

Complying with the CFPB 1033 rule

**Foundational requirements
and growth opportunities**

Contents

Executive summary	3
The 1033 CFPB rule	4
Current market situation	6
Implications of the CFPB rule for your organization	6
Timeline for your organization to comply with the CFPB rule	10
Maximizing the value of open banking to turbocharge growth	11
Getting started	13
Contacts and contributors	14

Executive summary

The Consumer Financial Protection Bureau (CFPB) has proposed the Personal Financial Data Rights Rule (“1033 rule”) that will accelerate the adoption of open banking by providing consumers more control over their financial data and mandating that banks and financial services providers make data available to authorized third parties.

Currently, there is an imbalance of power between financial services and customers, in which customer data has been used for cross-selling and other marketing purposes by financial institutions, often with limited transparency for consumers and their ability to view or revoke permissions granted for data sharing. There is also currently no standard definition of customer data that must be made available to authorized third parties nor is there a mandated method to make data available. In the past, this has led to aggregators and third-party providers using “screen scraping” and housing large amounts of customer credentials, among other challenges.

A less risky way of making customer data discoverable through application programming interfaces (APIs) has been gaining traction in the marketplace, but lack of standards and investments required has slowed the adoption throughout the industry.

The 1033 rule aims to alter how consumer financial data is managed and shared across institutions, centering on consumer choice, data privacy, and security. Based on the proposed rule’s draft requirements, there are three domain implications that financial institutions need to address to successfully implement the CFPB’s requirements: (1) evaluating infrastructure and architecture, (2) enhancing operational capacity, and (3) optimizing data security.

We anticipate financial institutions that can address all three domains will be positioned to win in the marketplace with elevated customer experiences, value-driven business models, and consumer trust. We also anticipate that fintechs playing the role of data aggregators will be reexamining their business processes as new standards are introduced.

The 1033 CFPB rule

The current US financial services industry is highly centralized, with incumbents owning and controlling a substantial portion of customer data. Large data aggregators hold the necessary relationships to gather and transfer data from data providers to authorized third parties. The regulators are helping to facilitate and accelerate open banking in a way that provides better safeguards and benefits for consumers, which is driven by newly established CFPB requirements, will provide consumers with control over their financial data, and will open the market to a variety of new players bound by stringent data protection protocols.

What is open banking? Open banking is a concept that involves the collaborative sharing of consumer banking, financial, and transactional data between financial institutions and third-party financial service providers. It:

- Allows consumers to share their financial information securely with authorized third-party providers, which can include data such as account balances, transaction history, and other financial details
- Creates a more competitive and innovative financial ecosystem by breaking down barriers for consumers to grant access to their financial data

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act¹ provides the United States with a legal framework that empowers consumers to access and control their financial information with the decision-making power to securely share their data with other financial institutions and authorized third parties.

Section 1033 of the Consumer Financial Protection Act is a statute that requires the CFPB to promulgate rulemaking (i.e., a regulation) with respect to consumer financial data rights. The statute itself does not establish detailed regulatory compliance requirements; rather, such requirements will come from the regulation to come. In this regard, the name of the proposed regulation is the Personal Financial Data Rights Rule, which coincidentally, the CFPB proposes to establish as a regulation located at 12 CFR 1033. The proposed rule has two primary provisions:

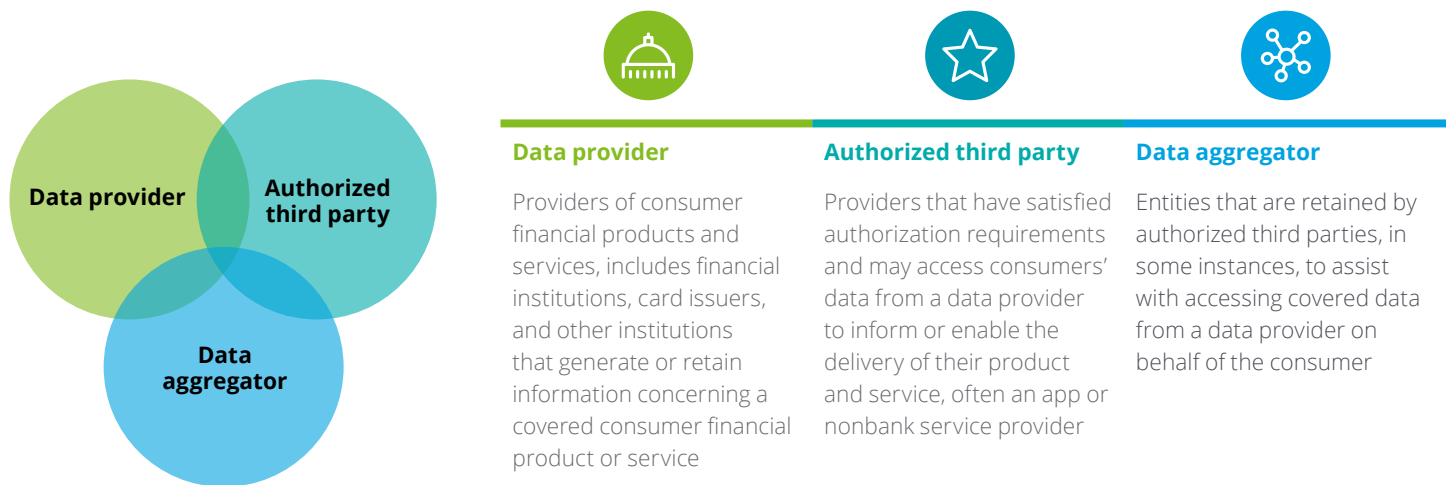
- Requires data providers to make covered data available to consumers and authorized third parties upon request
- Sets obligations of third parties that would access covered data on behalf of a consumer, including limitations on collection, use, and retention of covered data

Guidance around these provisions will be set forth by an industry standard-setting body established by marketplace institutions diversified in size and distinction. This will include financial institutions, nonbanks, and consumer and public interest groups with expertise in consumer protection and financial services,

allowing for collaboration among varied perspectives and a more open consumer banking market (figure 1). The industry will focus on not only achieving a balance of expertise, but also CFPB recognition.

Figure 1: Key stakeholders

All defined stakeholders must comply with the proposed rule



These categories are **not mutually exclusive** as defined in Section 1033. To the extent that a financial institution requests consumer data to inform or enable the delivery of a product and service, a data provider may also function as an authorized third party.

Each stakeholder must adhere to a common definition of covered data as defined by Section 1033. Covered data has been defined as information that a data provider will be required to provide to a consumer and authorized third party, which includes basic account information, transaction information, terms and conditions information, and upcoming bill information. Products and services in scope are those defined within Regulation E, Regulation Z, and facilitation of their respective payments—more specifically,

deposit accounts (i.e., checking, savings, other consumer asset accounts), prepaid accounts (i.e., payroll cards, government benefit cards, multiple unaffiliated merchant cards or cards that can be used at ATMs), credit cards, including hybrid prepaid credit cards, and the facilitation of payments from a Regulation E account or Regulation Z credit card.

Current market situation

Consumer impact in current market: Changes to consumer controls of financial data are required, in part, due to customer concerns with current marketplace actions.

- The lack of consumer autonomy over data has created circumstances of data abuse by data providers and aggregators. Specific circumstances include password storage and loss, transaction data used for cross-selling, and sale of data without consumer consent.

Acceleration of open banking in foreign markets: Regulatory and market-driven changes in foreign markets may provide a window into the future for what lies in store in the US financial ecosystem.

- In Europe, the revised Payment Services Directive (PSD2)² has driven open banking adoption since 2018. We have seen notable improvements within data protection and fraud prevention as initial use cases, as well as a steadily increasing adoption of Variable Recurring Payments.

Implications of the CFPB rule for your organization

There are three essential domains that financial institutions need to master to drive open banking adoption: (1) evaluating infrastructure and architecture, (2) enhancing operational capacity, and (3) optimizing data security.

Evaluating infrastructure and architecture

As set forth by the 1033 rule, data providers will need to evaluate whether their institution's existing technology infrastructure is equipped for enhancements to enable adherence with 1033 requirements and scalable to fulfill a large number of consumer and third-party requests.

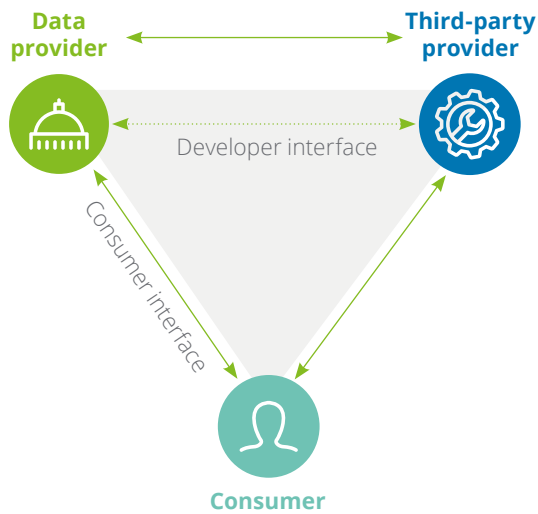
Data providers will be required to establish a consumer interface and a developer/API to facilitate the capture and subsequent sharing of covered data in a secure manner. These interfaces need to be



developed in a readable format that is widely accepted by similarly situated institutions. Given that data will now be securely shared via APIs, this prevents aggregators and authorized third parties from leveraging a consumer's credentials for "screen scraping" activities to gather covered data.

In addition, like data providers, aggregators and authorized third parties will need to institute an information security program that fulfills Federal Trade Commission (FTC) requirements;³ otherwise, data providers reserve the ability to deny a third party's request and withhold a consumer's covered financial data. Data providers will need to ensure they have the proper infrastructure and oversight in place to confirm aggregators and authorized third parties will be accessing data properly and securely.

Data providers will be required to make covered data available via distinct platforms for consumers and authorized third-party providers (figure 2).

Figure 2: Under the proposed rule, there are two ways data must be made available



 <p>Consumer interface</p> <p>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</p>	 <p>Developer interface</p> <p>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</p>
--	--

Data providers must require authorized third parties to use credentials other than those used for the consumer interface.

- Third parties must use their own access credentials to access the data provider’s developer interface instead of logging in as the consumer.
- Third parties will need to gain proper authorization from consumers and data providers to obtain access to consumer financial data and may only do so in relation to a product and/or servicing acquired by the consumer.

For your organization, it is critical to evaluate whether your institution’s infrastructure is ready to enable build-out of an API ecosystem as required above by the 1033 rule.

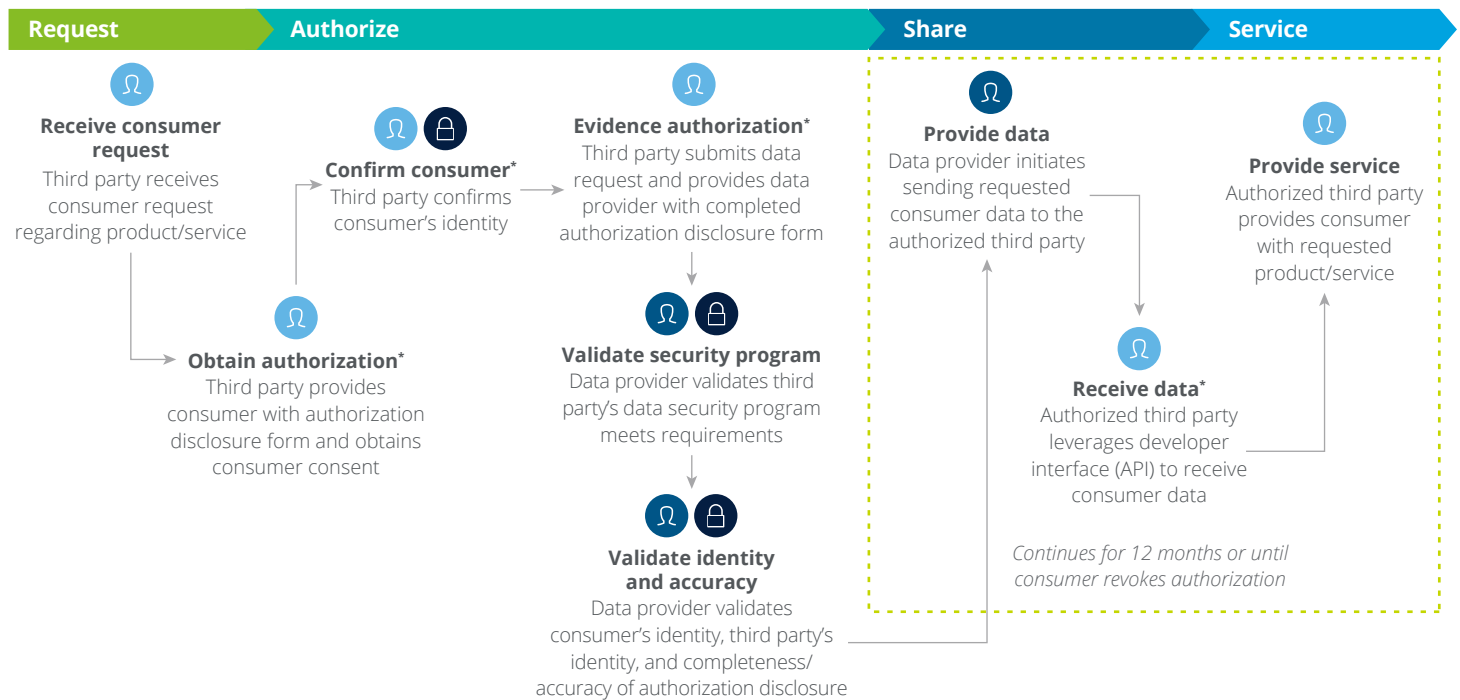
Enhancing operational capacity

With approximately 108 million⁴ fully banked US households, data providers will need to ensure they are ready to manage the intake, fulfillment, and risk oversight of third-party consumer data requests.

The 1033 rule outlines additional requirements for data providers to validate an authorized third party's identity, authorization status, and respective information security programs before permitting access to a consumer's financial data. Data providers will need to assess their existing operating models, consumer interface(s), and data footprint to identify needed changes to address technical scalability, staffing, and cyber/data control gaps.

Furthermore, the 1033 rule outlines a new process for authorized third parties to request, authorize, share, and service consumer data from data providers. The process provides additional layers of protection to the consumer when sharing data and controls how consumer data is used by third parties and data providers (figure 3).

Figure 3: Covered data request from third party



Ω Third party ⊙ Data provider 🔒 Control

* Indicates instances where data aggregator could be leveraged.

Data providers should ensure data accessibility standards remain effective to safeguard consumer information and avoid potential noncompliance and reputation risk. Access controls should be strictly enforced through verification of consumer consent with their respective third party.

For your organization, it is critical to evaluate whether your institution's operational capacity is aligned with 1033 rule requirements outlined above and to make necessary enhancements as needed.

Optimizing data security

While safeguarding and privacy rules around the collection and use of consumer financial protected data is not new, the proposed rule intersects with existing regulatory standards (e.g., Fair Credit Reporting Act, Gramm-Leach-Bliley [GLBA]) should a breach of this data occur. Organizations will be required to enhance established data privacy programs to monitor and prevent unauthorized access. Data providers must have a data and information security program consistent with Section 501 GLBA⁵ or FTC Standards for Safeguarding Customer Information 16 CFR 314.⁶

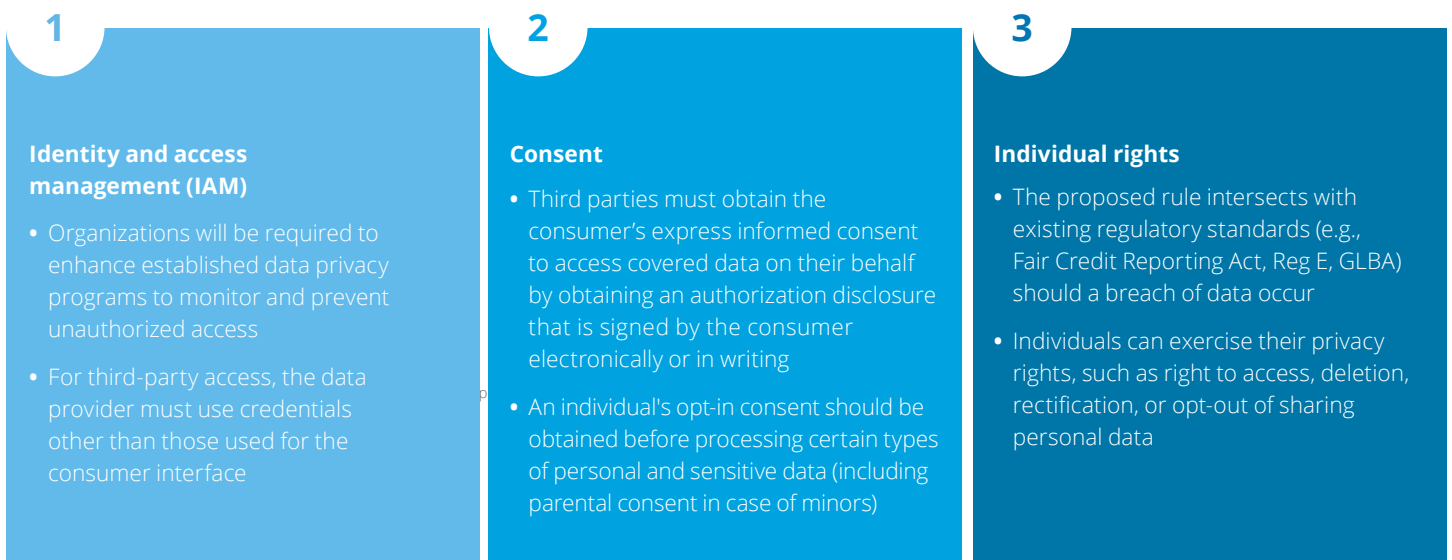
There are heightened expectations that data providers, data aggregators, and third parties have the proper information security programs in place to safeguard the transmission and retention of consumer financial data. In certain cases, this may require an enterprisewide, systematic, streamlined, and coordinated approach to privacy and security.

Third parties and data aggregators (where applicable) must obtain consumers' express informed consent to access covered data via an Authorization Disclosure. Consumers have the right to revoke third-party access at any time, and authorizations should be renewed each year.

Throughout the open banking ecosystem, data should be held and transmitted according to published encryption standards, and parties should use multifactor authentication when receiving consumer data. It is paramount that all parties receiving, storing, and using consumer data remain up to date and compliant on all relevant data transmission protocols. Many industry participants will need to focus on security, use, and oversight of consumer financial data to meet industry standards.

For your organization, it is critical to evaluate whether your data security capabilities are aligned with 1033 rule requirements outlined above (figure 4).

Figure 4: Considerations for privacy and data protection in open banking



Timeline for your organization to comply with the CFPB rule

Organizations need to start planning and working on their compliance journey now. Regulatory deadlines are close, requiring complex changes and capability enhancements for organizations.

expected in fall 2024 (figure 5). By the end of the compliance period, institutions are expected to comply across technical and operational aforementioned requirements.

Within the 1033 rule, the CFPB proposed staggered compliance dates for financial institutions, ranging from six months to four years, based on an institution's asset size or revenue. The compliance period will start once the CFPB ratifies the rule change, which is

Figure 5: CFPB proposed compliance period

Institution asset size/revenue	Compliance period*	Estimated no. of depository institutions
At least \$500B in assets/\$10B in revenue (Tier 1)	6 months	8
Between \$50B and \$500B in assets/<\$10B in revenue (Tier 2)	1 year	37
Between \$850M and \$50B in assets	2.5 years	1,109
Less than \$850M in assets	4 years	3,485

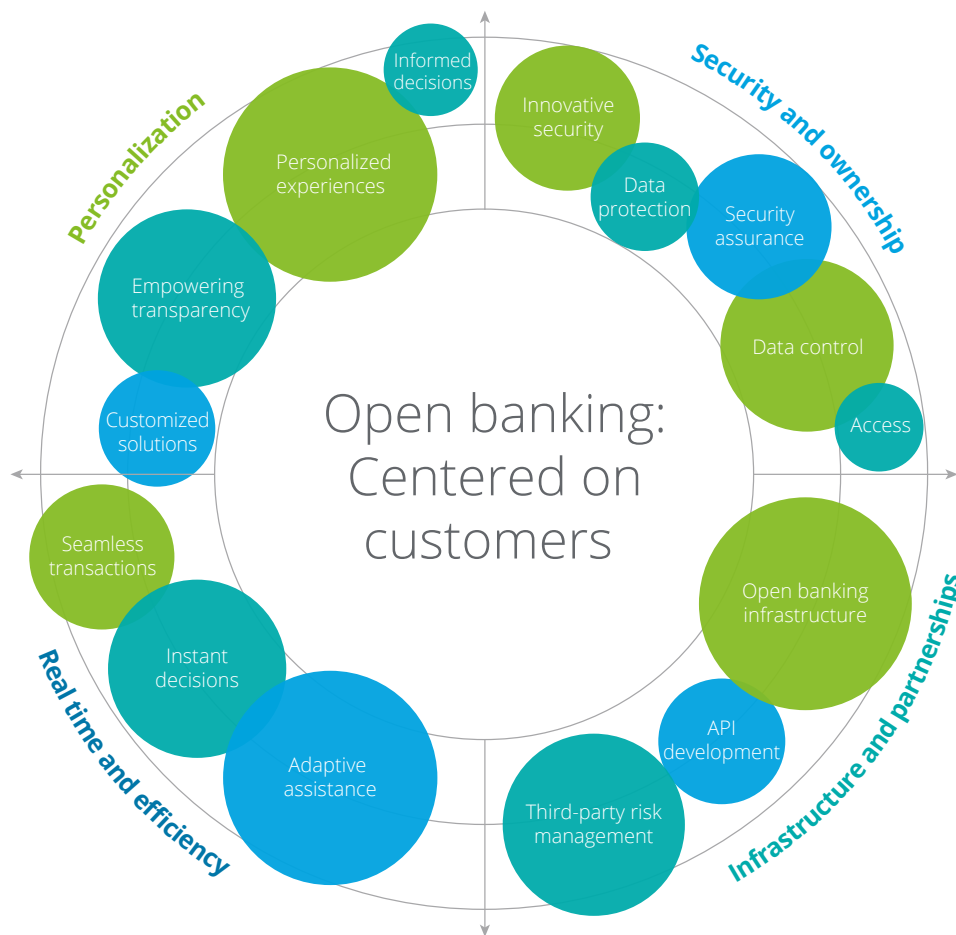
*Compliance period to begin once Section 1033 is finalized, which is expected fall 2024.

Maximizing the value of open banking to turbocharge growth

Beyond the compliance aspect of the regulations, implementing requirements defined by the CFPB 1033 rule will create value for financial services by fostering innovative and value-driven use cases.

We believe there are four major use case areas that open banking can unlock (figure 6): personalization, security and ownership, real time and efficiency, and infrastructure and partnerships.

Figure 6: Open banking use case themes



Personalization

Open banking will enable the activation of personalized experiences that will foster customer engagement and enable brands to drive conversion:

- Frictionless provider switch and onboarding experiences enabling customers to work with brands they love.
- Aggregated financial insights enabling customers to better manage their wealth.

- Dynamic pricing for financial products to drive conversion and maximize customer value.
- Personalized loyalty and rewards programs that drive customer retention and engagement.

Security and ownership

Consumer trust is paramount, and financial institutions have a key role in building and maintaining that trust. The CFPB 1033 rule enables enhanced security use cases:

- Security protocol standards to improve data safety across the ecosystem.
- Improved fraud analytics to lower risk and costs for financial institutions and consumers alike.
- Secure single sign-on that enhances customer experience, maximizes engagement, and promotes sales.
- Consumer-owned tracking of data access and approvals to drive increased trust across financial services.

Real time and efficiency

Enhanced availability of consumer data will improve credit risk experiences, enabling financial institutions to make faster credit decisions:

- Variable recurring payments and account-to-account (A2A) payments to lower transaction costs.
- Universal checkout experience to provide improved personalization and sales opportunities.
- Efficient, real-time underwriting, lowering costs and increasing success for financial institutions.
- Faster, improved business processes (invoicing, billing, budgeting, CRM data entry, KYC, collections, etc.), lowering costs and improving efficiencies for businesses across the economy.
- Faster, improved client servicing (refund/dispute management, loyalty and rewards integrations), lowering costs for businesses and improving customer experiences.

Infrastructure and partnerships

Retail banks and financial institutions will partner with third parties or develop the infrastructure internally to securely transfer financial data and support the open banking ecosystem:

- Increased/improved back-end IT infrastructure, providing an opportunity for larger financial institutions.
- API development/integrations, allowing institutions to partner with third parties, create innovative new products, and control for risk and security.
- Third-party risk management partnerships for financial institutions to maintain leadership in open banking.

Open banking redefines the financial landscape with unprecedented customer focus in which secure access to data will help unlock tailored financial services experiences. As customers are looking for personalized and trustworthy experiences, players aligned with the necessary requirements will likely benefit from growth opportunities and prevent themselves from slipping behind a rapidly changing industry.

Getting started

Organizations are at different levels of preparedness. We developed a priority checklist to help guide your organization's readiness assessment. Below is a list of questions you can use to assess your current state and plan on how to meet regulatory requirements:

- Do you know how the 1033 rule applies to your organization?
- Have you identified your API strategy for connectivity with third parties? Will you need to update existing systems or implement new systems?
- Does your consumer consent strategy comply with Section 1033 requirements?
- If applicable, do you have a portal in place for aggregators and authorized third parties to connect?
- Have you forecasted expected request volumes and throughput? Are your systems scalable to this expected volume?
- What are the operational impacts to any new or enhanced process?
- Do you have the resources, operational capacity, and technical scalability in place?
- Does your risk approach comply with Section 1033 requirements?
- Are you prepared to fulfill all Section 1033 requirements within your applicable compliance period?

We can help you navigate these considerations and more to address compliance requirements and win in the marketplace. Our experience in open banking, CFPB compliance, and managing the execution and operations of large-scale banking programs positions Deloitte as a one-stop shop for open banking engagements of any size or complexity. Our service offering ranges across open banking regulatory, technology, operations, strategy, and innovation to help your firm enhance open banking readiness and maximize growth opportunities.

- We provide banks with a ready-made solution to streamline data aggregation and more efficiently manage data storage.
- Our AI/machine learning solutions built on top of the data storage platform will enable banks to create a more personalized, holistic customer experience, proactively target fraud and scam risks, and realize operational efficiencies via enhanced customer servicing.

Regardless of where you are on your journey, we are here to help you maximize the value of open banking.

Contacts

John Graetz

Principal
Deloitte & Touche LLP
jgraetz@deloitte.com

Ulrike Guigui

Managing Director
Deloitte Consulting LLP
uguigui@deloitte.com

Shaun Nabil

Managing Director
Deloitte & Touche LLP
snabil@deloitte.com

Tim O'Connor

Principal
Deloitte Consulting LLP
tioconnor@deloitte.com

Menes Etingue Kum

Senior Manager
Deloitte Consulting LLP
metinguekum@deloitte.com

Nora Linkous

Senior Manager
Deloitte Consulting LLP
nlinkous@deloitte.com

Devan McCurry

Manager
Deloitte & Touche LLP
dmccurry@deloitte.com

Contributors

Danny Cho, Consultant, Deloitte Consulting LLP
Lauren Holohan, Principal, Deloitte Consulting LLP
Sohail Kagzi, Managing Director, Deloitte Consulting LLP
Jake Leshem, Senior Consultant, Deloitte Consulting LLP
Jake Pandrok, Consultant, Deloitte & Touche LLP
Manpreet Singh, Managing Director, Deloitte Consulting LLP
Jon Valenti, Principal, Deloitte Consulting LLP
Shalina Vadivale, Senior Manager, Deloitte Consulting LLP

Endnotes

1. Consumer Financial Protection Bureau (CFPB), "[Required Rulemaking on Personal Financial Data Rights](#)," proposed rule, October 31, 2023.
2. European Parliament and Council of the European Union, "[Payment Services Directive \(PSD2\)](#)," Directive (EU) 2015/2366, November 25, 2015.
3. Federal Trade Commission (FTC), "[FTC Safeguards Rule: What your business needs to know](#)," May 2022.
4. Federal Deposit Insurance Corporation (FDIC), "[2021 FDIC National Survey of Unbanked and Underbanked Households](#)," last updated July 24, 2023.
5. Gramm-Leach-Bliley Act, Pub. L. 106-102, 106th Cong. § 501(b). See Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), and Federal Deposit Insurance Corporation (FDIC), "[Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice](#)," March 29, 2005.
6. FTC, "[Standards for Safeguarding Customer Information](#)," May 23, 2002.



About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.