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. Section 1001.2 is amended by revising paragraph (b) and by adding and reserving 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. Part 1033 is added to read as follows:

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

SUBPART A—GENERAL

SUBPART B—OBLIGATION TO MAKE COVERED DATA AVAILABLE

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

SUBPART D—AUTHORIZED THIRD PARTIES

AUTHORITY: 12 U.S.C. 5512; 12 U.S.C. 5514; 12 U.S.C. 5532; 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 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.

§ 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, 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:

(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); and

(3) Facilitation of payments from a Regulation E account or Regulation Z credit card.

(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 the consumer obtained from that person.

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

(d) *Excluded data providers*. The requirements of this part do not apply to data providers that are depository institutions that do not have a consumer interface.

§ 1033.121 Compliance dates.

A data provider must comply with §§ 1033.201 and 1033.301 beginning on:

(a) [Approximately six months after the date of publication of the final rule in the *Federal Register*], for depository institution data providers that hold at least $500 billion in total assets and nondepository institution data providers that generated at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year.

(b) [Approximately one year after the date of publication of the final rule in the *Federal Register*], for data providers that are:

(1) Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets; or

(2) Nondepository institutions that generated less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year.

(c) [Approximately two and a half years after the date of publication of the final rule in the *Federal Register*], for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.

(d) [Approximately four years after the date of publication of the final rule in the *Federal Register*], for depository institutions that hold less than $850 million in total assets.

§ 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).

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

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 an entity 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).

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).

Qualified industry standard means a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with § 1033.141(a).

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 or entity 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.

(a) *Fair, open, and inclusive standard-setting body*. A standard-setting body is fair, open, and inclusive and is an issuer of qualified industry standards when it has all of 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 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, 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 some participants may play multiple roles, such as being both a data provider and an authorized third party. The ownership structure of entities is considered in achieving balance.

(3) Due process: 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.

(4) Appeals: An appeals process is available for the impartial handling of appeals.

(5) Consensus: Standards development proceeds by consensus, which is defined as general agreement, but not unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

(6) Transparency: Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

(7) CFPB recognition: The standard-setting body has been recognized by the CFPB within the last three years as an issuer of qualified industry standards.

(b) *CFPB consideration*. A standard-setting body may request that the CFPB recognize it as an issuer of qualified industry standards. The attributes set forth in paragraphs (a)(1) through (6) of this section will inform the CFPB's consideration of the request.

SUBPART B—OBLIGATION TO MAKE COVERED DATA AVAILABLE

§ 1033.201 Obligation to make covered data available.

(a) *Obligation to make covered data available*. 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. Compliance with the requirements in §§ 1033.301 and 1033.311 is required in addition to the requirements of this paragraph (a).

(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 debit card 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) if it makes available at least 24 months of such information.

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

(b) Account balance.

(c) Information to initiate payment to or from a Regulation E account.

Example 1 to paragraph (c): This category includes a tokenized account and routing number that can be used to initiate an Automated Clearing House transaction. In complying with its obligation under § 1033.201(a), a data provider is permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number.

(d) Terms and conditions.

Example 1 to paragraph (d): This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, 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.

§ 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 benefit of 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 establish and maintain interfaces*. A data provider subject to the requirements of this part must maintain a consumer interface and must establish and maintain 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 specific request.* Upon specific request, a data provider must make available to a consumer or an authorized third party covered data in a machine-readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

Example 1 to paragraph (b): A data provider makes available covered data in a machine-readable file that can be retained if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party.

(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 format. The interface is deemed to satisfy this requirement if:

(1) The interface makes available covered data in a format that is set forth in a qualified industry standard; or

(2) In the absence of a qualified industry standard, the interface makes available covered data in a format that is widely used by the developer interfaces of other similarly situated data providers with respect to similar data and is readily usable by authorized third parties.

(c) *Performance specifications.* The developer interface must satisfy the following performance specifications:

(1) *Commercially reasonable performance.* The performance of the interface must be commercially reasonable.

(i) *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 queries for covered data to the interface must be equal to or greater than 99.5 percent. For purposes of this paragraph (c)(1)(i), all of the following requirements apply:

(A) Any responses by and queries to the interface during scheduled downtime for the interface must be excluded respectively from the numerator and the denominator of the calculation.

(B) 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 adheres to a qualified industry standard.

(C) The total amount of scheduled downtime for the interface in the relevant time period, such as a month, must be reasonable. Indicia that the total amount of scheduled downtime may be reasonable include that the amount adheres to a qualified industry standard.

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

(*1*) The response either fulfills the query or explains why the query was not fulfilled;

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

(*3*) The response is provided by the interface within a commercially reasonable amount of time. The amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds.

(ii) *Indicia of compliance*. Indicia that the performance of the interface is commercially reasonable include that it:

(A) Meets the applicable performance specifications set forth in a qualified industry standard; and

(B) Meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.

(2) *Access cap prohibition*. 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 and 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 adhere to a qualified industry standard.

(d) *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.

(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.

§ 1033.321 Interface access.

(a) *Denials related to risk management*. A data provider does not violate the general obligation in § 1033.201(a) by reasonably denying a consumer or third party access to an interface described in § 1033.301(a) based on risk management concerns. Subject to paragraph (b) of this section, a denial is not unreasonable if it is necessary to comply with section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1 or section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801.

(b) *Reasonable denials.* To be reasonable pursuant to paragraph (a) of this section, a denial must, at a minimum, be 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 must be applied in a consistent and non-discriminatory manner.

(c) *Indicia of reasonable denials.* Indicia that a denial pursuant to paragraph (a) of this section is reasonable include whether access is denied to adhere to a qualified industry standard related to data security or risk management.

(d) *Denials related to lack of information*. A data provider has a reasonable basis for denying access to a third party under paragraph (a) of this section if:

(1) The third party does not present evidence that its data security practices are adequate to safeguard the covered data, provided that the denial of access is not otherwise unreasonable; 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 data security practices.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers*. To comply with the requirement in § 1033.201(a), 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 requirement in § 1033.201(a), 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) Confirm 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).

(c) *Response not required.* Notwithstanding the general rules in paragraphs (a) and (b) of this section, 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 provider has a basis to deny access pursuant to risk management concerns in accordance with § 1033.321(a);

(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).

(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 requirements of this section.

(e) *Mechanism to revoke third party authorization to access covered data.* A data provider does not violate the general obligation in § 1033.201(a) 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. To be reasonable, the revocation method must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party. Indicia that the data provider's revocation method is reasonable include its conformance to a qualified industry standard. A data provider that receives a revocation request from consumers through a revocation method it makes available must notify the authorized third party of the request.

§ 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. The documentation must:

(1) Be maintained and updated as the developer interface is updated;

(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 specification*. On or before the tenth calendar 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 described in § 1033.311(c)(1)(i) 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 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 that are 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. A data provider is permitted to comply with this requirement by incorporating the data fields defined by a qualified industry standard, provided doing so is appropriate to the size, nature, and complexity of the data provider's activities. Exclusive reliance on data fields defined by a qualified industry standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession.

(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 explaining the basis for denial; and

(ii) Communicates to the third party, electronically or in writing, the reason(s) for the denial, and that the communication occurs as quickly as is practicable.

(3) *Denials of information requests.* When a data provider denies a request for information pursuant to § 1033.331, the data provider:

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

(ii) Communicates to the consumer or third party, electronically or in writing, the type(s) of information denied and the reason(s) for the denial, and that the communication occurs as quickly as is practicable.

(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 qualified industry 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 related to a data provider's 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.

(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 of requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable;

(ii) Records of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable;

(iii) Copies of a third party's authorization to access data on behalf of a consumer; and

(iv) Records of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation mechanism made available by a data provider.

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) *General requirements*. 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.

(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 that the consumer has requested the third party identified in paragraph (b)(1) of this section provide and a statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer.

(4) The categories of covered data that will be accessed.

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

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

(c) *Language access*—(1) *General language requirements.* The authorization disclosure must be in the same language as the communication in which the third party conveys the authorization disclosure to the consumer. Any translation of the authorization disclosure 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 activities.* For purposes of paragraph (a)(1) of this section, the following activities 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 collected 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 qualified industry standard.

(4) *Effect of maximum duration*. If a consumer does not provide the third party with a new authorization as described in paragraph (b)(3) of this section, the third party will:

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

(ii) 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.

(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; and

(3) Servicing or processing the product or service the consumer requested.

(d) *Accuracy.* The 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 qualified industry 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 (g) of this section and the condition in paragraph (h)(3) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

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

(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.

(i) Categories of covered data collected;

(ii) Reasons for collecting the covered data;

(iii) Names of parties with which the covered data was shared;

(iv) Reasons for sharing the covered data;

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

(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.

(h) *Revocation of third party authorization*—(1) *Provision of revocation mechanism*. The third party will provide the consumer with a mechanism 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.

(3) *Effect of revocation.* Upon receipt of a consumer's revocation request as described in paragraph (h)(1) of this section or notice of a revocation request from a data provider as described in § 1033.331(e), a third party will:

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

(ii) 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(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data. Any data aggregator that is retained by the authorized third party after the consumer has completed the authorization procedures must also satisfy this requirement. 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 in a separate communication.

§ 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 or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent and a record of actions taken by the consumer, including actions taken through a data provider, 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 provided to the consumer separate from the authorization disclosure pursuant to § 1033.431(c)(2).