PART 1001—FINANCIAL PRODUCTS OR SERVICES

1. The authority citation for part 1001 continues to read as follows:

Authority: 12 U.S.C. 5481(15)(A)(xi); and 12 U.S.C. 5512(b)(1).

2. Amend § 1001.2 by revising paragraph (b) and adding reserved paragraph (c) to read as follows:

§ 1001.2 Definitions.

* * * * *

(b) Providing financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service, where the financial data processing is not offered or provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person.

(c) [Reserved].

3. Revise part 1033 to read as follows:

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

SUBPART A—GENERAL

Sec.
1033.101 Authority, purpose, and organization.
1033.111 Coverage of data providers.
1033.121 Compliance dates.
1033.131 Definitions.
1033.141 Standard-setting bodies.

SUBPART B—MAKING COVERED DATA AVAILABLE

1033.201 Availability and prohibition against evasion.
1033.211 Covered data.
1033.221 Exceptions.

1 This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

1033.301 General requirements.
1033.311 Requirements applicable to developer interface.
1033.321 Interface access.
1033.331 Responding to requests for information.
1033.341 Information about the data provider.
1033.351 Policies and procedures.

SUBPART D—AUTHORIZED THIRD PARTIES

1033.401 Third party authorization; General.
1033.411 Authorization disclosure.
1033.421 Third party obligations.
1033.431 Use of data aggregator.
1033.441 Policies and procedures for third party record retention.

APPENDIX A TO PART 1033-PERSONAL FINANCIAL DATA RIGHTS RULE: HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

Authority: 12 U.S.C. 5512; 12 U.S.C. 5514; 12 U.S.C. 5533.

SUBPART A—GENERAL

§ 1033.101 Authority, purpose, and organization.

(a) *Authority*. The regulation in this part is issued by the Consumer Financial Protection Bureau (CFPB) pursuant to the Consumer Financial Protection Act of 2010 (CFPA), Pub. L. 111-203, tit. X, 124 Stat. 1955.

(b) *Purpose*. This part implements the provisions of section 1033 of the CFPA by requiring data providers to make available to consumers and authorized third parties, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service, in an electronic form usable by consumers and authorized third parties; and by prescribing standards to promote the development and use of standardized formats for covered data, including through industry standards developed by standard-setting bodies recognized by the CFPB. This part also sets forth obligations of third parties that would

 This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

access covered data on a consumer's behalf, including limitations on their collection, use, and retention of covered data.

(c) *Organization*. This part is divided into subparts as follows:

(1) Subpart A establishes the authority, purpose, organization, coverage of data providers, compliance dates, and definitions applicable to this part.

(2) Subpart B provides the general obligation of data providers to make covered data available upon the request of a consumer or authorized third party, including what types of information must be made available.

(3) Subpart C provides the requirements for data providers to establish and maintain interfaces to receive and respond to requests for covered data.

(4) Subpart D provides the obligations of third parties that would access covered data on behalf of a consumer.

(5) Appendix A provides instructions for how a standard-setting body would apply for CFPB recognition.

§ 1033.111 Coverage of data providers.

(a) *Coverage of data providers.* A data provider has obligations under this part if it controls or possesses covered data concerning a covered consumer financial product or service that the consumer obtained from the data provider, subject to the exclusion in paragraph (d) of this section.

(b) *Definition of covered consumer financial product or service*. *Covered consumer financial product or service* means a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is:

This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

(1) A *Regulation E account*, which means an account, as defined in Regulation E, 12 CFR 1005.2(b);

(2) A *Regulation Z credit card*, which means a credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i); or

(3) Facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments. For purposes of this part, 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.

(c) *Definition of data provider*. *Data provider* means a covered person, as defined in 12 U.S.C. 5481(6), that is:

(1) A *financial institution*, as defined in Regulation E, 12 CFR 1005.2(i);

(2) A *card issuer*, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or

(3) Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.

Example 1 to paragraph (c): A digital wallet provider is a data provider.

(d) *Coverage threshold—Certain depository institutions*. The requirements of subparts B and C do not apply to data providers defined under § 1033.111(c)(1) through (3) that are depository institutions that hold total assets equal to or less than the SBA size standard, as determined in accordance with this paragraph (d). If at any point a depository institution that held total assets greater than that SBA size standard as of or at any point after **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]** subsequently holds total assets below that amount, the requirements of subparts B and C continue to apply.

(1) *Determining SBA size standard*. For purposes of paragraph (d) of this section, the SBA size standard is the SBA size standard for the data provider's 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.

(2) *Calculating total assets*. For purposes of paragraph (d) of this section, total assets held by a depository institution are determined by averaging the assets reported on its own four preceding quarterly call report submissions to the Federal Financial Institutions Examination Council or National Credit Union Association, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the Federal Financial Examination Council or National Credit Union Administration.

(3) *Merger or acquisition—coverage of surviving depository institution when there are not four quarterly call report submissions*. After a merger or acquisition the surviving depository institution shall determine quarterly assets prior to the merger or acquisition by using the combined assets reported on the quarterly call report submissions by all predecessor depository institutions. The surviving depository institution shall determine quarterly assets after the merger or acquisition 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 quarterly assets for the four preceding quarters, whether the quarterly assets are the combined assets of the predecessor depository institutions or from the surviving depository institution.

§ 1033.121 Compliance dates.

(a) *Determining assets and revenue for purposes of initial compliance dates*. A data provider's compliance date in paragraph (b) of this section is based on the calculation of total assets or total receipts, as appropriate, described in paragraphs (a)(1) and (2) of this section.

 This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

(1) With respect to a depository institution data provider, total assets are determined by averaging the assets reported on its 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter call report submissions to the Federal Financial Institutions Examination Council or National Credit Union Administration, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the Federal Financial Examination Council or National Credit Union Administration. If, as a result of a merger or acquisition, a depository institution data provider does not have the named four quarterly call report submissions, the depository institution data provider shall use the process set out in § 1033.111(d)(3) to determine total assets for the time period named in this paragraph (a)(1).

(2) With respect to a nondepository institution data provider, total receipts are calculated based on the SBA definition of receipts, as codified in 13 CFR 121.104(a).

(b) *Initial compliance dates*. A data provider defined under § 1033.111(c)(1) through (3) must comply with the requirements in subparts B and C beginning on:

(1) April 1, 2026, for depository institution data providers that hold at least $250 billion in total assets and nondepository institution data providers that generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024.

(2) April 1, 2027, for data providers that are:

(i) Depository institutions that hold at least $10 billion in total assets but less than $250 billion in total assets; or

(ii) Nondepository institutions that did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024.

(3) April 1, 2028, for depository institution data providers that hold at least $3 billion in total assets but less than $10 billion in total assets.

(4) 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.

(5) 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.

(c) *Compliance dates for depository institution data providers that subsequently cross coverage threshold*. A depository institution data provider under § 1033.111(c)(1) through (3) that has total assets as calculated in § 1033.111(d)(2) equal to or less than the SBA size standard as determined in accordance with § 1033.111(d)(1), but that subsequently holds total assets that exceed that SBA size standard, as measured in § 1033.111(d)(2), must comply with the requirements in subparts B and C within a reasonable amount of time after exceeding the size standard, not to exceed five years.

§ 1033.131 Definitions.

For purposes of this part, the following definitions apply:

Authorized third party means a third party that has complied with the authorization procedures described in § 1033.401.

Card issuer is defined at § 1033.111(c)(2).

Consensus standard means a standard that is adopted by a recognized standard setter and that continues to be maintained by that recognized standard setter.

Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition. *Consumer* also includes guardians,

This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

trustees, custodians, or other similar natural persons acting on behalf of a consumer pursuant to State law.

Consumer interface means an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers in response to the requests.

Covered consumer financial product or service is defined at § 1033.111(b).

Covered data is defined at § 1033.211.

Data aggregator means a person that is retained by and provides services to the authorized third party to enable access to covered data.

Data provider is defined at § 1033.111(c).

Depository institution means 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.

Developer interface means an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by authorized third parties in response to the requests.

Financial institution is defined at § 1033.111(c)(1).

Recognized standard setter means a standard-setting body that has been recognized by the CFPB under § 1033.141.

Regulation E account is defined at § 1033.111(b)(1).

Regulation Z credit card is defined at § 1033.111(b)(2).

Third party means 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.

§ 1033.141 Standard-setting bodies.

(a) *Recognition of a standard-setting body*. A standard-setting body may request CFPB recognition. 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.

SUBPART B—MAKING COVERED DATA AVAILABLE

§ 1033.201 Availability and prohibition against evasion.

(a) *Obligation to make covered data available*—(1) *General*. A data provider must make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties.

(2) *Prohibition against evasion*. A data provider must not take any action:

(i) With the intent of evading the requirements of subparts B and C of this part;

(ii) That the data provider knows or should know is likely to render unusable the covered data that the data provider makes available; or

(iii) 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 this part.

(b) *Current data*. In complying with paragraph (a) of this section, 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. A data provider must make available information concerning authorized but not yet settled transactions.

§ 1033.211 Covered data.

Covered data in this part means, as applicable:

(a) Transaction information, including historical transaction information in the control or possession of the data provider. A data provider is deemed to make available sufficient historical transaction information for purposes of § 1033.201(a)(1) if it makes available at least 24 months of such information.

Example 1 to paragraph (a): This category includes amount, transaction date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.

(b) Account balance information.

(c) 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 Clearing House transaction.

(1) In complying with its obligation under § 1033.201(a)(1), a data provider is permitted to make available a tokenized account number instead of, or in addition to, a non-tokenized account number, as long as the tokenization is not used as a pretext to restrict competitive use of payment initiation information.

(2) This paragraph (c) does not apply to data providers who do not directly or indirectly hold the underlying Regulation E account. 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.

(d) Terms and conditions. For purposes of this section, 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 is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

Example 1 to paragraph (d): 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.

(e) Upcoming bill information.

Example 1 to paragraph (e): 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.

(f) Basic account verification information, which 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 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.

§ 1033.221 Exceptions.

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

(a) Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. Information 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.

(b) 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. Information 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.

(c) Any information required to be kept 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.

(d) Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

§ 1033.301 General requirements.

(a) *Requirement to maintain interfaces*. A data provider subject to the requirements of this part must maintain a consumer interface and a developer interface. The consumer interface and the developer interface must satisfy the requirements set forth in this section. The developer interface must satisfy the additional requirements set forth in § 1033.311.

(b) *Machine-readable files upon request*. Upon request for covered data in a machine-readable file, and subject to paragraphs (b)(1) and (2) of this section, a data provider must make available to a consumer or an authorized third party covered data 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.

(1) *Consumer interface*. With respect to covered data provided through its consumer interface, a data provider is not required to comply with:

(i) The requirements of this paragraph (b) for the covered data described in § 1033.211(c) (payment initiation information) and (f) (account verification information); and

This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

(ii) The requirement of this paragraph (b) to provide in a file that is machine-readable the covered data described in § 1033.211(d) (terms and conditions).

(2) *Developer interface.* With respect to covered data provided through its developer interface, a data provider satisfies the requirements of this paragraph (b) if it makes available covered data in a form that satisfies the requirements of § 1033.311(b).

(c) *Fees prohibited.* A data provider must not impose any fees or charges on a consumer or an authorized third party in connection with:

(1) *Interfaces*. Establishing or maintaining the interfaces required by paragraph (a) of this section; or

(2) *Requests*. Receiving requests or making available covered data in response to requests as required by this part.

§ 1033.311 Requirements applicable to developer interface.

(a) *General.* A developer interface required by § 1033.301(a) must satisfy the requirements set forth in this section.

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

(1) *Meaning of format.* For purposes of this section, *format* includes structures and definitions of covered data and requirements and protocols for communicating requests and responses for covered data.

(2) *Meaning of standardized.* For purposes of this section, *standardized* means conforms to a format widely used by other data providers and designed to be readily usable by authorized third parties.

(c) *Commercially reasonable performance.* A developer interface's performance must be commercially reasonable.

(1) *Response rate; quantitative minimum performance specification*. The performance of the interface cannot be commercially reasonable if it does not meet the following quantitative minimum performance specification regarding its response rate: The number of proper responses by the interface divided by the total number of requests for covered data to the interface must be equal to or greater than 99.5 percent in each calendar month. For purposes of this paragraph (c)(1), all of the following requirements apply:

(i) 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.

(ii) 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.

(iii) 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.

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

(A) The response either fulfills the request or explains why the request was not fulfilled;

(B) The response is consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a); and

(C) 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.

(2) *Indicia of compliance*—(i) *Indicia*. Indicia that a developer interface's performance is commercially reasonable as required by paragraph (c) of this section include:

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

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

(C) How the interface's performance compares to the performance levels achieved by the data provider's consumer interface.

(ii) *Performance specifications*. For each of the three indicia set forth in paragraph (c)(2)(i) of this section, relevant performance specifications include:

(A) The interface's response rate as defined in paragraphs (c)(1) through (c)(1)(iv) of this section;

(B) The interface's total amount of scheduled downtime;

(C) The amount of time in advance of any scheduled downtime by which notice of the downtime is provided;

(D) The interface's total amount of unscheduled downtime; and

(E) The interface's response time.

(d) *Access caps*. Except as otherwise permitted by §§ 1033.221, 1033.321, and 1033.331(b) and (c), 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 § 1033.351(a). Indicia that any frequency restrictions applied are reasonable include that they conform to a consensus standard.

(e) *Security specifications*—(1) *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. A contract between a data provider and the data provider's service provider, pursuant to which the service provider establishes or maintains the data provider's developer interface, does not violate this paragraph if the contract provides that the service provider will make covered data available, in a form and manner that satisfies the requirements of this part, 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.

(2) *Security program.* (i) A data provider must apply to the developer interface an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

(ii) If the data provider is not subject to section 501 of the Gramm-Leach-Bliley Act, the data provider must apply to its developer interface the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

 This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

§ 1033.321 Interface access.

(a) *Denials related to risk management*. A data provider does not violate the general obligation in § 1033.201(a)(1) by denying a consumer or third party access to all elements of the interface described in § 1033.301(a) if:

(1) granting access would be inconsistent with policies and procedures reasonably designed to comply with:

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

(ii) information security standards required by section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

(iii) other applicable laws and regulations regarding risk management; and

(2) the denial is reasonable pursuant to paragraph (b).

(b) *Requirements for reasonable denials.* A denial is reasonable pursuant to paragraph (a)(2) of this section if it is:

(1) Directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security; and

(2) Applied in a consistent and non-discriminatory manner.

(c) *Indicia bearing on reasonable denials.* Indicia bearing on the reasonableness of a denial pursuant to paragraph (b) of this section include:

(1) Whether the denial adheres to a consensus standard related to risk management;

(2) Whether the denial proceeds from standardized risk management criteria that are available to the third party upon request; and

(3) Whether 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.

(d) *Conditions sufficient to justify a denial*. Each of the following is a sufficient basis for denying access to a third party:

(1) The third party does not present any evidence that its information security practices are adequate to safeguard the covered data; or

(2) The third party does not make the following information available in both human-readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website:

(i) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(ii) A link to its website;

(iii) Its Legal Entity Identifier (LEI) that is issued by:

(A) A utility endorsed by the LEI Regulatory Oversight Committee, or

(B) A utility 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; and

(iv) Contact information a data provider can use to inquire about the third party's information security and compliance practices.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers*. To comply with the requirements in § 1033.201(a)(1), upon request from a consumer, a data provider must make available covered data when it receives information sufficient to:

(1) Authenticate the consumer's identity; and

(2) Identify the scope of the data requested.

(b) *Responding to requests—access by third parties.* (1) To comply with the requirements in § 1033.201(a)(1), upon request from an authorized third party, a data provider must make available covered data when it receives information sufficient to:

(i) Authenticate the consumer's identity;

(ii) Authenticate the third party's identity;

(iii) Document the third party has followed the authorization procedures in § 1033.401; and

(iv) Identify the scope of the data requested.

(2) 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:

(i) The account(s) to which the third party is seeking access; and

(ii) The categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to § 1033.411(b)(4).

Example 1 to paragraph (b): An authorized third party that a data provider has authenticated requests covered data on behalf of an authenticated consumer through the data provider's developer interface. The data provider asks the consumer to confirm the scope of the third party's authorization using a means of communication that the consumer is not accustomed to using with the data provider and that the data provider knows or should know will take a long period of time to reach the consumer and allow the consumer to respond with the confirmation. As a result of the long wait time, the consumer cannot provide a timely confirmation, delaying the third party's access to the covered data. This data provider has violated the § 1033.201(a)(2) prohibition against evasion by taking an action that the data provider knows or should know is likely to interfere with an authorized third party's access to covered data.

(c) *Covered data not required to be made available.* A data provider is not required to make covered data available in response to a request when:

(1) The data are withheld because an exception described in § 1033.221 applies;

(2) The data are not in the data provider's control or possession, consistent with the requirement in § 1033.201(a)(1).

(3) The data provider's interface is not available when the data provider receives a request requiring a response under this section. However, the data provider is subject to the performance specifications in § 1033.311(c);

(4) The request is for access by a third party; and

(i) The consumer has revoked the third party's authorization pursuant to paragraph (e) of this section;

(ii) The data provider has received notice that the consumer has revoked the third party's authorization pursuant to § 1033.421(h)(2); or

(iii) The consumer has not provided a new authorization to the third party after the maximum duration period, as described in § 1033.421(b)(2).

(5) The data provider has not received information sufficient to satisfy the conditions in § 1033.331(a) or (b).

(d) *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 this section.

(e) *Method to revoke third party authorization to access covered data.* A data provider does not violate the general obligation in § 1033.201(a)(1) by making available to the consumer a reasonable method to revoke any third party's authorization to access all of the consumer's covered data, provided that such method does not violate § 1033.201(a)(2). 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.

§ 1033.341 Information about the data provider.

(a) *Requirement to make information about the data provider readily identifiable*. A data provider must make the information described in paragraphs (b) through (d) of this section:

(1) Readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website; and

(2) Available in both human-readable and machine-readable formats.

(b) *Identifying information*. A data provider must disclose in the manner required by paragraph (a) of this section:

(1) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(2) A link to its website;

(3) Its LEI that is issued by:

(i) A utility endorsed by the LEI Regulatory Oversight Committee, or

(ii) A utility 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; and

(4) Contact information that enables a consumer or third party to receive answers to questions about accessing covered data under this part.

(c) *Developer interface documentation*. For its developer interface, a data provider must disclose in the manner required by paragraph (a) of this section documentation, including

metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface. 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 § 1033.321. Indicia that documentation is sufficient for a third party to access and use a developer interface include conformance to a consensus standard. The documentation must:

(1) 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 this part;

(2) Include how third parties can get technical support and report issues with the interface; and

(3) Be easy to understand and use, similar to data providers' documentation for other commercially available products.

(d) *Performance disclosure*. On or before the final day of each calendar month, a data provider must disclose in the manner required by paragraph (a) of this section the quantitative minimum performance specification for the response rate described in § 1033.311(c)(1)(i) through (iv) that the data provider's developer interface achieved in the previous calendar month. The data provider's disclosure must include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The data provider must disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent."

§ 1033.351 Policies and procedures.

(a) *Reasonable written policies and procedures*. A data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the objectives

set forth in subparts B and C of this part, including paragraphs (b) through (d) of this section. 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 required by this section and update them as appropriate to ensure their continued effectiveness.

(b) *Policies and procedures for making covered data available.* The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:

(1) *Making available covered data.* A data provider creates a record of the data fields of covered data in the data provider's control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reasons the exception applies. Indicia that a data provider's record of such data fields complies with the requirements of this paragraph include listing data fields that conform to those published by a consensus standard.

(2) *Denials of developer interface access.* When a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider:

(i) Creates a record substantiating the basis for denial; and

(ii) Communicates in a timely manner to the third party, electronically or in writing, the reason(s) for the denial.

(3) *Denials of information requests.* When a data provider denies a request for information for a reason described in § 1033.331(c), to the extent the communication of the denial is not required to be standardized by § 1033.311(b), the data provider:

(i) Creates a record substantiating the basis for the denial; and

(ii) Communicates in a timely manner to the consumer or third party, electronically or in writing, the type(s) of information denied, if applicable, and the reason(s) for the denial.

(c)(1) *Policies and procedures for ensuring accuracy*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface.

(2) *Elements.* In developing its policies and procedures regarding accuracy, a data provider must consider, for example:

(i) Implementing the format requirements of § 1033.311(b); and

(ii) Addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface.

(3) *Indicia of compliance.* 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.

(d) *Policies and procedures for record retention*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part.

(1) *Retention period*. Records that are evidence of a data provider's actions in response to a consumer's or third party's request for information or a third party's request to access a developer interface must be retained for at least three years after a data provider has responded to the request. All other records that are evidence of compliance with subparts B and C of this part must be retained for a reasonable period of time of at least three years from the date of the action required under subparts B and C of this part.

25 This is an unofficial version of the regulatory text. If any conflicts exist between this version and the version published in the *Federal Register*, the latter is the controlling document.

(2) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under paragraph (a) of this section must include, without limitation:

(i) 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, for at least three years after the data provider has responded to the request;

(ii) Records providing evidence of fulfillment of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable, for at least three years after the data provider has responded to the request;

(iii) Records documenting that the third party has followed the authorization procedures in § 1033.401 to access data on behalf of a consumer, for at least three years after such records are generated;

(iv) 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, for at least three years after the revocation;

(v) Records providing evidence of commercially reasonable performance described in § 1033.311(c)(2)(C)(ii), for at least three years after the period recorded;

(vi) Written policies and procedures required under § 1033.351 for three years from the time such material was last applicable; and

(vii) Disclosures required under § 1033.341, for three years from the time such material was disclosed to the public.

SUBPART D—AUTHORIZED THIRD PARTIES

§ 1033.401 Third party authorization; General.

To become an authorized third party, the third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested and:

(a) Provide the consumer with an authorization disclosure as described in § 1033.411;

(b) Provide a statement to the consumer in the authorization disclosure, as provided in § 1033.411(b)(5), certifying that the third party agrees to the obligations described in § 1033.421; and

(c) 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.

§ 1033.411 Authorization disclosure.

(a) *In general.* To comply with § 1033.401(a), a third party must provide the consumer with an authorization disclosure electronically or in writing. The authorization disclosure must be clear, conspicuous, and segregated from other material. The names included in the authorization disclosure as required by paragraphs (b)(1) and (2) of this section and by § 1033.431(b) must be readily understandable to the consumer.

(b) *Content.* The authorization disclosure must include:

(1) The name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures in § 1033.401.

(2) The name of the data provider that controls or possesses the covered data that the third party identified in paragraph (b)(1) of this section seeks to access on the consumer's behalf.

(3) A brief description of the product or service the consumer has requested from the third party identified in paragraph (b)(1) of this section 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) The categories of data that will be accessed. Categories must have a substantially similar level of specificity as the categories in § 1033.211.

(5) The certification statement described in § 1033.401(b).

(6) 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) A description of the revocation method described in § 1033.421(h)(1).

(c) *Language access*—(1) *In general.* 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.

(2) *Additional languages.* If the authorization disclosure is in a language other than English, it must include a link to an English-language translation, and it is permitted to include links to translations in other languages. If the authorization disclosure is in English, it is permitted to include links to translations in other languages.

§ 1033.421 Third party obligations.

(a) *General limitation on collection, use, and retention of consumer data*—(1) *In general*. The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.

(2) *Specific purposes*. For purposes of paragraph (a)(1) of this section, the following are not part of, or reasonably necessary to provide, any other product or service:

(i) Targeted advertising;

(ii) Cross-selling of other products or services; or

(iii) The sale of covered data.

(b) *Collection of covered data*—(1) *In general*. Collection of covered data for purposes of paragraph (a) of this section includes the scope of covered data requested and the duration and frequency of collection of covered data.

(2) *Maximum duration*. In addition to the limitation described in paragraph (a) of this section, the third party will limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization.

(3) *Reauthorization after maximum duration*. To collect covered data beyond the one-year maximum period described in paragraph (b)(2) of this section, the third party will obtain a new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. The third party is permitted to ask the consumer for a new authorization pursuant to § 1033.401 in a reasonable manner. Indicia that a new authorization request is reasonable include its conformance to a consensus standard.

(c) *Use of covered data*. Use of covered data for purposes of paragraph (a) of this section includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. Examples of uses of covered data that are permitted under paragraph (a) of this section include:

(1) 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;

(2) Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(3) Servicing or processing the product or service the consumer requested; and

(4) Uses that are reasonably necessary to improve the product or service the consumer requested.

(d) *Accuracy.* A third party 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 accurately provided to another third party, if applicable.

(1) *Flexibility.* A third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(2) *Periodic review.* A third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

(3) *Elements*. In developing its policies and procedures regarding accuracy, a third party must consider, for example:

(i) Accepting covered data in a format required by § 1033.311(b); and

(ii) Addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data.

(4) *Indicia of compliance*. Indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy.

(e) *Data security*. (1) A third party will apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801); or

(2) If the third party is not subject to section 501 of the Gramm-Leach-Bliley Act, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

(f) *Provision of covered data to other third parties*. Before providing covered data to another third party, subject to the limitation described in paragraphs (a) and (c) of this section, the third party will require the other third party by contract to comply with the third party obligations in paragraphs (a) through (f) of this section and the condition in paragraph (i) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

(g) *Ensuring consumers are informed*. (1) Upon obtaining authorization to access covered data on the consumer's behalf, the third party will provide the consumer with a copy of the authorization disclosure that the consumer has signed electronically or in writing and that reflects the date of the consumer's electronic or written signature. The third party will deliver that copy of the authorization disclosure 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.

(2) The third party will provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The contact information must be readily identifiable to the consumer.

(3) The third party 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 in this paragraph (g)(3) about the third party's access to the consumer's covered data. The third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, and the third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. The policies and procedures must be designed to ensure that the third party provides the following to the consumer, upon request:

(i) Categories of covered data collected;

(ii) Reasons for collecting the covered data;

(iii) Names of parties with which the covered data was shared. The names must be readily understandable to the consumer;

(iv) Reasons for sharing the covered data;

(v) Status of the third party's authorization;

(vi) 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

(vii) A copy of any data aggregator certification statement that was provided to the consumer pursuant to § 1033.431(c)(2).

(h) *Revocation of third party authorization*—(1) *Provision of revocation method*. The third party will provide the consumer with a method to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial

authorization. The third party will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization.

(2) *Notice of revocation*. 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 the consumer.

(i) *Effect of maximum duration and revocation on collection, use, and retention*. If a consumer does not provide a new authorization as described in paragraph (b)(3) of this section, or if a third party receives a revocation request as described in paragraph (h)(1) of this section or notice of a consumer's revocation request as described in § 1033.331(e), a third party will:

(1) No longer collect covered data pursuant to the most recent authorization; and

(2) 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 under paragraph (a) of this section.

§ 1033.431 Use of data aggregator.

(a) *Responsibility for authorization procedures when the third party will use a data aggregator*. A data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party seeking authorization under § 1033.401 to access covered data. However, the third party seeking authorization remains responsible for compliance with the authorization procedures described in § 1033.401, and the data aggregator must comply with paragraph (c) of this section.

(b) *Disclosure of the name of the data aggregator*. The authorization disclosure must include the name of any data aggregator that will assist the third party seeking authorization

under § 1033.401 with accessing covered data and a brief description of the services the data aggregator will provide.

(c) *Data aggregator certification.* When the third party seeking authorization under § 1033.401 will use a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in § 1033.421(a) through (f) and the condition in § 1033.421(i) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data. For this requirement to be satisfied:

(1) The third party seeking authorization under § 1033.401 must include the data aggregator's certification in the authorization disclosure described in § 1033.411; or

(2) The data aggregator must provide its certification to the consumer, electronically or in writing, separate from the authorization disclosure. The certification must be in the same language as the authorization disclosure and must be clear, conspicuous, and segregated from other material. The name of any data aggregator in the certification must be readily understandable to the consumer. If, after the consumer has completed the authorization procedures, the authorized third party retains a data aggregator to assist with accessing covered data on behalf of the consumer, this data aggregator must provide its certification in accordance with this paragraph (c)(2).

§ 1033.441 Policies and procedures for third party record retention.

(a) *General requirement.* 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 the requirements of subpart D.

(b) *Retention period.* Records required under paragraph (a) of this section 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 under § 1033.401(a).

(c) *Flexibility.* A third party covered under paragraph (a) of this section has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(d) *Periodic review.* A third party covered under paragraph (a) of this section must periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness to evidence compliance with the requirements of subpart D.

(e) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under this section must include, without limitation:

(1) 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

(2) With respect to a data aggregator covered under paragraph (a) of this section, a copy of any data aggregator certification statement that was provided to the consumer pursuant to § 1033.431(c)(2).

APPENDIX A TO PART 1033-PERSONAL FINANCIAL DATA RIGHTS RULE: HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

If you want the CFPB to designate your organization as a recognized standard setter, you should follow the steps described below.

We may amend this process from time to time.

STEP ONE: REQUESTING RECOGNITION

Submit a written request for recognition.[1]

This should include key contact information, evidence of your organization's policies and practices,[2] and an explanation of how your organization satisfies each of the requirements in the Personal Financial Data Rights rule to be a recognized standard setter.[3] Your request should also describe how current and/or anticipated standards issued by your organization relate to open banking.

In advance of filing your request, you can seek a pre-filing meeting with us. We can walk you through the application process and help you make a complete submission.

Send formal submissions, as well as requests for pre-filing meetings, to: openbankingstandards@cfpb.gov.

STEP TWO: ADDITIONAL INFORMATION AND PUBLIC COMMENT

After reviewing your submission, we may request additional information to ensure that your application is complete.

We may publish your application.

We may also seek public input on your application and invite your responses to any information we receive on that basis.

STEP THREE: OUR REVIEW

When reviewing your application, we consider whether your policies and practices meet

[1] Sensitive personal information should not be provided.

[2] Evidence may include (but is not limited to) charters, bylaws, policies, procedures, fee schedules, meeting minutes, membership lists, financial statements/disclosures, publicly available materials, and issued standards.

[3] Relevant legal requirements are described at 12 CFR 1033.141. When explaining how your organization meets these requirements, you should reference relevant elements of the evidence you submit in support of your application.

all the requirements for recognition. We also evaluate whether your application is accurate and complete.

We prioritize and review applications based on the extent to which recognizing your organization helps us to implement open banking.[4]

STEP FOUR: APPLICATION DECISION

CFPB recognition will be publicly disclosed on our website, along with the applicable terms and conditions of such recognition, such as its duration.

If the CFPB declines to recognize your organization, we will notify you.

You may withdraw your application at any time or for any reason.

If we determine that your organization is close to meeting, but does not yet meet, the requirements for CFPB recognition, we may ask you to provide a written plan specifying how and when you will take the steps required for full recognition. If that plan is satisfactory, we may state on our website that your organization has received contingent recognition. Once you provide us with evidence that you have successfully executed on that plan (or otherwise addressed the relevant contingences), the CFPB may extend full recognition.

STEP FIVE: RECOGNITION

There are several points to keep in mind about recognition.

As a recognized standard setter, you agree that the CFPB may monitor your organization and that you will provide information that we request.

You must also provide us, within 10 days, written explanation of any material change to information that was submitted with your application or during recognition, as well as any reason

[4] Section 1033 of the Consumer Financial Protection Act, 12 U.S.C. 5533, describes the CFPB's role in implementing open banking.

your organization may no longer meet underlying requirements for recognition.

In addition, you must meet any other specified terms and conditions of your recognition, which may include our reserving the right to observe or participate in standard setting.

If your recognition is set to expire, you can apply for re-recognition by re-starting at Step One at least 180 days before expiration. We may temporarily extend your recognition while we consider your request for re-recognition.

We may modify or revoke your recognition. The CFPB expects to notify you of the reasons it intends to revoke or modify recognition, and to provide your organization with an opportunity to address the CFPB's concerns.