Personal Financial Data Rights – Final Rule (Section 1033 of the Dodd Frank Act)

Presenter:
Maureen Busch, Director of Compliance and CRA
The Bank of Tampa

Disclaimer

The materials provided represent my own opinions and not necessarily that of The Bank of Tampa.

Current Status *(ao 2-13-2025)*

Final Rule issued October 22, 2024

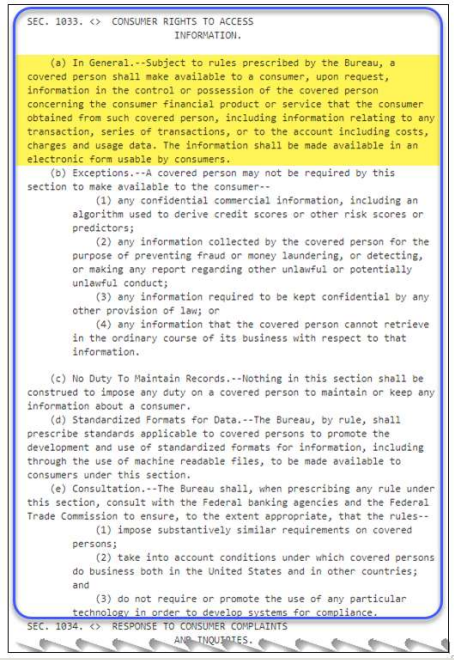
Published in Federal Register in November 18, 2024, with an effective date of January 17, 2025 *(compliance dates beginning April 2026)*

However, the effective date is stayed.

Where it began…

A provision on consumer rights to access information was included in the Dodd-Frank Act (Section 1033)

There were only 8 lines of general requirements …but they "packed a punch"



SEC. 1033. <> CONSUMER RIGHTS TO ACCESS INFORMATION.

(a) In General.--Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.

(b) Exceptions.--A covered person may not be required by this section to make available to the consumer--

(1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;

(2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;

(3) any information required to be kept confidential by any other provision of law; or

(4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.

(c) No Duty To Maintain Records.--Nothing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer.

(d) Standardized Formats for Data.--The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section.

(e) Consultation.--The Bureau shall, when prescribing any rule under this section, consult with the Federal banking agencies and the Federal Trade Commission to ensure, to the extent appropriate, that the rules--

(1) impose substantively similar requirements on covered persons;

(2) take into account conditions under which covered persons do business both in the United States and in other countries; and

(3) do not require or promote the use of any particular technology in order to develop systems for compliance.

SEC. 1034. <> RESPONSE TO CONSUMER COMPLAINTS AND INQUIRIES.

Implementation Timeline for Banks

April 1, 2026 – Assets* of $250B or greater

April 1, 2027 – Assets* of at least $10B but less than $250B

April 1, 2028 – Assets* of at least $3B but less than $10B

April 1, 2029 – Assets* of at least $1.5B but less than $3B

April 1, 2030 – Assets* of at least $850MM but less than $1.5B

Exempt – Banks with assets of $850MM or less

Assets = Total assets based on an average of the bank's Q3 2023 through Q2 2024 call report submissions

Final Rule in a Nutshell – Making "covered data" available to consumers

Under the final rule, "data providers" are required to make "covered data" about "covered financial products and services" available in electronic form to consumers and to certain "authorized third parties."

Covered Entities

Data Providers

Data provider means a covered person (which means a person* that engages in offering or providing a consumer financial product or service (and an affiliate if the affiliate acts as a service provider to that person)) that is:

- A financial institution as defined under Regulation E
- A card issuer as defined under Regulation Z
- Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.

In short, banks are data providers, but may be exempt from the Regulation based on asset size

*The term person means an individual, partnership, company, corporation, association (incorporated or unincorporated), trust, estate, cooperative organization, or other entity.

Covered Consumer Financial Products/ Services

1. An **account** covered under Regulation E (1005.2(b))
   - (aka a Regulation E account)
   - A demand deposit (checking), savings, or other consumer asset account (e.g., a club account) (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes.
2. A **credit card** covered under Regulation Z (1026.2(a)(15)(i)
   - (aka a Regulation Z credit card)
   - Any card, plate, or other single credit device that may be used from time to time to obtain credit (includes hybrid prepaid-credit cards under 1026.61).
3. The facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments.

Additional Important Definitions

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

- NOTE: A bank may serve as a data provider as well as an authorized third party

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

- *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.

Data Provider Obligations

A data provider has obligations under the regulation if it controls or possesses covered data concerning a covered consumer financial product or service that the consumer obtained from the data provider

AND

the consumer directly, or through an authorized third party, makes a request for information.

Covered Data

1. Transaction information
2. Account balance information
3. Information to initiate payment to or from a Regulation E account
4. Terms and conditions
5. Upcoming bill payment information
6. Basic account verification information

*Data provider **NOT** required to make available:*

- Confidential commercial information
- Information collected for the sole purpose of preventing fraud or money laundering or making any report regarding unlawful/potentially unlawful conduct
- Information required to be kept confidential
- Any information that cannot be retrieved in the ordinary course of business with respect to that information.

BUT – data provider cannot take steps to evade requirements, make covered data unusable, or discourage consumers/authorized third parties from accessing covered data

1. Transaction information

Includes:

Historical transaction information in the control or possession of the data provider (24 months of data).

Transaction Information – *Example cited in the Regulation*

This category includes:

- amount,
- transaction date,
- payment type,
- pending or authorized status,
- payee or merchant name,
- rewards credits, and
- fees or finance charges.

2. Account balance information

Not detailed in the Regulation.

3. Information to initiate payment to or from a Regulation E account

Applies only if the data provider directly or indirectly hold the Regulation E account and does not apply to a data provider that merely facilitates pass-through payments.

A data provider may make available a tokenized account number instead of, or in addition to, a non-tokenized account number, as long as the tokenization is not used as a pretext to restrict competitive use of payment initiation information.

4. Terms and Conditions

Includes data in the agreements evidencing the terms of the legal obligation between data provider and a consumer, such as data int eh account opening agreement and any amendments or additions to that agreement, including pricing information.

Terms and Conditions – *Example cited in the Regulation*

This category includes

- the applicable fee schedule,
- any annual percentage rate or annual percentage yield,
- credit limit,
- rewards program terms,
- whether a consumer has opted into overdraft coverage, and
- whether a consumer has entered into an arbitration agreement.

5. Upcoming bill payment information

Not detailed in the regulation; though an example is included (see next slide).

Upcoming Bill Payment Information – *Example cited in the Regulation*

Includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.

6. Basic account verification information

Information associated with the covered consumer financial product/service:

- Name
- Address
- Email address
- Phone number
- Truncated account number or other identified (data providers must make available for Regulation E and Regulation Z accounts)

Data Access Requirements

1. Standardized format
2. Commercially reasonable format
3. Access caps
4. Access credentials
5. Security program

NOTE: The final rule does not require a data provider to use any particular technology to satisfy the requirements.

Denial of Data Access

Data provider may deny consumer/authorized third party access if:

1. Granting access would be inconsistent with policies/procedures reasonable designed to comply with:
   - Safety and soundness standards of the data provider's prudential regulator
   - Information security standards required by the Gramm-Leach-Bliley Act (GLBA)
   - Other applicable laws and regulations regarding risk management.

2. The denial is reasonable – i.e., it must be directly related to a specific risk of which the data provider is aware and must be applied in a consistent and non-discriminatory manner.

Denial of Access – Additionally, as it pertains to a third party

Can deny access to third party if:

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

Responding to requests

General requirements:

- Maintain interfaces (consumer and developer interfaces).
- Make information available in a machine-readable format and the consumer or authorized third party can retain or transfer for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.
- Fees prohibited – a data provider may not impost any fees or charges on a consumer or authorized third party in connection with establishing/maintaining interfaces or information requests covered by the regulation.

Responding to Requests (cont'd)

Request/Access by consumers:

A data provider must make available covered data available through its interface when it receives information sufficient to:

- Authenticate the consumer's identity; and
- Identify the scope of data requested.

Request/Access by third parties:

A data provider must make available covered data available through its interface when it receives information sufficient to:

- Authenticate the consumer's identity
- Authenticate the third party's identity
- Document that the third party has followed the authorization procedures in the regulation (1033.401); and
- Identify the scope of data requested.

Responding to Requests (cont'd)

The data provider is permitted to confirm the scope of the third party's authorization to access the consumer's data by asking the consumer to confirm:

- The account(s) to which the third party is seeking access and
- The categories of covered data the third party is requesting to access

Making Information About the Data Provider Readily Identifiable

Data provider must make certain information readily identifiable to members of the public and available in human and machine-readable formats.

Includes:

- Legal name
- LEI
- Link to its website
- Contact information that enables a consumer/third party to receive answers to questions about accessing covered data

Additionally, each month, a data provider must disclose to the public certain information about its data interface's response rate to authorized third party requests for covered data in the previous calendar month.

Policies, Procedures and Recordkeeping Requirements for Data Providers

Policies and procedures should be designed to ensure that the data provider:

- Creates a record of data fields of covered data in its control/possession.
- Creates certain records regarding denials of access to authorized third parties.
- Accurately makes covered data available to an authorized third party.
- Retains records to reflect compliance of requirements under the final rule.

Authorized Third Parties, Authorization Procedures, and Authorization Disclosures

To become an authorized third party, the third party must:

- Provide the consumer with an authorization disclosure as described in the final rule;
- Provide a statement to the consumer in the **authorization disclosure** certifying that the third party agrees to certain obligations set forth in the final rule; and
- Obtain the consumer's express informed consent by obtaining an authorization disclosure signed by the consumer (electronically or in writing).

Authorization Disclosure

Must include all of the following:

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

Third Party Obligations

1. **Limit its collection, use and retention of covered data** (e.g., targeted advertising/cross-selling of other products/services not permitted).
2. **Maximum duration**. Limit duration of collection of covered data to one year after the consumer's most recent authorization.
   - To collect data beyond the one-year period, reauthorization required.
3. **Uses of covered data.** Abide by permitted uses of covered data (e.g., servicing or processing the product/or service the consumer requested or uses that are reasonably necessary to improve the product/service the consumer requested).
4. **Accuracy.** Establish and maintain written policies and procedures designed to ensure data is accurately received (from a data provider) and accurately provided to another third party (if applicable).
5. **Data security.** Apply an information security program for the collection, use and retention over covered data (GLBA)
6. **Provision of covered data to other third parties**. Before providing covered data to another third party, require that party to comply with third party obligations.
7. **Ensuring consumers are informed.** Provide consumer with copy of signed authorization disclosure, along with contact information.
8. **Revocation of third party authorization.** Provide consumer with method to revoke authorization.

Policies/Procedures for Third Party Record Retention

Third party must:

- Have written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the final rule. Retain for at least three years after the third party obtains the consumer's most recent authorization.
- Periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

Use of Data Aggregators

Use of data aggregator permitted to perform the authorization procedures (set forth in the final rule) on behalf of a third party. The third party seeking authorization remains responsible for compliance with the authorization procedures.

Data aggregator must certify to the consumer (and provide the certification to the consumer) that it will satisfy third party obligations.

The third party's authorization disclosure must include the data aggregator's name and a description of the services that the data aggregator will provide in connection with accessing the consumer's covered data.

Thank you.