available pursuant to 12 CFR 1033.221 (i.e., they are not retrievable in the ordinary course of the data provider's business; are confidential commercial information; are other confidential information; or are information collected to prevent, detect, or report unlawful conduct);
- The data are not in the data provider's control or possession;

- The data provider's interface is not available when the data provider receives a request requiring a response as discussed in Section 3.4.1;
- The request is for access by a third party; and:
  - The consumer has revoked the third party's authorization pursuant to the revocation method that the data provider has made available to the consumer;
  - The data provider has received notice that the consumer has revoked the third party's authorization; or
  - The consumer has not provided a new authorization to the third party after the maximum duration period set forth in the authorization disclosure; or
- The request does not include sufficient information to trigger the requirement to provide covered data as discussed in Section 3.4.1.

12 CFR 1033.331(c).

3.4.3 Jointly Held Accounts

A data provider that receives a request for covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of such a consumer must make available covered data to that consumer or authorized third party, subject to the other provisions of the final rule. 12 CFR 1033.331(d).

- The final rule permits, but does not require, a data provider to provide notice of the request or authorization to all joint account holders.

3.4.4 Method to Revoke Authorization

A data provider does not violate the final rule if it provides a reasonable method for a consumer to revoke a third party's authorization to access covered data, provided that such method does not violate the final rule's anti-evasion provision. Indicia that the data provider's revocation method is reasonable include its conformance to a consensus standard. A data provider that receives a revocation request from a consumer through a revocation method it makes available must revoke the authorized third party's access and notify the authorized third party of the request in a timely manner. 12 CFR 1033.331(e).

- The final rule does not permit data providers to give consumers the option to request partial revocations through the data provider's method to revoke authorization. The final rule only permits a data provider to provide a reasonable method for all-or-nothing revocations.

3.5 Requirement to Make Data Provider and Developer Interface Information Identifiable

A data provider must make the following information readily identifiable to members of the public in both human- and machine-readable formats:

- The data provider's legal name and, if applicable, any assumed name it is using while doing business with the consumer;
- A link to the data provider's website;
- The data provider's LEI;[6] and
- Contact information that enables a consumer or third party to receive answers to questions about accessing covered data.

12 CFR 1033.341(a) and (b).

A data provider also must make information about its developer interface readily identifiable to members of the public in both human- and machine-readable formats. Specifically, the data provider must make readily identifiable metadata describing all covered data and their corresponding data fields and other documentation sufficient for a third party to access and use its developer interface. However, a data provider is not required to make publicly available information that would impede its ability to deny a third party access to its developer interface consistent with the final rule's denial of access provision, which is discussed in Section 3.3. 12 CFR 1033.341(c).

> To be readily identifiable to members of the public, the information about the data provider, its developer interface, and its developer interface's performance must be at least as available as it would be on a public website. 12 CFR 1033.341(a)(1).

Indicia that documentation is sufficient for a third party to access and use a developer interface include conformance to a consensus standard. Additionally, the documentation must:

[6] The LEI must be issued by a utility endorsed by the LEI Regulatory Oversight Committee, or endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system.

- Be maintained and updated as reasonably necessary for third parties to access and use the interface in accordance with the terms to which data providers are subject under the final rule;
- Include how third parties can get technical support and report issues with the interface; and
- Be easy to understand and use, similar to data providers' documentation for other commercially available products.

12 CFR 1033.341(c).

Finally, a data provider must make certain information about its developer interface's performance readily identifiable to members of the public in both human- and machine-readable formats. On or before the final day of each calendar month, a data provider must make readily identifiable the response rate[7] that the data provider's developer interface achieved in the previous calendar month. This information must include at least a rolling 13 months of the required monthly figure.[8] The data provider must disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent."
12 CFR 1033.341(d).

> This approach does not require a data provider to maintain its own website for disclosures or bar multiple data providers from publishing their required disclosures in a single location, as long as the disclosures are at least as available as they would be on a public website. For example, the final rule does not preclude a data provider from posting the information described in this Section 3.5 in a central repository that is publicly available, and directing consumers and others to that central repository, for example through a link.

3.6 Required Policies and Procedures for Data Providers

A data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the final rule's objectives applicable to data providers. 12 CFR 1033.351(a). These policies and procedures must address:

[7] The response rate is described in 12 CFR 1033.311(c)(1) through (iv) and is discussed in Section 3.2.2.

[8] A data provider need not include the monthly figure for months prior to the date that the data provider is required to comply with the final rule.

1. *Making covered data available*. A data provider must have policies and procedures that are reasonably designed to ensure that the data provider creates a record of the data fields of covered data in the data provider's control or possession, the covered data that data provider does not make available through a consumer or developer interface pursuant to an exception in the final rule, and the reasons the exception applies. Indicia that a data provider's record of such data fields complies with these requirements include listing data fields that conform to those published by a consensus standard. 12 CFR 1033.351(b)(1).

2. *Denials of access to the data provider's developer interface*. The policies and procedures must be reasonably designed to ensure that, if the data provider denies a third party access to a developer interface, it creates a record substantiating the basis for denial and communicates the reasons for the denial to the third party. The policies and procedures must be reasonably designed to ensure that the data provider communicates the reasons for denial electronically or in writing and in a timely manner. 12 CFR 1033.351(b)(2).

- In limited cases, disclosure of the specific reason for a denial of access to an interface or for information might be prohibited by law, otherwise be inconsistent with compliance obligations, or hinder law enforcement. A data provider can design policies and procedures to avoid acting inconsistently with its other legal obligations, or in a way that could reasonably hinder law enforcement. 12 CFR 1033.351(a). For example, the final rule does not require a data provider to inform a third party that a "Suspicious Activity Report" was involved in a decision to deny information or interface access. However, the data provider must nonetheless create a record substantiating the basis for denial.

3. *Denials of requests for information*. A data provider's policies and procedures must be reasonably designed to ensure that, if the data provider denies a request for information for a reason described in 12 CFR 1033.331(c), it creates a record substantiating the basis for the denial and communicates the type(s) of information denied, if applicable, and the reasons for the denial to the third party or consumer. The policies and procedures must be reasonably designed to ensure that the data provider communicates the types of information and

- A data provider's policies and procedures need not provide for communicating what types of information are denied if the denial was made without regard to the availability of particular types of information, such as when requests are denied due to an inability to authenticate a consumer or third party.
- To the extent a data provider communicates a denial pursuant to a standardized communication protocol discussed in Section 3.2.2 (such as through a standardized error code), the data provider's policies and procedures do not need to separately address those aspects of the communication.

reasons for denial electronically or in writing and in a timely manner. 12 CFR 1033.351(b)(3).

4. *The accuracy of covered data provided through the data provider's developer interface.* A data provider's policies and procedures must be reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface. 12 CFR 1033.351(c)(1). In developing its policies and procedures regarding accuracy, a data provider must consider, for example, implementing the final rule's standardized format requirements and addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface. 12 CFR 1033.351(c)(2). Indicia that a data provider's policies and procedures regarding accuracy are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy. 12 CFR 1033.351(c)(3).

5. *Record retention*. The policies and procedures must be reasonably designed to ensure retention of records that are evidence of compliance with the final rule. 12 CFR 1003.351(d). The final rule specifies that the records retained pursuant to policies and procedures must include, without limitation:

    a. Records documenting requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable. A data provider must retain these records for at least three years after the data provider has responded to the request.

    b. Records providing evidence that the data provider has responded to requests for information, actions taken in response to such requests, and reasons for not making requested information available, if applicable. A data provider must retain these records for at least three years after the data provider has responded to the request.

    c. Records documenting that the third party has followed the final rule's authorization procedures to access data on behalf of a consumer. A data provider must retain these records for at least three years after they are generated.

    d. Records providing evidence of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation method made available by a data provider. A data provider must retain these records for at least three years after the revocation.

    e. Records providing evidence of the commercially reasonable performance of the data provider's developer interface. A data provider must retain these records for at least three years after the period recorded.

f. The written policies and procedures required under the final rule. A data provider must retain the written policies and procedures for three years from the time such material was last applicable.

g. Records of the information regarding the data provider and its developer interface that the data provider must make available to the public under the final rule. See Section 3.5 for discussion of this requirement. A data provider must retain these records for three years from the time such material was disclosed to the public. 12 CFR 1033.351(d)(2).

All other records that are evidence of compliance must be retained for a reasonable period of time of at least three years from the date of the action required under the final rule. 12 CFR 1033.351(d)(1).

A data provider's 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. A data provider must periodically review the policies and procedures and update them as appropriate to ensure their continued effectiveness. 12 CFR 1033.351(a).

3.7 Prohibition on Evasion

The final rule prohibits data providers from engaging in any action to evade or attempt to evade the final rule. Specifically, data providers must not take any action: (1) with the intent of evading the final rule's requirements; (2) that the data provider knows or should know is likely to render unusable the covered data that the data provider makes available; or (3) that the data provider knows or should know is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data consistent with the final rule. 12 CFR 1033.201(a)(2).

3.8 Compliance Dates

The final rule provides different compliance dates for data providers depending on their size and whether the data provider is a depository institution. 12 CFR 1033.121. For this purpose, a depository institution is any depository institution as defined by the Federal Deposit Insurance Act, 12 U.S.C. 1813(c)(1), or any credit union as defined by 12 CFR 700.2. 12 CFR 1033.131.

The dates on which depository institution data providers must begin complying with the final rule are discussed in Section 3.8.1. The dates on which data providers that are not depository institutions (i.e., nondepository institutions) must begin complying with the final rule are discussed in Section 3.8.2.

By their compliance date, data providers must have established functioning developer and consumer interfaces that are technically capable of complying with the final rule's requirements. For example, developer interfaces must be able to make all covered data available in a standardized format and be capable of performing in a commercially reasonable manner.

While the final rule does not allow a data provider to delay access to its interfaces unreasonably, it permits data providers to manage the process of onboarding third parties onto the developer interface in a staged manner. In managing the onboarding process, data providers are also subject to the final rule's anti-evasion provision and other applicable consumer financial laws, including the prohibition on unfair, deceptive, or abusive acts or practices. Once a third party has access to the developer interface, a data provider must respond to requests for covered data in accordance with the terms of the final rule.

3.8.1 Depository Institutions

If a data provider is a depository institution, its compliance date is based on its total assets calculated pursuant to the final rule. 12 CFR 1033.121(a)(1).

For purposes of determining compliance dates, total assets are determined by averaging the assets reported on the depository institution's 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter call report submissions to the FFIEC or 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. 12 CFR 1033.121(a)(1).

If, as a result of a merger or acquisition, a depository institution does not have the above-referenced four quarterly call report submissions, the depository institution uses the process set out in 12 CFR 1033.111(d)(3) to determine total assets. Under this provision, a depository institution combines the total assets reported on each of the call report submissions by all predecessor depository institutions for any of the four applicable quarters that are prior to the merger or acquisition. For quarters occurring after the merger or acquisition, the surviving depository institution uses the total assets reported on the quarterly call report submissions by the surviving depository institution. The surviving depository institution shall determine total assets by using the average of the total assets reported for the 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter submissions, whether the total assets are

the combined assets of the predecessor depository institutions or from the surviving depository institution. 12 CFR 1033.121(a)(1) and .111(d)(3).

Based on its total assets (calculated in the manner and for the time period described above), a depository institution must begin complying with the final rule on one of the following dates:

- *April 1, 2026*, for depository institutions that hold at least $250 billion in total assets
- *April 1, 2027*, for depository institutions that hold at least $10 billion in total assets but less than $250 billion in total assets
- *April 1, 2028*, for depository institutions that hold at least $3 billion in total assets but less than $10 billion in total assets.
- *April 1, 2029*, for depository institution data providers that hold at least $1.5 billion in total assets but less than $3 billion in total assets.
- *April 1, 2030*, for depository institution data providers that hold less than $1.5 billion in total assets but more than $850 million in total assets.

12 CFR 1033.121(b).

If a depository institution holds $850 million or less in total assets (calculated in the manner and for the time period described above), that depository institution does not meet the coverage threshold and is not subject to the final rule's requirements. However, if that depository institution subsequently holds total assets that exceed that SBA size standard, as discussed in Section 2.1, it must comply with the final rule within a reasonable amount of time after exceeding the size standard. A reasonable time shall not exceed five years. 12 CFR 1033.121(c).

3.8.2 Nondepository Institutions

If a data provider is a nondepository institution, its compliance date is based on the calculation of its total receipts for calendar years 2023 and 2024. Total receipts are calculated based on the SBA definition of receipts, as codified in 13 CFR 121.104(a). 12 CFR 1033.121(a)(2).

If a nondepository institution data provider generated $10 billion or more in total receipts in either calendar year 2023 or calendar year 2024, it must begin complying with the final rule by April 1, 2026. If a nondepository institution data provider did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024, it must begin complying by April 1, 2027. 12 CFR 1033.121(b).

4. Third Parties, Authorization Procedures, and Obligations

An authorized third party is a third party that seeks to access covered data on behalf of a consumer to provide a product or service that the consumer requested and that has satisfied the final rule's authorization procedures. These authorization procedures are discussed in Section 4.1.

- The product or service that the consumer requests from the third party need not be a covered consumer financial product or service.

As part of the authorization procedures, a third party must provide the consumer with an authorization disclosure that satisfies the final rule's requirements and certify that it agrees to the third party obligations described in the final rule. The requirements for the authorization disclosure are discussed in Section 4.2, and the third party obligations are discussed in Section 4.3.

The final rule permits a data aggregator to perform the authorization procedures on behalf of the third party seeking access to covered data. The final rule also contains provisions related to data aggregators that will assist authorized third parties with accessing covered data. The final rule's provisions regarding data aggregators are discussed in Section 4.4.

Finally, if a third party is also a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), it must have the written policies and procedures described in Section 4.5.

4.1 Authorization Procedures

To become an authorized third party, a third party must seek access to covered data on behalf of a consumer to provide a product or service that the consumer requested and must satisfy the following authorization procedures:

- Provide the consumer with an authorization disclosure that satisfies the final rule. The requirements for the authorization disclosure are discussed in Section 4.2.

- Under the final rule, a third party is 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.

- Provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to the third party obligations described in the final rule. These third party obligations are discussed in Section 4.3.
- 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.

12 CFR 1033.401.

4.2 Authorization Disclosure

As noted above, to satisfy the authorization procedures, a third party must provide an authorization disclosure to the consumer. The third party must provide the authorization disclosure electronically or in writing. The authorization disclosure must be clear, conspicuous, and segregated from other material. 12 CFR 1033.411(a).

The authorization disclosure must include:

1. *Name of the third party*. The authorization disclosure must include the name of the third party that the consumer would be authorizing to access covered data pursuant to the authorization procedures. The third party's name used in the authorization disclosure must be readily understandable to the consumer. 12 CFR 1033.411(a).

> When a third party is seeking access to covered data on behalf of a consumer that jointly holds an account, the third party must comply with the authorization procedures for the joint account holder on whose behalf the third party is requesting access. An authorization from a single account holder is sufficient for an authorized third party to access covered data. The final rule does not require that other joint account holders be notified or receive copies of the authorization disclosure.

2. *Data provider's name*. The authorization disclosure must include the name of the data provider that controls or possesses the covered data that the third party seeks to access on the consumer's behalf. This name must also be readily understandable to the consumer. 12 CFR 1033.411(a).
3. *Description of the requested product or service*. The authorization disclosure must include 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.

4. *Categories of data*. The authorization disclosure must include the categories of data that will be accessed. Categories must have a substantially similar level of specificity as the categories used to describe covered data in the final rule. These categories, which are discussed in Section 3.1.2, are transaction information, account balance information, payment initiation information, terms and conditions, upcoming bill information, and basic account verification information.

5. *Certification statement*. The authorization disclosure must include a statement to the consumer that the third party certifies that the third party agrees to the obligations described in 12 CFR 1033.421. These third party obligations are discussed in Section 4.3.

6. *Duration of data collection*. The authorization disclosure must include 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.

7. *Revocation method*. The authorization disclosure must include a description of a method that the consumer can use to revoke the third party's authorization. Section 4.3.6 discusses the third party obligations related to revocation.

12 CFR 1033.411(b).

The authorization disclosure must be in the same language as the communication in which the authorization disclosure is conveyed to the consumer. Any translation of the authorization disclosure provided to the consumer must be complete and accurate. 12 CFR 1033.411(c)(1). If the authorization disclosure is in a language other than English, it must include a link to an English-language translation and may include links to translations in other languages. If the authorization disclosure is in English, it may include links to translations in other languages. 12 CFR 1033.411(c)(2).

4.3 Third Party Obligations

As noted above, a third party must certify that it will satisfy certain obligations in order to become an authorized third party. This Section 4.3 discusses these obligations.

4.3.1 Limits on Collection, Use, and Retention of Covered Data

A third party must certify that it will limit its collection, use, and retention of covered data to what is reasonably necessary provide the product or service that the consumer requested from

the third party and that it will limit the duration of its collection of covered data to a maximum period of one year after the consumer's most recent authorization. 12 CFR 1033.421.

Reasonably Necessary to Provide the Consumer's Requested Product or Service

The third party must certify that it will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. 12 CFR 1033.421(a)(1) and (b).

> The final rule's limitation on use applies only to covered data. It does not affect how third parties may use data they generate in the course of providing their products or services to consumers.

For the purposes of this general limitation, targeted advertising, cross-selling of other products or services, and the sale of covered data are not part of, or reasonably necessary to provide, any other product or service. 12 CFR 1033.421(a)(2). The final rule does not prevent third parties from obtaining authorizations from a consumer to collect, use, and retain their covered data for any one of these specified purposes if offered as a standalone product or service. To the extent that the consumer seeks a product or service in the market which functions as targeted advertising, cross-selling of other products or services, or the sale of covered data, a third party could obtain a consumer's authorization to collect, use, and retain their covered data to provide that product or service to the consumer consistent with, and subject to the final rule. Collection, use, and retention of covered data to provide such a product or service would be subject to other applicable laws, including the Act's prohibition on unfair, deceptive, and abusive practices.

To be a "standalone" product or service, it must be clear that the targeted advertising, cross-selling, or sale of covered data is a distinct product or service the consumer could obtain in the market without obtaining other products or services. One provider could offer multiple products to a consumer, including the activities described as targeted advertising, cross-selling, or sale of covered data as standalone products, obtain separate authorizations for consumer's data to be used for those products or services, and provide both those products and services to the consumer.

Examples of uses of covered data that are permitted under the general limitation on collection, use, and retention include:

- Uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority;

- Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- Servicing or processing the product or service the consumer requested; and
- Uses that are reasonably necessary to improve the product or service the consumer requested.

12 CFR 1033.421(c).

For purposes of the final rule's limitation on use, use of covered data includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. 12 CFR 1033.421(c). See also the discussion in Section 4.3.4 regarding sharing covered data with other third parties.

> In some circumstances, an authorized third party might receive from the data provider more data than it requested or receive data after a consumer has revoked the third party's authorization, but before the data provider has processed the revocation. In circumstances where the third party receives more covered data than it requested or received covered data after a consumer has revoked their authorization, the general limitation on use and retention does not allow the third party to use that covered data if such use is not reasonably necessary. The final rule allows a third party to retain that covered data for as long as reasonably necessary to locate and delete the covered data.

Duration of Collection

In addition to the general limitation set forth above, the third party must also certify that it will limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization. 12 CFR 1033.421(b)(2). To collect covered data beyond the one-year maximum period, the third party must obtain a new authorization from the consumer pursuant to the authorization procedures described in 12 CFR 1033.401 (these are discussed in Section 4.1) no later than the anniversary of the consumer's most recent authorization. The third party is permitted to ask the consumer for a new authorization in a reasonable manner. Indicia that a third party has requested a new authorization in a reasonable manner include the third party's conformance to a consensus standard. 12 CFR 1033.421(b)(3).

If a consumer does not provide a new authorization by the anniversary of the consumer's most recent authorization, the third party will:

- No longer collect covered data pursuant to the most recent authorization; and
- No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

12 CFR 1033.421(i).

4.3.2 Written Policies and Procedures Reasonably Designed to Ensure Accuracy

A third party must certify that it will establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and, if applicable, accurately provided to another third party. 12 CFR 1033.421(d). A third party must also certify that it will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. 12 CFR 1033.421(d)(2).

While a third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, it must consider, for example, accepting covered data in a standardized format and addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data. 12 CFR 1033.421(d)(1) and (3).

Indicia that a third party's policies and procedures regarding accuracy are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy. 12 CFR 1033.421(d)(4).

4.3.3 Applying an Information Security Program

A third party must certify that it will apply to its systems for the collection, use, and retention of covered data either:

- An information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA (15 U.S.C. 6801); or
- If the third party is not subject to section 501 of the GLBA, the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

12 CFR 1033.421(e).

4.3.4 Providing Covered Data to Other Third Parties

A third party must certify that, before it provides covered data to another third party, it will require the other third party by contract to comply with the third party obligations set forth in the final rule and discussed in this Section 4.3, except the obligations related to ensuring consumers are informed about the authorized third party's access to covered data, which are set forth in 12 CFR 1033.421(g) and discussed in Section 4.3.5. 12 CFR 1033.421(f).

- Under the general limit on collection, use, and retention, an authorized third party is able to share covered data with other third parties only as reasonably necessary to provide the product or service requested by the consumer from the authorized third party. Accordingly, downstream third parties will be able to use covered data only to assist the authorized third party with providing the requested product or service and not for their own purposes.

As part of these certifications, a downstream third party must certify that, before providing covered data to another third party, it will require that third party by contract to comply with these same obligations. 12 CFR 1033.421(f).

4.3.5 Ensuring Consumers are Informed about Data Access

The third party must certify that, upon obtaining authorization to access covered data on the consumer's behalf, it 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 deliver that copy to the consumer or make it available in a location that is readily accessible to the consumer, such as the third party's interface. If the third party makes the authorization disclosure available in such a location, the third party will ensure it is accessible to the consumer until the third party's access to the consumer's covered data terminates.
12 CFR 1033.421(g)(1).

The third party must also certify that it will provide the consumer with contact information that enables the consumer to receive answers to questions about the third party's access to the consumer's covered data. The contact information must be readily identifiable to the consumer.
12 CFR 1033.421(g)(2).

- If its existing customer service function is equipped to address questions about the third party's access to the consumer's covered data, the third party may satisfy the final rule's obligation to provide contact information by providing contact information for its existing customer service function.

Finally, the third party must certify that it will establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon

request, the information listed below about the third party's access to the consumer's covered data:

- Categories of covered data collected;
- Reasons for collecting the covered data;
- Names of parties with which the covered data was shared. The names must be readily understandable to the consumer;
- Reasons for sharing the covered data;
- Status of the third party's authorization;
- How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation; and
- A copy of any data aggregator certification statement that was provided to the consumer pursuant to the final rule.

The third party must certify that it will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. The third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities. 12 CFR 1033.421(g)(3).

4.3.6 Revocation of Third Party Authorization

The third party must certify that it will provide the consumer with a method to revoke the third party's authorization to access the consumer's covered data. The revocation method must be as easy to access and operate as the initial authorization. The third party must also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization. 12 CFR 1033.421(h)(1). The third party must certify that, if a consumer uses this revocation method, the third party will notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer's covered data when the third party receives a revocation request from a consumer. 12 CFR 1033.421(h)(2).

> For revocation of authorization to be free of cost or penalties, consumers should be able to revoke their authorization to data access for purposes of one product or service but maintain that same third party's data access for purposes of another product or service they are receiving from the third party. In other words, third parties conditioning the provision of one product or service on the consumer providing consent to data access for another product or service is a cost or penalty on the consumer.

Additionally, the third party must certify that, if it receives a revocation request from a consumer or notice of a consumer's revocation request, such as from a data provider, a third party will:

- No longer collect covered data pursuant to the most recent authorization; and
- No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

12 CFR 1033.421(i).

4.4 Data Aggregators

Under the final rule, a data aggregator is a person that is retained by and provides services to the authorized third party to enable access to covered data. 12 CFR 1033.131. A data aggregator is permitted to perform the authorization procedures described in 12 CFR 1033.401 (and discussed in Section 4.1) on behalf of the third party seeking authorization to access covered data. However, the third party seeking authorization remains responsible for compliance with the authorization procedures. 12 CFR 1033.431(a).

- A data aggregator can only collect, use, and retain the consumer's covered data as reasonably necessary to provide the product or service the consumer requested from the authorized third party.
- If the data aggregator is performing authorization procedures for multiple third parties, it must perform the authorization procedures separately for each third party, even if the third parties are seeking authorization from the same consumer.

The third party's authorization disclosure must include the name of the data aggregator that will assist the third party with accessing covered data and a brief description of the services the data aggregator will provide. 12 CFR 1033.431(b). The name of any data aggregator in the authorization disclosure must be readily understandable to the consumer. 12 CFR 1033.411(a).

Before accessing the consumer's data, the data aggregator must certify to the consumer that it agrees to the third party obligations set forth in the final rule and discussed in Section 4.3, except the obligations related to ensuring consumers are informed about the authorized third party's access to covered data, which are set forth in 12 CFR 1033.421(g) and discussed in Section 4.3.5. 12 CFR 1033.431(c).

Pursuant to the condition on accessing covered data in 12 CFR 1033.421(i), the data aggregator must certify that, if a consumer does not provide a new authorization by the most recent authorization's anniversary date or if the aggregator receives notice of a consumer's revocation request, it will:

> The final rule does not require a data aggregator to certify that it will provide consumers with a revocation method. However, data aggregators are permitted to provide a revocation method if they choose to do so.

- No longer collect covered data pursuant to the most recent authorization; and
- No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

Either the third party can include the data aggregator's certification in the third party's authorization disclosure, or the data aggregator can separately provide its certification to the consumer, electronically or in writing. If the data aggregator provides its certification to the consumer separately, the certification must be in the same language as the third party's authorization disclosure and must be clear, conspicuous, and segregated from other material. 12 CFR 1033.431(c). The name of the data aggregator in the certification must be readily understandable to the consumer. 12 CFR 1033.411(a). If an authorized third party retains a data aggregator after completing the authorization procedures, the data aggregator must separately provide its certification to the consumer. 12 CFR 1033.431(c)(2).

4.5 Third Party Policies and Procedures for Record Retention

A third party that is a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with subpart D of the final rule (the provisions of the final rule related to authorized third parties). 12 CFR 1033.441(a). A third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities. 12 CFR 1033.441(c). Records retained pursuant to the third party's policies and procedures must include at least the following:

- A copy of the authorization disclosure that is signed by the consumer electronically or in writing and reflects the date of the consumer's signature and a record of actions taken by the consumer, including actions taken through a data provider or another third party, to revoke the third party's authorization; and

- With respect to a data aggregator that is a covered person or service provider, as defined in 15 U.S.C. 5481(6) and (26), a copy of any data aggregator certification statement that was provided to the consumer separately from the third party's authorization disclosure.

12 CFR 1033.441(e).

Records must be retained for a reasonable period of time, not less than three years after a third party obtains the consumer's most recent authorization. 12 CFR 1033.441(b).

A third party that is a covered person or service provider as defined in 12 U.S.C. 5481(6) and (26) must periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness to evidence compliance with subpart D of the final rule. 12 CFR 1033.441(d).

5. Standard Setting Bodies and Consensus Standards

In some instances, the final rule states that conformance with an applicable consensus standard provides indicia of compliance with a specified provision in the final rule. For example, as discussed in Section 3.2.2, the final rule requires a developer interface to make covered data available in a standardized and machine-readable format and states that conformance with a consensus standard is indicia that the format satisfies this requirement. See 12 CFR 1033.311(b).

> Conformance to a consensus standard is not required to comply with any provision of the final rule and does not constitute compliance with any specified provision. Furthermore, the final rule does not require a data provider or third party to comply with any consensus standard.

For this purpose, consensus standard means a standard that is adopted by a recognized standard setter and that continues to be maintained by that recognized standard setter. Additionally, a recognized standard setter is a standard-setting body that has been recognized by the CFPB pursuant to the final rule. 12 CFR 1033.131.

A standard-setting body may request CFPB recognition. A guide for requesting recognition is available at https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights-industry-standard-setting/. If approved, recognition will last up to five years, absent revocation. The CFPB will not recognize a standard-setting body unless it demonstrates that it satisfies the following attributes:

1. *Openness*. The sources, procedures, and processes used are open to all interested parties, including consumer and other public interest groups with expertise in consumer protection, financial services, community development, fair lending, and civil rights; authorized third parties; data providers; data recipients; data aggregators and other providers of services to authorized third parties; and relevant trade associations. Parties can meaningfully participate in standards development on a non-discriminatory basis.

2. *Balance*. The decision-making power is balanced across all interested parties, including consumer and other public interest groups, and is reflected at all levels of the standard-setting body. There is meaningful representation for large and small commercial entities within these categories. No single interest or set of interests dominates decision-making. Achieving balance requires recognition that, even when a participant may play multiple roles, such as data provider and authorized third party, the weight of that participant's

commercial concerns may align primarily with one set of interests. The ownership of participants is considered in achieving balance.

3. *Due process and appeals*. The standard-setting body uses documented and publicly available policies and procedures, and it provides adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views. An appeals process is available for the impartial handling of procedural appeals.

4. *Consensus*. Standards development proceeds by consensus, which is defined as general agreement, though not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

5. *Transparency*. Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

12 CFR 1033.141.