ICBA

One Mission. **Community Banks.**

Open Banking Guidebook

(Section 1033)

January 2025

Disclaimer: The information provided in this document does not constitute legal advice and is for general informational purposes only. Information in this document may not contain the most up-to-date information. Readers of this material should contact their attorney to obtain advice with respect to how federal regulations apply to any given financial institution or consumer.

Table of Contents

What is Section 1033?

Section 1033 of the Dodd-Frank Act requires the Consumer Financial Protection Bureau (CFPB) to create rules requiring covered financial institutions to make available certain financial information to consumers.[1] The CFPB has interpreted this statute to create a consumer right of "data portability," which is a right for consumers to be able to move their financial data in a standardized, machine readable format between financial services providers. Data portability is intended to enable "open banking," in whichwhere consumers can give permission to third- party companies known as data recipients to access their financial information retained by banks.

Proponents of open banking argue that giving the consumers the ability to easily share their financial data with data recipients will increase the competition in the financial services industry, allowing consumers to access more customized financial products and to benefit from lower interest rates on loans. They also argue that it will benefit financial institutions by making it more practical for financial institutions to offer loan or deposit products to consumers who bank with a competing bank while benefiting consumers by making , or become evenit more seamlesseasier for them consumers to switch banks, entirely.

On the other hand, detractors of open banking argue that it creates increased fraud risk because it may enable consumers to share sensitive information—including information like account numbers—with unregulated, unsupervised fintech companies that do not maintain robust data security programs. This could make consumers more vulnerable to data breaches, or even allow consumers to share data with companies that misuse the data themselves. Finally, from a compliance and IT perspective, open banking will increase costs to financial institutions because it will require banks to bear the cost of creating and maintaining an online "developer portal" where third party data recipients can access customer information.

Background on the Personal Financial Data Rights Rule

The CFPB began the process of implementing Section 1033 in 2016 by issuing a rRequest for iInformation in the Federal Register and later, in 2022 by hosting a two-day long panel with various impacted small businesses, including small banks, credit unions, and fintech companies, as required by the Small Business Regulatory Enforcement Fairness Act (SBREFA). ICBA participated in every step of the rulemaking process, submitting numerous comment letters and being represented by a member bank on the CFPB's SBREFA panel. Finally, on Oct. ober 19, 2023, the CFPB issued a Notice of Proposed Rulemaking, which provided a detailed outline of its proposed open banking rule. Informed by feedback from our banker-led Section 1033 Working Group, ICBA submitted a comment letter making numerous detailed proposals on how the Bbureau's rule could be improved, including

1 12 U.S.C. 5533.

exempting banks that are legally considered to be small businesses (those with less than $850 million in assets) and allowing banks to charge a reasonable fee to third parties for accessing consumer information.[2]

On Oct. 22, 2024, the CFPB issued a Ffinal Rrule implementing Section 1033.[3] In a speech at the Federal Reserve Bank of Philadelphia, CFPB Director Rohit Chopra extolled the benefits of the rule saying, "The rule will provide more freedom, promote decentralization, and spur greater competition. It is an important step toward ensuring that these principles, embedded in the fabric of our financial system dating back to the earliest days of the republic, are reflected in this digital era."[4]

ICBA was pleased to see that the bBureau adopted several of our recommended changes to the proposed rule, including an exemption for small banks with less than $850 million in assets. No other national banking trade association advocated a similar exemption. The community bank exemption would not be included in the final rule without our advocacy. ICBA also was pleased that the CFPB retained many of the positive aspects of its proposed rule that we supported as proposed, including creating a role for industry standard- setting bodies and imposing limitations on the secondary use of consumer data (i.e. for targeted advertising and cross-selling) on third- party data recipients. A detailed analysis of the provisions of the final rule will follow:

Coverage of Data Providers

Under the rule, depository institutions (banks and credit unions) and non-depository institutions that issue credit cards (Reg Z accounts), hold transaction accounts (Reg E accounts), issue devices to access an account, or provide other types of payment facilitation products or services will be covered "data providers," required to comply with the rule.

Banks that hold total assets equal to or less than the Small Business Administration (SBA)SBA size standard to be considered a small business are not required to comply with the requirements of the rule that pertain to making customer data available to third parties through a developer interface. The Small Business Administration (SBA) size standard is currently $850 million in assets.[5] **Banks below $850 million in assets are not considered covered data providers under the final rule.** Total assets are calculated by averaging the assets reported on its own four preceding quarterly call report submissions to the Federal Financial Institutions Examination Council.

2 See Mickey Marshall, "Re: ICBA Comments in Response to Section 1033 Notice of Proposed Rulemaking (Required Rulemaking on Personal Financial Data Rights) [Docket No. CFPB–2023–0052; RIN 3170–AA78]" (Dec. 29, 2023), available at: https://www.icba.org/advocacy/letter-details/icba-letter-in-response-to-section-1033.

3 CFPB, "Required Rulemaking on Personal Financial Data Rights," (Oct. 22, 2024), available at: https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/.

4 Rohit Chopra, "Prepared Remarks of CFPB Director Rohit Chopra at the Federal Reserve Bank of Philadelphia on the Personal Financial Data Rights Rule" (Oct 22, 2024), available at: https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-federal-reserve-bank-of-philadelphia-on-the-personal-financial-data-rights-rule/.

5 For a list of industry specific size standards, see 13 CFR 121.201.

The exemption threshold may increase over time if the SBA increases its small business size threshold for depository institutions. Banks may cross the size threshold and become subject to the rule by virtue of a merger.

Banks below the exemption threshold are not required to create and maintain a developer interface to provide customer data to third parties, but they are also not prohibited from doing so if they choose. Exempt banks may choose to voluntarily act as data providers in response to customer demand or to facilitate customer access to a greater range of financial services. In addition, banks above and below the exemption threshold may act as authorized third parties and receive data from data providers.

Compliance Dates

Currently, depository institutions with over $850 million in assets will be required to comply with the rule as covered data providers. The compliance dates for depository institutions are:

Bank Size	Compliance Date
Banks over $250 billion in assets	April 1, 2026
Banks between $10 billion and $250 billion in assets	April 1, 2027
Banks between $3 billion and $10 billion in assets	April 1, 2028
Banks between $1.5 billion and $3 billion in assets	April 1, 2029
Banks between $850 million and $1.5 billion in assets	April 1, 2030

A depository institution data provider that has total assets less than the SBA size standard but that subsequently holds total assets that exceed that SBA size standard, must comply within a reasonable amount of time after exceeding the size standard, not to exceed five years.

Definitions

The final rule includes several basic defined terms that govern which financial institutions are covered by the rule, the scope of the data they must share, and other factors.

- **Authorized third party**—a third party that has complied with the authorization procedures described in the rule.
- **Consensus standard**—a standard that is adopted by a recognized standard setter and that continues to be maintained by that recognized standard setter.

- **Consumer**—a natural person. Trusts established for tax or estate- planning purposes are considered natural persons for purposes of this definition. Businesses and non-profit organizations are not consumers for purposes of this rule.
- **Consumer interface**—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**—covered products and services are defined to include a Regulation E account, a Regulation Z credit card, and facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments.
- **Covered data**—the data a data provider may be required to provide to an authorized third party. The types of covered data are discussed in the next section of this guide.
- **Data aggregator**—a person that is retained by and provides services to the authorized third party to enable access to covered data.
- **Data provider**—a financial institution, as defined in Regulation E, a card issuer, as defined in Regulation Z, and any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.
- **Developer interface**—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.
- **Recognized standard setter**—a standard-setting body that has been recognized by the CFPB pursuant to the recognition process established in the final rule.
- **Third party**—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.

Covered Data

Covered data is the data that a data provider may be required to provide to an authorized third party. Data providers will not be required to provide every category of covered data in response to every request from an authorized third party as third parties are only permitted to collect, use, and retain consumer data only as reasonably necessary to provide a particular product or service to the consumer. The types of covered data are:

1. **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 if it makes available at least 24 months of such information. 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**

3. **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. In complying with its obligation under this section, a data provider is permitted to make available a Tokenized Account Number (TAN) instead of, or in addition to, a non-tokenized account number, as long as the tokenization is not used as a pretext to restrict competitive use of payment initiation information.

A Note on TANs: A Tokenized Account Number or TAN is a randomly generated number that replaces a customer's actual account number that allows a third party to initiate a transfer out of a customer's account. TANs have the potential to increase data security—but also increase the technical complexity of open banking. ICBA urged the CFPB to permit but not require the use of TANs in lieu of account numbers unless and until the technology becomes more accessible to community banks.

4. **Terms and conditions**—Terms and conditions are limited to data in agreements evidencing the terms of the legal obligation between a data provider and a consumer for a covered consumer financial product or service, such data in the account opening agreement and any amendments or additions to that agreement, including pricing information. This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, credit limit, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.
5. **Upcoming bill information**—This category includes information about third- party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.
6. **Basic account verification information**—This category includes the customer's name, address, email address, and the phone number associated with the covered consumer financial product or service.

Exceptions

Covered data providers are not required to provide covered data in the following circumstances:

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 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.

3. **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.
4. Any information that the data provider cannot retrieve in the **ordinary course of its business** with respect to that information.

Developer Interface Requirements

All covered data providers must make covered data available through a developer interface. Developer interfaces must provide data in machine- readable format 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. Developer interfaces will generally be online web portals where authorized third parties can present customer authorization and gain access to certain covered data through the intermediation of an Application Program Interface, or API.

Fee Prohibition—Covered data providers are not permitted to charge any fee association with establishing or maintaining the developer interface or any fee associated with receiving requests or making available covered data.

An Unfair Prohibition: Prohibiting data providers from charging fees for data access is one of the most significant oversights in the final rule. Authorized third parties derive considerable benefits from this rule, including the ability to access valuable customer information from banks and market financial products and services to those customers. In contrast, the cost burden falls entirely on the banks, which are responsible for creating the developer portal themselves or outsourcing this task to their core processor or another third party. We will continue to advocate for the removal of the fee prohibition.

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. Consensus standards are to be established by recognized standard setters through the process described on page 12 of this guide.

Commercially Reasonable Performance—A developer interface's performance must be commercially reasonable. A developer interface cannot be commercially reasonable if it does not provide a proper response rate of 99.5% in each calendar month. Other indicia of compliance include whether the interface's performance conforms to a consensus standard and whether the interface's performance is comparable to the performance levels achieved by the developer interfaces of similarly situated data providers.

Access Caps—A data provider must not unreasonably restrict the frequency with which it receives or responds to requests for covered data from an authorized third party through its developer interface. Any frequency restrictions must be applied in a manner that is nondiscriminatory and consistent with the reasonable written policies and procedures that the data provider establishes.

Security—A data provider must not allow a third party to access the data provider's developer interface using the same credentials that a consumer uses to access his or her interface. In other words, the practice of "screen scraping" is prohibited for banks not exempt from the rule. The developer interface must be subject to an information security program that complies with the Privacy and Safeguards rules of the Gramm-Leach-Bliley Act (GLBA)GLBA.

Fair Credit Reporting Act (FCRA)—The CFPB has determined that data providers will not be considered furnishers for the purposes of the FCRA solely by virtue of permitting data access pursuant to an authorization that is consistent with the final rule. This is the case even assuming data are provided to a data aggregator that qualifies as a consumer reporting agency.

Consumer Interfaces

In addition to developer interfaces, the rule requires banks over $850 million to maintain a consumer interface, where consumers can access their own financial data. In general, a bank's online banking portal should be sufficient to satisfy the requirement to provide a consumer interface.

Denying Access to Third Parties

A data provider may deny a request to access covered data by an authorized third party when:

1. granting access would be inconsistent with policies and procedures reasonably designed to comply with:
    a. safety and soundness standards of a prudential regulator;
    b. information security standards required by the GLBA;
    c. other applicable laws and regulations regarding risk management; and

2. the denial is reasonable because it is directly related to a specific risk of which the data provider is aware.

Privacy Risk: ICBA is concerned that circumstances in which data providers are permitted to make risk-based denials are too narrow. For example, while data providers

are permitted to make denials that are "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," such failures are often only known after a breach has occurred and customer data is already compromised. This rule, in effect, requires data providers to constantly conduct third-party due diligence on the entire universe of possible third parties, including all banks, credit unions, financial technology companies, and more.

This is not possible, particularly with respect to third parties that are not subject to regular examination. The bureau could mitigate these concerns by clearly specifying that financial liability for breaches lies with the party where the breach occurs—and requiring third-party data recipients to indemnify data providers when breaches at the third party occur.

Responding to Requests by Third Parties

A data provider must make available covered data once it receives information from an authorized third party sufficient to:

1. Authenticate the consumer's identity;
2. Authenticate the third party's identity;
3. Document the third party has followed the authorization procedures required by the rule;
4. Identify the scope of the data requested.

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:

1. The account(s) to which the third party is seeking access; and
2. The categories of covered data the third party is requesting to access, as disclosed by the third party.

Requirements for Authorized Third Parties

An authorized third party receives consent from a customer in order to provide a product or service that the customer requests. Banks that are covered data providers must provide covered data to authorized third parties. However, all banks, whether they are covered data providers or not, may act as authorized third parties and receive data from covered data providers. Because of this, banks should keep in mind that open banking is a two-way street for data. While covered banks will be required to make certain customer information available to their competitors, all banks will have the ability to access information about their competitors' customers and try to win their business.

Authorized third parties must:

1. Provide the consumer with an authorization disclosure containing certain key terms of the data access;
2. 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
3. Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

Contents of the authorization disclosure—The authorization disclosure must be clear, conspicuous, and segregated from other material provided to the consumer. It must include the following content:

1. The name of the third party that will be authorized to access covered data.
2. The name of the data provider that controls or possesses the covered data that the third party seeks to access on the consumer's behalf.
3. A brief description of the product or service the consumer has requested from the third party and a statement that the third party will collect, use, and retain the consumer's data only as reasonably necessary to provide that product or service to the consumer.
4. The categories of data that will be accessed.
5. A certification statement certifying that the third party adheres to all of the third-party obligations described in the next section of this guide.
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 method by which the consumer can revoke the third parties' access to the covered data.

Third Party Obligations—Third parties are subject to a number of obligations that govern the privacy rights of consumers and limit the use of consumer data by the third party. Banks are also subject to these obligations when they act as a data recipient and access information about customers of other financial institutions. Third- party data recipients must certify to consumers that they are bound by the following obligations to access customer data:

1. **General limitation on collection, use, and retention of consumer data.** The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. For the purposes of the Section 1033 rule, targeted advertising, cross-selling of other products or services, and the sale of covered data are deemed to be not reasonably necessary to provide any product or service and are therefore not permitted.

2. **Maximum duration.** 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. Third parties must obtain a new authorization after one year.
3. **Use of covered data.** Permitted use of covered data includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. For example, it may be permissible to share customer data with another third party if it is necessary to facilitate the servicing or processing of the product or service the consumer requested.
4. **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.
5. **Data security.** A third party will apply to its systems an information security program for the collection, use, and retention of covered data that satisfies the Privacy and Safeguards rules of the GLBA. If the third party is not subject to the GLBA (i.e. if it does not meet the legal definition of a financial institution), 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.
6. **Provision of covered data to other third parties.** Before providing covered data to another third party, the third party will require the subsequent third party to comply with all of the third- party obligations described in this section by contract.
7. **Ensuring consumers are informed.** 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. 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.
8. **Revocation of third-party authorization.** 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.

Use of a data aggregator—A data aggregator is permitted to perform the authorization procedures on behalf of the third party seeking authorization to access covered data. When a data aggregator is used, the authorization disclosure must include the name of any data aggregator that will assist the third party seeking authorization with accessing covered data and a brief description of the services the data aggregator will provide.

Third party record retention—Authorized third parties 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 the Open Banking rule (Section 1033) . They must also retain records for a period of not less than three years after a third party obtains the consumer's most recent authorization.

Standard-Setting Bodies

Standard- setting bodies may seek CFPB recognition to develop a consensus standard , which governs the technical requirements of data sharing through developer portals. To become a *recognized standard setter*, a standard- setting body must meet the following requirements:

1. **Openness:** The procedures and processes used by the standard setter are open to all interested parties. Interested 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. There is meaningful representation for large and small commercial entities.
3. **Due process and appeals:** 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.
5. **Transparency:** Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

ICBA advocated for allowing industry standard- setting bodies to establish standards for data sharing. We argued that technical standards should be set by industry groups rather than by regulation because both technology and best practices can change quickly. ICBA is a member of the Financial Data Exchange (FDX), which has sought recognition from the CFPB as a recognized standard setter.[6] Community bankers wishing to get more involved in the standard- setting process should contact ICBA.

More on FDX: FDX is a non-profit association that was spun off FS-ISAC in 2018 for the purpose of creating a common, interoperable and royalty-free technical standard for user-permissioned financial data sharing. The FDX API, or Application Program Interface, is a set of rules and protocols that allows the software systems of data providers and data recipients to share information in a controlled way. ICBA is a member of FDX's small data provider working group and has input on the API's rules.

Conclusion

The CFPB's final rule implementing Section 1033 of the Dodd-Frank Act marks a significant shift in how consumer financial data is managed and shared. By mandating data portability, the rule aims to foster innovation and competition in the financial services sector, making

6 For more information about FDX, See their "About FDX" webpage available at: https://financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6; or read their white papers and guides, available at: https://financialdataexchange.org/FDX/FDX/White-Papers-Guides.aspx?hkey=e084d471-4a70-4bf2-abbe-8835c441fca0.

it easier for consumers to access, share, and control their financial information. While the potential for more tailored financial products and services may benefit consumers, the rule also introduces critical challenges for community banks, particularly around data security and the cost of compliance.

ICBA is committed to supporting community banks as they navigate these new requirements. Our advocacy efforts have helped secure important provisions, such as increasing CFPB oversight of third- party data recipients and eliminating the onerous fee prohibition. Moving forward, ICBA will continue to monitor developments in open banking and advocate for policies that protect consumer privacy, ensure data security, and support community banks' unique role in serving local communities.

Section 1033 presents both risks and opportunities for community banks. By adapting to the new regulatory landscape and focusing on delivering a high level of service and trust, community banks can turn this challenge into a chance to differentiate themselves in a competitive market. ICBA remains a partner to community banks through this regulatory shift, ensuring that they are well-positioned to succeed in an open banking future. Please feel free to reach out to us to learn more about open banking regulations or to provide feedback that can impact our advocacy efforts in the future.

Continue the Conversation

Mickey Marshall
AVP, Regulatory Counsel
Independent Community Bankers of America
Michael.Marshall@icba.org
202-821-4411

Press Inquiries

Nicole Swann
VP, Communications
Independent Community Bankers of America
Nicole.Swann@icba.org
202-821-4458