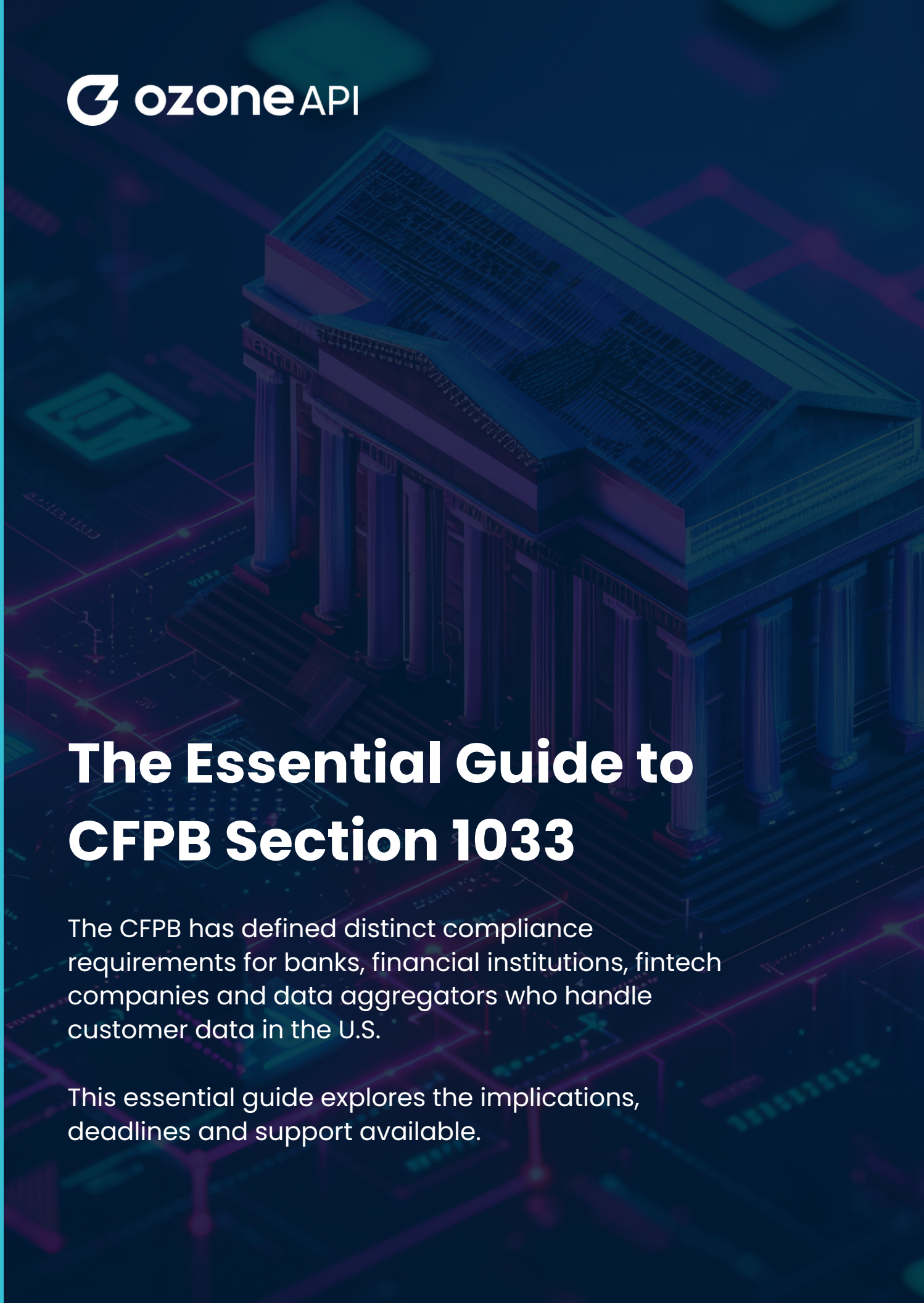
ozone API



The Essential Guide to CFPB Section 1033

The CFPB has 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

02. Who is the CFPB?

03. What is Section 1033?

04. What data rights are granted under Section 1033?

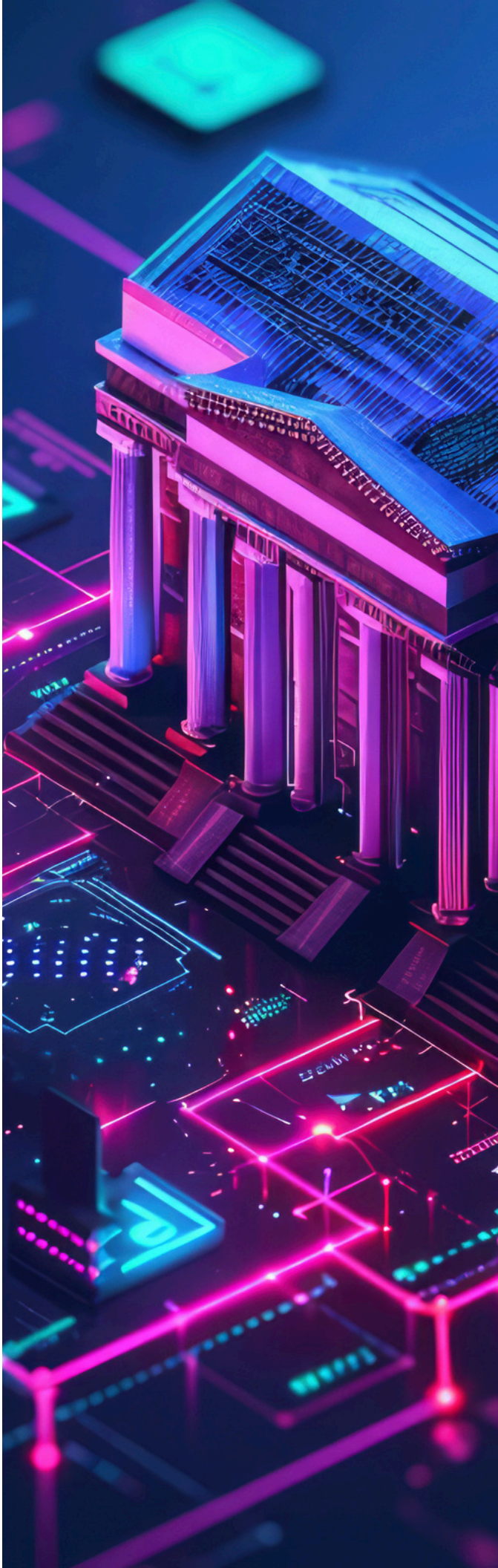
05. What does Section 1033 actually do?

06. How does Section 1033 impact financial institutions, fintech companies and data aggregators?

07. What are the Section 1033 compliance deadlines?

08. Challenges financial institutions may face under Section 1033

09. How can Ozone API help?



01. Introduction

The Consumer Financial Protection Bureau (CFPB) in the United States finalised the Personal Financial Data Rights rule on October 22nd, 2024. The rule, commonly known as Section 1033, is specifically targeted at regulating open banking in the United States, and its mission is to allow consumers to access their financial data and share that data with third parties.

In this guide, we explore the implications for financial consumers, fintech companies, and financial institutions, and what they now need to do.

02. Who is the CFPB?

The Consumer Financial Protection Bureau (CFPB) is a government agency created by the Dodd-Frank Wall Street Reform and Consumer Protection 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 2008 financial crisis to ensure a safer and more responsible financial system.

One of the CFPB's primary roles is to ensure that banks follow the provisions set out in Dodd-Frank, including through rule-making which facilitates the clarification or enforcement of those provisions. It is this rule-making process which ultimately led to the release of Section 1033.

03. What is Section 1033?

Section 1033 of the Dodd-Frank Act grants consumers the right to access their financial records upon demand, including account details, transactions, and balances. Under Section 1033 of Dodd-Frank, the CFPB has the authority to issue rules governing data rights related to the portability of personal financial information. Since 2016, the CFPB has been working on implementing Section 1033, including publishing consumer protection principles and holding consultations on financial data access.

The CFPB's final rule, officially called the Personal Financial Data Rights rule, is now known as Section 1033. It obliges banks, third-parties and aggregators to support the sharing of financial data while protecting that data from unauthorised access and data breaches, both through the adoption of secure API standards and protocols, as well as via appropriate data governance processes.

The goal of Section 1033 is to make banking across institutions more interoperable and 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. What data rights are granted under Section 1033?

The full name of the Section 1033 rule is Personal Financial Data Rights. This is because it grants consumers certain rights over how their financial data is shared, handled and used by financial institutions, service providers and third-parties.

Below is an overview of how consumer rights towards their financial data are specifically 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 financial institutions (see below for more details).

Control Over Data Sharing

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

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. Granted consents must be re-authorized every 12 months.

Transparency

Banks and third-party providers must inform consumers on what data they collect and how it is used. Users must be explicitly made aware of what data is being used, who it is being shared with and for what purpose.

Data Protection

Financial institutions must protect consumer data from unauthorised access and data breaches by using secure APIs. Third-parties cannot use that data for advertising, cross-selling or any secondary use not related to the consumer's request.

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. What does Section 1033 actually do?

The rule has established a framework for secure, standardised data sharing through APIs (what the rule calls 'developer interfaces'), thereby empowering consumers to control their financial data. The rule requires financial institutions and certain payment facilitators to make data accessible to consumers and authorised third parties, promoting competition and innovation in financial services while significantly enhancing consumer protections when sharing their financial data via digital channels.

It 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.

Under Section 1033, certain types of data providers must make specific categories of personal financial data available via API, as described below:

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 (explicitly named as a type of provider).

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 a customer's 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 categories of financial data, made available across a broad set of service providers, enable consumers to have a comprehensive view of their financial status. Moreover, the sharing of this information with third-parties facilitates significant financial benefit to individual consumers, as well as promoting improved financial health for the economy as a whole.

06. How does Section 1033 impact financial institutions, fintech companies and data aggregators?

The CFPB has defined distinct compliance requirements for banks and financial institutions, fintech companies and data aggregators.

Banks and Financial Institutions

The Section 1033 rule will change how banks and financial institutions handle customer data. Banks must now 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 also 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, including the consents that customers have granted.

Data Aggregators

Under Section 1033, 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 financial institutions and third party fintech companies, as well as the data aggregators themselves, meaning all parties will need to work together to provide a seamless and trustworthy data-sharing experience for consumers.

Fintech Companies

Fintech companies, referred to in the rule as 'third-parties', 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 for what purpose.

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 unless it is explicitly related to servicing a request made by the customer (although there are some exceptions for fraud detection). Fintech companies are also required to follow strict security rules to protect data from unauthorised access and breaches, and must keep detailed records.

07. What are the Section 1033 compliance deadlines?

The CFPB has created a tiered timeline of compliance dates, varying depending on the type of company and its asset size. This makes it extremely important that financial institutions and service providers stay well-informed of the most current information to ensure they are aware of how and when Section 1033 applies to them. The list below summarizes the Section 1033 finalised timeline for compliance across the five tiers:

Tier One

Depository Institutions: >$250B in total assets
Non Depository Institutions: >$10B in total receipts in 2023 or 2024
Compliance Deadline: April 1st, 2026

Tier Two

Depository Institutions: >$10B & <$250B in total assets
Non Depository Institutions: <$10B in total receipts in 2023 & 2024
Compliance Deadline: April 1st, 2027

Tier Three

Depository Institutions: >$3B & <$10B in total assets
Compliance Deadline: April 1st, 2028

Tier Four

Depository Institutions: >$1.5B & <$3B in total assets
Compliance Deadline: April 1st, 2029

Final Tier

Depository Institutions: >$850M & <$1.5B in total assets
Compliance Deadline: April 1st, 2030

Note that financial institutions with less than $850 million in total assets under management are exempt from the Section 1033 rule.

08. Challenges financial institutions may face under Section 1033

Section 1033 introduces a number of unique challenges that affect all participants, but perhaps the most impacted are banks and financial institutions, who are now obliged to support data sharing via secure, standardized APIs, based on the consent of their customers. In their role as data providers, financial institutions will need to tackle a number of technical challenges that are distinct to open banking.

Managing Consent

Customers are likely to be concerned about their data being shared, so 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. Offering easy-to-use controls and mechanisms for managing or revoking the consent to share their data will further improve adoption and ultimately drive the consumer benefits that come from open banking.

Technical Integration

Banks need to create secure APIs for sharing data with third-parties, based on a well-established consensus 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 from delivery teams that have real-world experience with these standards.

Cost and Resource Allocation

Setting up security measures, APIs, and compliance processes can be expensive. Companies need to budget ahead to be ready for Section 1033 compliance, based on the tiers described in section 7. 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 the beginning of an ongoing evolution towards open finance.

09. How can Ozone API help?

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 and open finance 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 delivering 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:

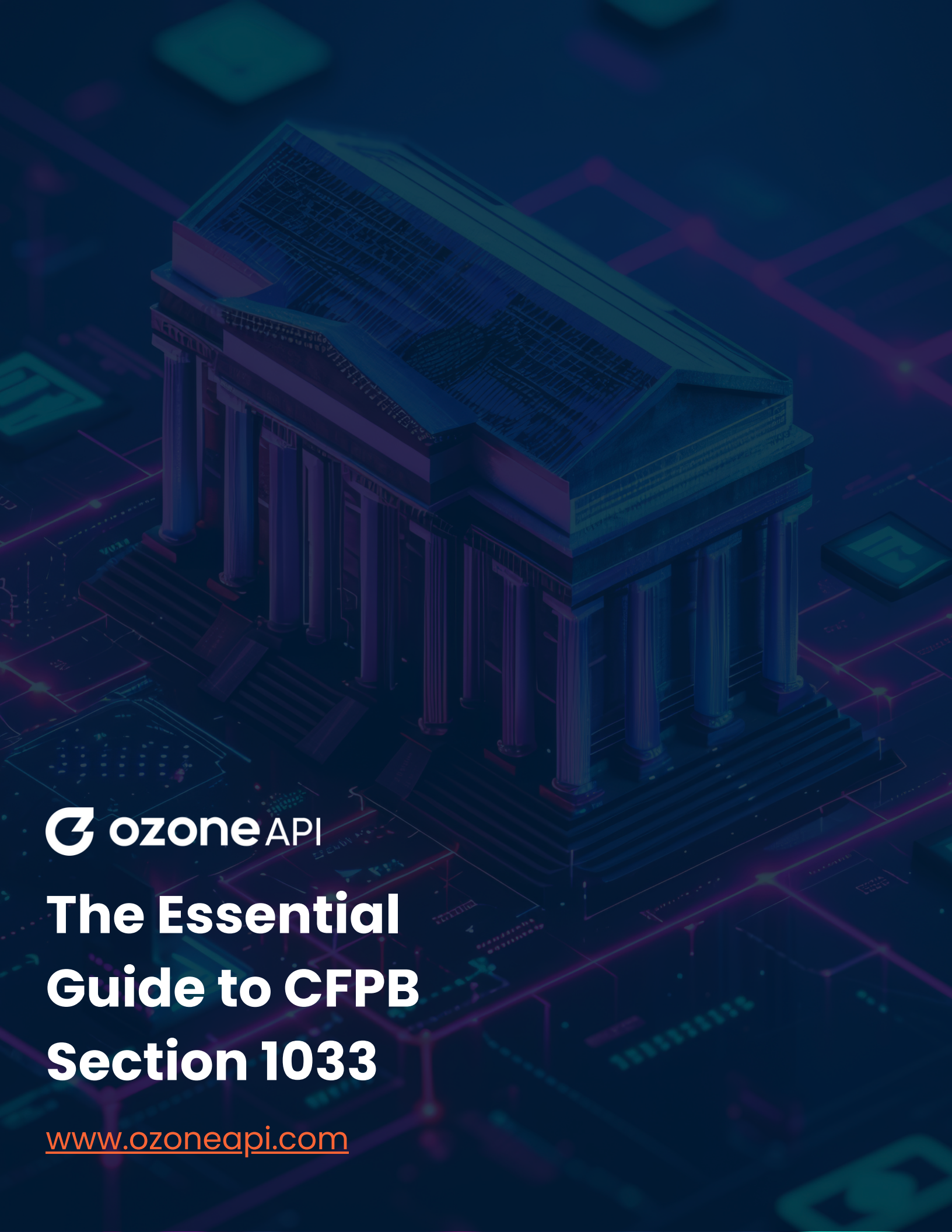
- **Cost efficiency and value**: Building in-house requires substantial investment in development and maintenance. Ozone API provides a cost-effective, ready-to-deploy solution for quick launch and competitive advantage. Our API also reduces operational costs and complexity, enabling compliance without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