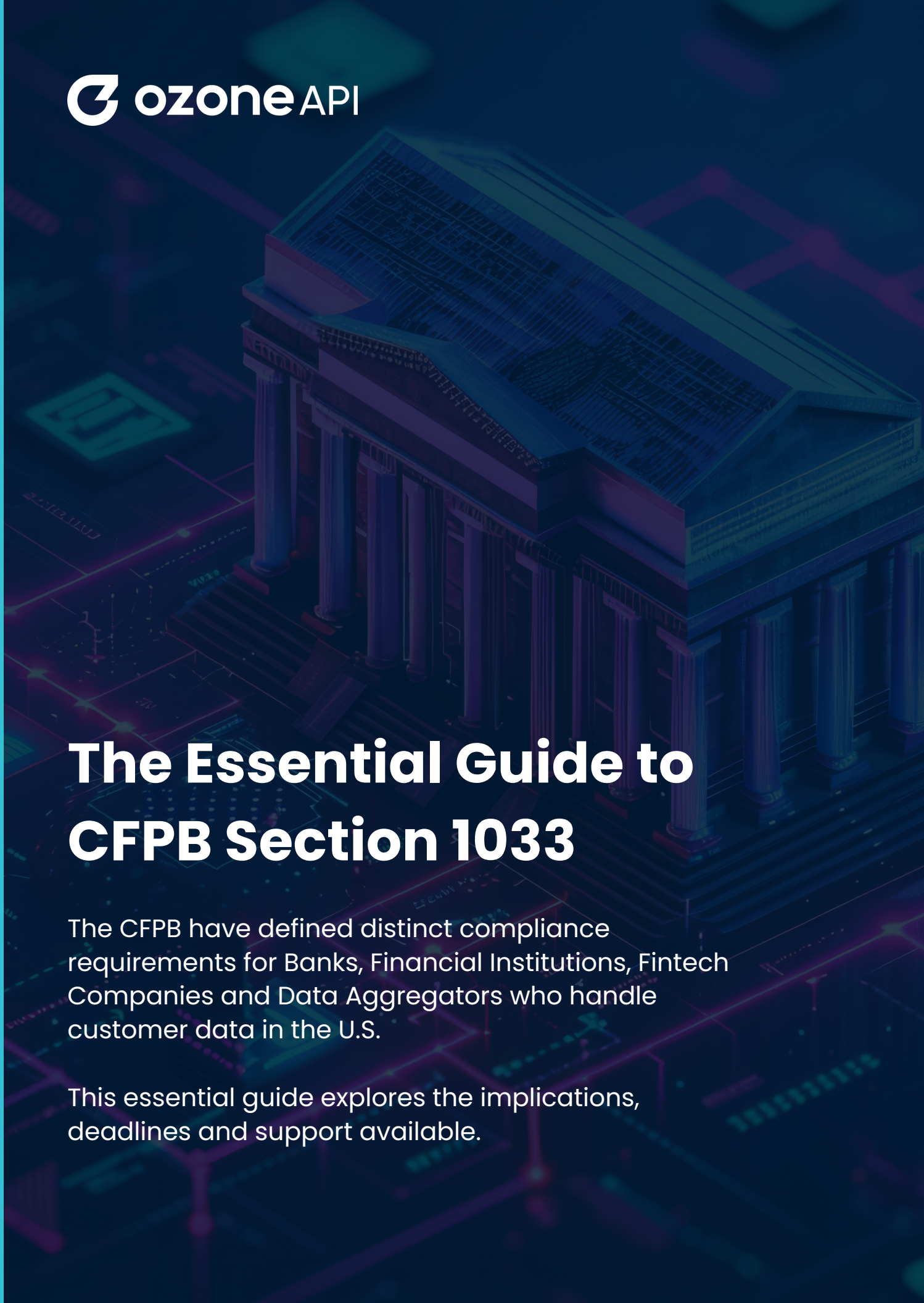
ozone API



# The Essential Guide to CFPB Section 1033

The CFPB have defined distinct compliance requirements for Banks, Financial Institutions, Fintech Companies and Data Aggregators who handle customer data in the U.S.

This essential guide explores the implications, deadlines and support available.

# Contents



# 01. Introduction

In October 2023, the U.S. Consumer Financial Protection Bureau (CFPB) proposed rules to implement Section 1033 of the Consumer Financial Protection Act, more commonly referred to as the Dodd-Frank Act. This Section provides the basis for the establishment of Personal Financial Data Rights, marking the beginning of regulated open banking in the United States. Key points include:

- Consumer Control: Provides consumers the right to securely access and share their financial data with whomever they choose.
- Security Measures: Requires the use of secure APIs and robust data protection protocols in place of insecure legacy methods.
- Common Standards: Demands the establishment of a qualified industry standard for those APIs and mandates adoption.
- Transparency and Consent: Ensures that consumers have full knowledge and control over how their financial data is being shared.

In this white paper, we explore the implications for financial consumers, fintech companies, and financial institutions, and how they can prepare for the upcoming regulatory changes.

# 02. Who is the CFPB and what is their role in the proposed Section 1033 rule making?

The Consumer Financial Protection Bureau (CFPB) is a government agency created by the Dodd-Frank Act to protect people who use financial products and services, including bank accounts, loans and credit cards. The Dodd-Frank Act was passed by the US Congress in 2010 following the 2007-2008 financial crisis to ensure a safer financial system. The CFPB's role is to ensure that banks follow these rules.

Section 1033 of the Dodd-Frank Act grants consumers the right to access their financial data, including account details, transactions, and balances. The CFPB has the authority to issue rules governing these data rights. Since 2016, the CFPB has been working on implementing Section 1033, including publishing consumer protection principles and holding panels on financial data access. Key milestones include releasing rule making proposals in 2022 and convening a Small Business Review Panel in 2023.

The proposed rule, set to be finalised in late 2024, aims to establish a framework for secure, standardised data sharing through APIs, empowering consumers to control their financial data. This rule will require financial institutions and certain payment facilitators to make data accessible to consumers and authorised third parties, promoting competition and innovation in financial services while enhancing consumer protections.

# 03. What is 1033 in open banking?

Section 1033 of the Dodd-Frank Act is specifically targeted at open banking in the United States. It allows consumers to access their financial data and share that data with third parties.

The CFPB's proposed rule also obliges banks, third-parties and aggregators to protect personal financial data from unauthorised access and data breaches, both through the adoption of secure API protocols as well as via appropriate data governance processes. The goal of Section 1033 is to make banking more transparent, in turn driving more competition and innovation in the financial ecosystem. It helps consumers find better financial products and services, make smarter financial decisions, and have more control over their financial information.

# 04. How are personal financial data rights affected under Section 1033?

A quick overview of how consumer rights are affected under section 1033:

## Access to financial data

Consumers are able to access data such as account balances, transaction histories, bill payments and detailed product information held by banks.

## Control over data sharing

Consumers may allow third-party applications and services of their choosing, such as budgeting tools, to access their financial data wherever it is available.

### Consent and revocation

Consumers must express informed consent before they share data, and are able to revoke that consent at any time, resulting in a notification to data holders.

### Transparency

Banks and third-party providers must inform users what data they collect and how it is used. Users must be aware of what data is being used and why.

### Data protection

Banks must protect consumer data from unauthorised access and data breaches by using secure APIs. Third-parties cannot use that data for advertising or cross-selling.

### Compliance and enforcement

The Consumer Financial Protection Bureau (CFPB) ensures banks follow these rules and protects consumer financial rights to ensure a level playing field in the financial sector.

## 05. Types of data covered under Section 1033

Under the CFPB's 1033 open banking standard, the following types of financial data are covered, and must therefore be made available via API by data providers such as banks:

### Types of data providers

A data provider is any institution that offers a deposit account (Reg E), a credit card (Reg Z), or can facilitate a payment from either of these two, such as a digital wallet.

### Account information & balances

Account information, including account numbers and types, and respective balances. Account types in scope include credit, debit, prepaid and deposit accounts.

### Transaction histories

Records of all deposits, withdrawals, and purchases made through customers bank accounts for at least 24 months.

### Payment initiation information

Information necessary to initiate a payment from an account using electronic fund transfers (EFTs), prepaid accounts and gift cards/certificates.

### Bill information

Details about bills, including those historically paid and those scheduled to be paid in the future, including payee information.

### Account verification information

Basic account verification information associated with your financial accounts, such as name, address, and contact information (but not date of birth).

### Terms and conditions

Information about account types and products, Including applicable fee schemes, reward programmes and annual percentage rates.

These data types enable consumers to have a comprehensive view of their financial status and the sharing of this information with third-parties facilitates significant financial benefit and improved financial health for the economy as a whole.

## 06. Compliance requirements

The CFPB has defined distinct compliance requirements for Banks and Financial Institutions, Fintech Companies and Data Aggregators.

### Banks and financial institutions

The Section 1033 open banking standards change how banks and financial institutions handle customer data. Banks must allow their customers to use secure application programming interfaces (APIs), based on a qualified industry standard, to share data safely with third-party apps and services at no cost. They are required to protect customer data from unauthorised access and data breaches. Before granting third party access to consumer data, banks must get clear consent from customers and explain what data they collect and how it is used, as well as validating the identity of the consumer and the third-party as part of the request. They must provide developer portals for their APIs, including documentation and support mechanisms. Banks must prepare for regular audits and reporting to the CFPB to demonstrate compliance with the 1033 open banking standards. This involves maintaining detailed records of data access and sharing activities.

## Data Aggregators

Under CFPB's proposed rule, Data Aggregators (companies that collect and organise financial data for third-party applications) must follow strict security measures to protect consumer data and ensure it is shared only with authorised third-party services. This introduces specific requirements for Third-Party Risk Management (TPRM) which will significantly impact both banks and aggregators, as well as third-parties, meaning all parties will need to work together to provide a seamless and secure data-sharing experience for consumers. The technical mechanisms by which these TPRM requirements will be implemented are still to be determined, with the CFPB giving no explicit direction regarding a third-party registry or directory such as those introduced in other regions.

## Fintech companies

Fintech companies are able to access consumers' financial data through secure, standards-based APIs; however, they are required to get clear consent from consumers before accessing their data, ensuring users are aware of what data is being shared and why. There must be clear mechanisms to revoke that consent at any time, and the consent must be renewed every 12 months. When the status of a consent is changed, a notification must be broadcast to all affected data providers. Fintechs or other third-parties cannot collect any more data than is necessary, and cannot use that data to advertise, cross-sell or for any other secondary use. They are also required to follow strict security rules to protect data from unauthorised access and breaches, and must keep detailed records.

# 07. When will the CFPB's proposed rule come into effect?

At the time of writing, the CFPB has not given an exact date as to when the proposed rule comes into effect, although it is expected to be implemented in late 2024.

Whilst the exact dates have not been confirmed, the CFPB have created a tiered timeline of compliance dates, varying depending on the type of company and its assets, ranging from 6 months to 4 years, making it extremely important companies stay well-informed of the most current information.

These timelines are subject to change after the final rule. The below tier list is the proposed timeline for compliance from the date the rule is implemented.

### Tier one

Depository Institutions: >$50B in assets
Non Depository Institutions: >$10B in annual revenue
Compliance timeline: 6 months

### Tier two

Depository Institutions: >$50B & <$500B in assets
Non Depository Institutions: <$10B in annual revenue
Compliance timeline: 12 months

### Tier three

Depository Institutions: >$850M & <$50B in assets
Compliance timeline: 2.5 years

### Tier four

Depository Institutions: <$850M in assets
Compliance timeline: 4 years

**Authorised third parties are required to comply within 60 days**

## 08. Challenges banks and fintech companies may face under section 1033

### Data security and privacy

Banks and fintechs will be required to implement adequate data security measures to protect financial data from breaches and hackers.Using encryption, tokenizing confidential information, and performing regular security checks will help companies stay on top of risk management concerns. Implementing governance processes focused on sound practices for data retention and disposal will further reduce risk.

### Managing consent

Users may be concerned about their data being shared, providing clear information about what data is being shared, who it is being shared with, and what it is being used for will

inevitably build trust with consumers. Offering easy-to-use controls and mechanisms for managing or revoking the consent to share their data will further improve adoption and drive consumer benefits.

### Technical integration

Banks need to create secure APIs for sharing data with third-parties, based on a qualified industry standard. Although the CFPB has not explicitly named a standard, it is very likely to be the FDX API from the Financial Data Exchange (FDX), coupled with security protocols from the OpenID Foundation (OIDF) as adopted in other regions. This requires a great deal of specialised technical skills and resources.

### Cost and resource allocation

Setting up security measures, APIs, and compliance processes can be expensive. Companies need to budget ahead to be ready for CFPB's final rule. Looking ahead, they must also recognize that adding developer interfaces such as APIs and portals is akin to adding a new channel, and will therefore require continuous improvement and investment. Rather than being perceived as a compliance exercise, firms must see this as a beginning.

## 09. How can banks, financial institutions, data aggregators and fintechs prepare for section 1033?

To prepare for Section 1033, these entities must focus on compliance with the upcoming regulations, with an eye towards moving beyond in the future. Here are the key steps:

### Implement secure, standards-based APIs

Banks and financial institutions should deploy secure APIs for data sharing based on common, shared standards, such as FDX. This ensures that consumer data is shared safely and efficiently, reducing the reliance on older methods like screen scraping and guaranteeing broad interoperability across the financial ecosystem. With Section 1033 fast approaching, financial entities should turn to compliant API providers like Ozone API to ensure implementation is efficient and successful, and that compliance is maintained on an ongoing basis moving forward.

## Obtain and facilitate clear consumer consent

All entities, including banks, fintechs and data aggregators, must establish robust processes and interfaces for obtaining and managing consumer consent, as this plays a crucial role in the CFPB vision for open banking in the United States. This includes clear disclosures about what data is being collected, how it will be used, and obtaining explicit permission from consumers before accessing their data, both on the data recipient side and the data provider side. The emphasis is on providing consumers explicit knowledge and control over how their data is shared.

## Enhance data security measures

All parties must strengthen their data security technologies to protect consumer information from unauthorised access and breaches. This involves adopting industry best-practices and staying updated with new security protocols; in particular, those published by the OIDF, including the most recent implementations of the Financial Grade API (FAPI) security profile. As the ecosystem evolves to include a registry of accredited participants and respective trust framework, work to integrate it into existing data sharing flows.

## Maintain detailed records

Prepare for regular audits by maintaining comprehensive records of data access and sharing activities. This documentation will be essential for demonstrating compliance with CFPB regulations, as well as promoting reliability, transparency and trust in the ecosystem overall. Not only will these records be valuable in developing an internal open banking strategy within an individual institution, but in the aggregate, these records will help the CFPB and market participants to drive the roadmap for future iterations of U.S. open banking at large.

## Stay informed and adaptable

Keep up with updates from the CFPB regarding the finalisation of Section 1033 rules and be ready to adapt your compliance strategies accordingly. Actively participate in any calls for feedback issued by the CFPB, which they have done periodically throughout the development of these rules. Engage with industry groups, including critical standards bodies such as FDX, and participate in relevant forums tp gain valuable insights and support from other institutions going through similar deliberations. Ultimately, open banking demands that all participants work together towards a common goal.

## Working with Ozone API

Partnering with Ozone API is the easiest route for banks and financial institutions to achieve compliance with Section 1033, while laying the foundation for a future-ready open banking strategy. As a first step, the Ozone API platform quickly and simply helps any bank implement high performing, standards-compliant APIs to ensure ongoing open banking compliance. We then help you go beyond compliance by providing industry leading security and value adding API sets to create new revenue streams and deliver an enhanced consumer data-sharing experience. Our solutions are proven with banks globally and are designed to ensure fast and simple integration with your existing technology. With Ozone API, you can truly unlock the power of open finance.

## Benefits of working with Ozone API:

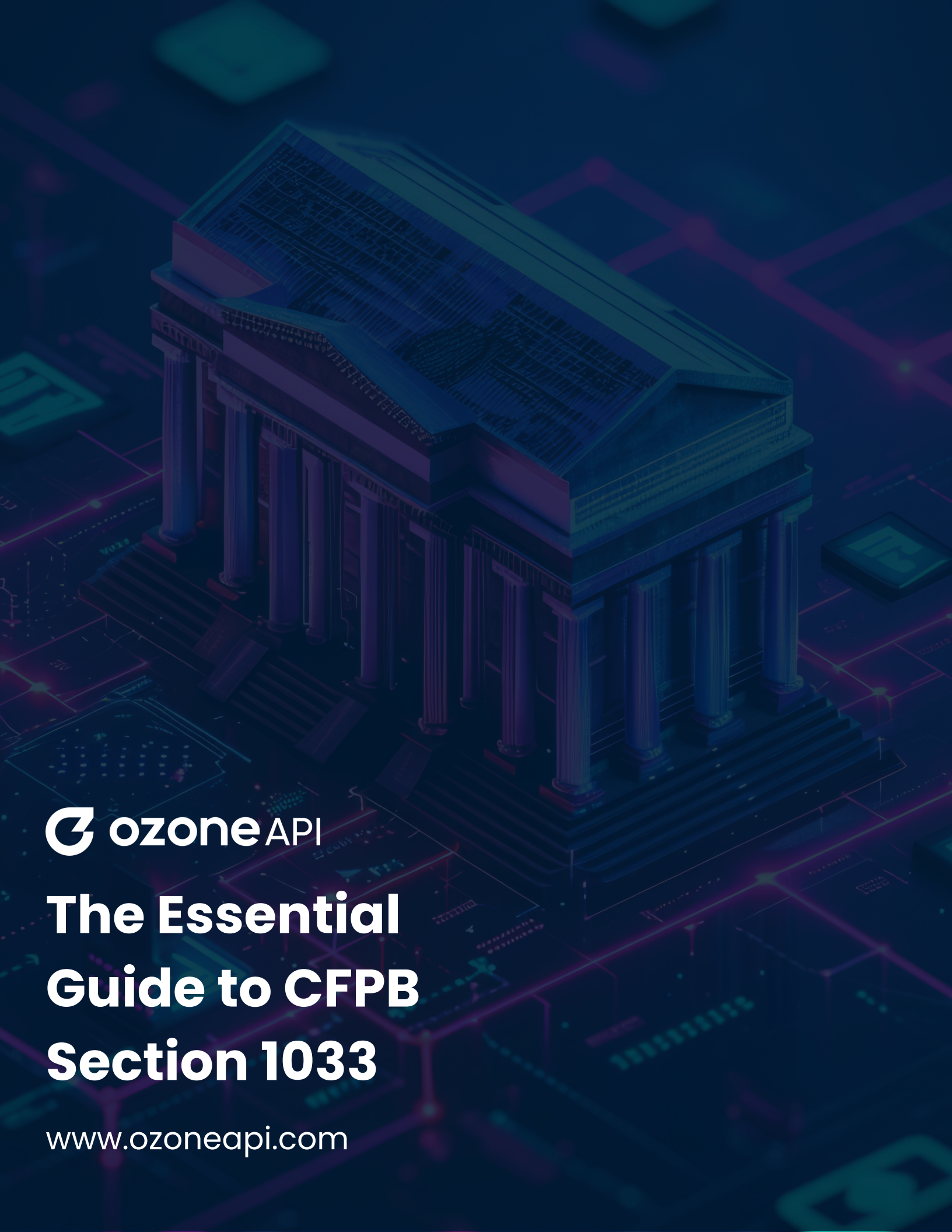
- **Cost efficiency and value**: Building in-house requires substantial investment in development and maintenance. Ozone API provides a cost-effective, ready-to-deploy solution for quick launch and competitive advantage. Our API also reduces operational costs and complexity, enabling compliance without the high expense of developing and maintaining your own framework.

- **You stay in control**: Developing in-house solutions diverts resources. Ozone API handles open banking complexities, letting you focus on strategic initiatives and customer engagement. With Ozone API, you also get a proven open banking foundation, reducing development challenges for your premium API strategy.

- **Innovation and future proofing**: Keeping up with technology and regulations demands ongoing investment. Ozone API provides cutting-edge technology and regular updates to keep your solutions current and compliant. Our APIs are always updated with new regulations and standards, ensuring future compliance as new rules emerge.

- **Trust and experience**: With extensive global experience, Ozone API is a trusted partner for achieving compliance. Our proven track record ensures your APIs meet all regulatory standards and more. Working with us also ensures smooth, efficient implementation as our expert team will handle the complexities, ensuring seamless integration with minimal disruption.

If you're confused about what this update means for you, or you want to remove the complexity of implementing Section 1033, we're here to help. Get in touch on www.ozoneapi.com



ozone API

# The Essential Guide to CFPB Section 1033

www.ozoneapi.com