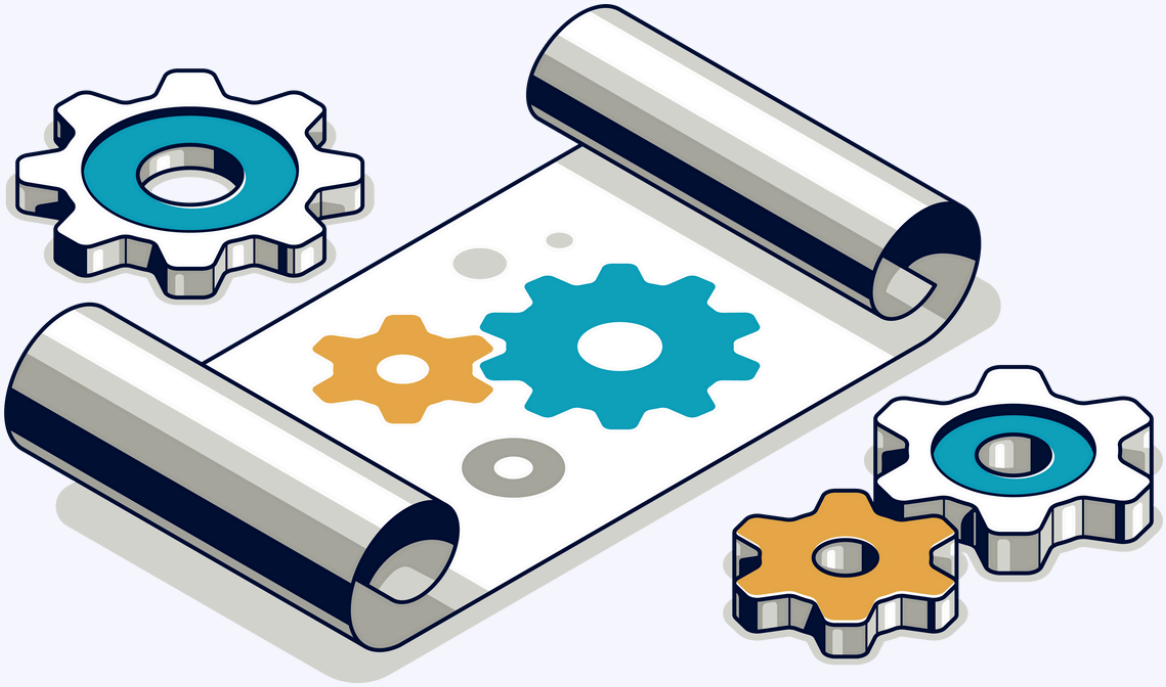
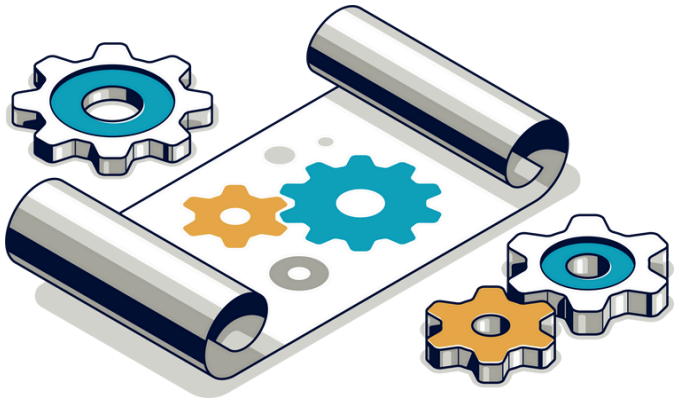
ozone API



Technical Guide to CFPB Section 1033

This guide provides insight and direction to technology teams at banks, financial institutions and other financial data-holders in the US ecosystem who are preparing to comply with Section 1033, the open banking regulation recently passed by the US CFPB.

Contents



01. CFPB Section 1033 – Personal Financial Data Rights in the United States

On October 22nd, 2024, the Consumer Financial Protection Bureau (CFPB) finalized their Section 1033 ruling on Personal Financial Data Rights, commonly understood as the introduction of regulated open banking in the US market.

The October 22nd date marked the end of a one-year review period following the release of the proposed legislation on October 19th, 2023, during which over eleven thousand responses were submitted and consulted on with stakeholders across the financial services ecosystem. Much of the original draft legislation remained untouched when the final rule was published, and the general trajectory of regulated open banking / finance in America is now fairly well understood by market participants.

Prior to Section 1033, the US market remained largely untouched by open banking regulations similar to those seen in other regions, such as Europe, Australia and Brazil. However, American consumers have been sharing their financial data with third-party providers since the nineties. Data sharing and service initiation currently exist through custom integrations, proprietary account aggregators and screen scraping. The Section 1033 ruling aims to bolster and regulate these market-driven efforts as they move towards common shared standards for the secure exchange of user-permissioned data, in part by mandating consistent data sharing for financial services providers across the industry.

For data-holding FI's who are in scope of the ruling, some aspects of the technical requirements are strongly guided by the regulatory text of Section 1033, but the CFPB has also recognised the need for widely adopted, consensus-based industry standards to support regulated open finance. With this in mind, on June 5th, 2024, the CFPB also finalized a rule outlining the required qualifications to become a recognized industry standard-setting body, which issues standards that FI's can implement in order to support compliance with the CFPB's Section 1033 Personal Financial Data Rights Rule.

Only one standards-setting body that represents a fully-fledged API technical standard has applied for recognition to the CFPB: The Financial Data Exchange, a private, non-profit commonly known as FDX. Since its inception in 2018, FDX and its members have been creating and developing open standards which underpin how open finance currently operates in the US market. As of 2024, the FDX API is used to share over 94 million consumer records, roughly 75% of the addressable market, so it is inevitable that FDX will have a key role in facilitating the US

transition to regulated open finance. Based on what is known about the final text of the Section 1033 ruling, the likely recognition of FDX as a standards setting-body by the CFPB, and the key details of the FDX technical specifications, a strong picture emerges for data-holders of what they will need to do to become Section 1033 compliant.

Section 1033 requires organizations that hold personal financial data, formally called Data Providers, to adopt standardized developer interfaces (understood to mean Application Programming Interfaces or APIs – see below) and ensure data is provided in a format using consensus industry standards. The standardized interface must facilitate a series of core technical requirements in order to achieve compliance:

- Validation of the third-party Data Recipients (i.e. those requesting the data).
- Identification of the consumer and validation of their authorization to share data.
- Make all covered data available in a format based on a recognized standard.
- Meet the minimum performance requirements for a 'commercially viable' offering.

The developer interface must also not allow a third-party to access the data provider's services by using any credentials a consumer uses to access the consumer interface (i.e. online banking), facilitating a transition away from screen-scraping while not expressly prohibiting its use outright. The implementation of the Section 1033 technical requirements can therefore be summarized as follows:

- Existing open banking standards will be used to provide the API specification.
- Third parties must be validated and authenticated as part of their data requests.
- Customer consent to share specific data sets must be captured and secured.
- Customer experience must be as seamless and intuitive as online banking.
- A suitable operating model is required to provide governance for operations.

We can gain insights into how the technology to support Section 1033 will emerge in the US ecosystem by expanding on each of these features and understanding how they are manifested in the FDX API specification, as well as in existing open banking / finance standards from other markets around the world.

02. Use of Consensus Industry Standards for APIs

The creation of open banking ecosystems is inextricably linked with the creation, description and implementation of standardized Application Programming Interfaces, or APIs for short.

All current open banking standards, including the Financial Data Exchange (FDX) standard created by and for the US market, are based on APIs that communicate over HTTP using JSON to send and receive data. OpenAPI specifications provide the basis for creating API requests and responses within the ecosystem, ensuring the required data attributes are well understood by API providers and consumers. FDX and other global standards also adopt security standards such as the Financial Grade API profile (FAPI), an OpenID Connect (OIDC) profile specifically designed for financial services and open banking use cases.

Note that compliance with a given standard's data framework is distinct from compliance with its security framework, and certification mechanisms often test these two separately.

At the time of writing, the formal certification process for FDX has yet to be finalized and, as such, it is not yet clear whether participants will need to confirm only to the data framework or to the security framework as well. The Section 1033 ruling delegates this decision to the standards body, but does in fact recognize the distinction between a data model and a secure communication protocol in its definition of standard data format.

In the vast majority of regulated open finance markets, a participant must have an assigned role granted by the local competent authority for financial services, a role which can be programmatically verified via an ecosystem registry operated by that competent authority or their delegate. Such a certification and registration mechanism allows participants to automatically enter the ecosystem once they have been verified and concretely attested they can support open finance use cases, capabilities reflected in the respective security model.

While Section 1033 recognizes the value of such mechanisms, it will likely defer these to the standards-setting body. FDX has a rudimentary member registry today, but includes on its roadmap support a programmatic ecosystem registry.

While the standards body for Section 1033 has not yet been confirmed, the Section 1033 text, as well as the subsequent standards body selection criteria published on June 5th, 2024, both outline that the standards body must be 'fair, open and inclusive'. Considering the highly-specific nature of the Section 1033 ruling, there are unlikely to be standards setting bodies outside of FDX which provide an adequate level of technical specificity. Moreover, FDX is already used to share over 94 million records in North America as of September 2024, providing it with the critical mass necessary to continue driving adoption, and therefore increasing the likelihood that FDX is recognized as a standard.

03. Authentication of Third Parties Using a Trust Framework

Agreement on the high-level technical model for communicating through APIs provides the means for establishing how Data Recipients and Data Providers can communicate securely, using a commonly agreed-upon trust framework. Third-party access has traditionally been enabled like any other API, namely through bi-lateral agreements between Data Recipients, Data Providers and any Data Aggregators. The benefit of a common trust framework is that bi-direction, proprietary trust mechanism can be largely replaced by a more scalable, consistent and secure alternative.

If the future model under Section 1033 is consistent with that in other markets, Data Recipients will likely obtain authorization through a standards body recognized by the CFPB to support the enrollment and attestation of compliance for third party participants. The authorization process is likely to involve the Data Recipient specifying their use case, the version of the technical standards they are using, as well as key contact details. The standards body may have a process for verifying the business identity alongside the specified contacts responsible for standards compliance at the organization.

As the CFPB has yet to specify which body provides this function, there may be a transitionary period whereby some form of bi-lateral agreements persist and Data Providers, as well as Data Aggregators, authorize third party Data Recipients themselves; however, this mechanism will evolve over time based on market and regulatory cooperation. Just as FDX is likely to be selected as a recognized standards setting body, they are equally likely to be responsible for establishing mechanisms for certification, registration and ongoing trust.

Once the Data Recipient has obtained authorization from the body operating the recognized trust framework, they can begin the process of integrating directly with the Data Providers upon which their open banking use case will depend. This often begins with the Data Recipient registering with the Data Provider for API access.

Registering for API Acccess

Providing API access only to authorized third parties is critical to the functioning of an open banking ecosystem, and security frameworks like FAPI, FAPI 2 and OpenID Federation are designed to help this happen seamlessly.

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.

FDX and many other open finance standards support the OpenID Connect Dynamic Client Registration (DCR) profile to facilitate API-based onboarding of third party Data Recipients with Data Providers, without the need for any registration user interface. DCR allows the Data Recipient making an API request to specify the details of the API client they want to register via the Data Provider's designated registration endpoint. The registered client details will include information like the name of the client product, description of the product, redirect URIs and logos.

This API registration process typically has multiple layers of security, including:

- Mutual Transport-Level Security (MTLS).
- Sender-constrained Access Tokens.
- Use of a recognized Data Recipient registry.
- 'Offline' approval processes (if required).

Data Recipients will first mutually authenticate with the Data Provider using certificates recognised within the shared API trust framework. This relies on Public Key Infrastructure (PKI), whereby the communication channel between the Data Recipient and the Data Provider is directly secured.

Once connectivity is established between the Data Provider and the Data Recipient, the Recipient must request an Access Token in order to register their client. The Data Provider will issue an Access Token which is strictly bound to the third party Client's certificate, which the Data Recipient can then use to register a client with a Data Provider. The information registered can be verified by the Data Provider using the registry APIs provided by the trust framework, which will maintain the certification status of the Data Recipient.

The organization details provided to the Data Provider by the Data Recipient would need to match the organization details held by the public registry at the standards setting body. While Data Providers can grant 'automatic' approval to Data Recipients that meet all of the above criteria, there is also an option to create API Clients in a 'pending' status and have a separate manual, or 'offline' review process. Once registration is complete and the registered

client is in an active authorization status, the Data Recipient can invoke the Data Provider's authorization flow to facilitate access to customer data.

Although this is how many regions operate today, note that FDX have not yet been selected as a standards setting body by the CFPB, nor have they specified the exact technical mechanisms for providing this function programmatically. However, based on their roadmap and their ongoing analysis of other regions, it is fair to assume they are heading in the same direction as regards trust framework capabilities.

Until these automated mechanisms become available, registering for API access will continue to be a largely manual process based on bi-lateral agreements between Data Recipients and Data Providers, often facilitated by Data Aggregators acting as brokers. Nevertheless, preparation for more advanced mechanisms is highly recommended.

04. Securing Customer Consent to Share Financial Data

The FDX security standard implements the FAPI 1.0 Advanced Security Profile to provide secure API access for ecosystem participants.. FAPI is already used globally in open data specifications in markets such as the UK, Australia, the MENA region and South America. Any standards body endorsed by CFPB is therefore very likely to adopt the FAPI standards.

Note that at the time of this writing the adoption of FAPI is yet to be officially required by the CFPB or FDX, and there may be a transitionary period to enable the migration of existing security mechanisms towards FAPI 1.0 Advanced as defined in the FDX standard. To that end, there may be a period where adherence to the FDX data model is sufficient to achieve certification for the purpose of Section 1033 compliance, and that adherence to the FDX security communications protocol will not be initially required.

The final Section 1033 ruling expands upon the definition of a 'standardized format' to include a secure communication protocol between Data Recipients and Data Providers, and the finalized FDX Certification process will likewise give further specificity on how both parties can achieve certification.

Regardless of whether it is required for certification or not, the FDX security standard remains highly-recommended by the standards body itself, so the remainder of this section describes how exactly it operates.

The FAPI 1.0 Advanced Security Profile is a tailored OpenID Connect and OAuth 2.0 implementation suitable for financial services use cases. The Profile builds on the core goals of OpenID Connect (OIDC) to provide proof-of-authentication and authorization by users so that data access is both secure and constrained to only the permitted data.

Data security and control is paramount in open banking, as account-holding customers are trusting their data to third parties with whom they want to do business. A standard built around the exacting requirements of FAPI enables trust, and is therefore critical to the ultimate success of open finance ecosystems.

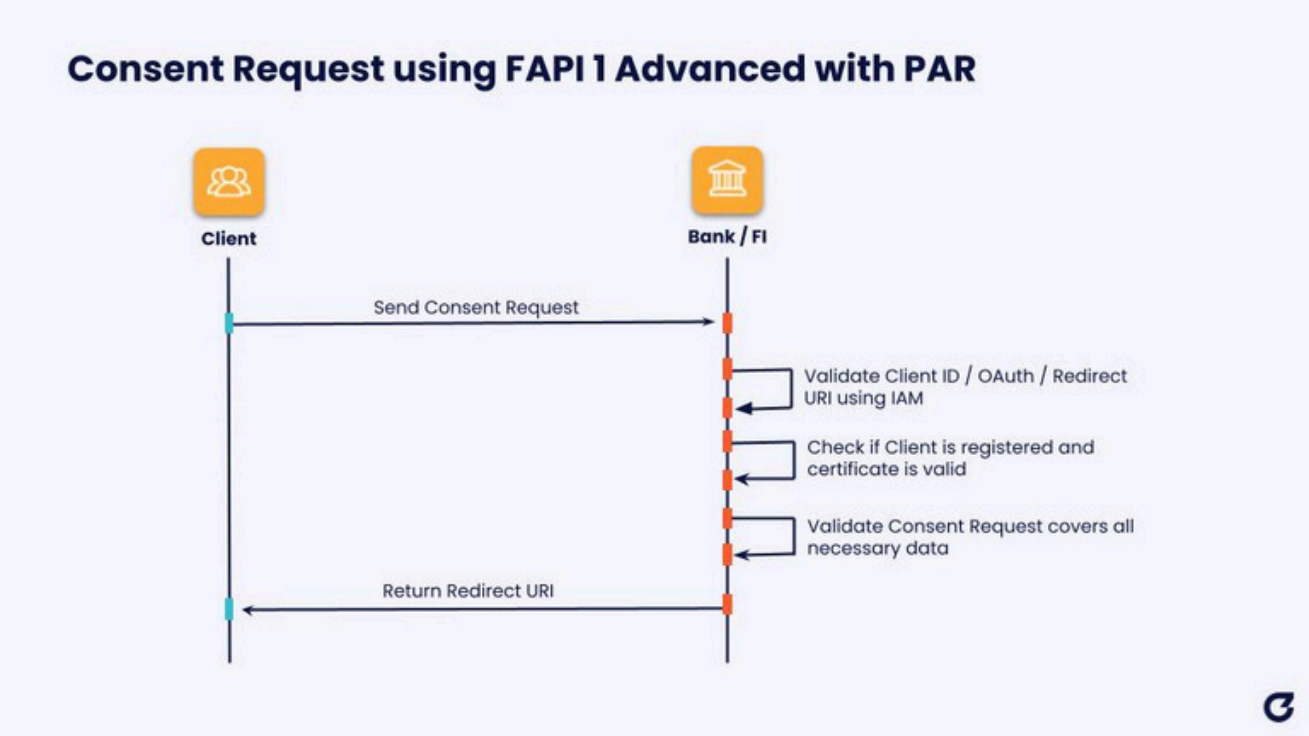
FAPI, like other OpenID Connect and OAuth implementations, mandates a specific flow that results in a Data Recipient being granted an Access Token to retrieve data from the Data Provider. In simple terms this flow implements the following three steps:

- The Data Recipient creates a Pushed Authorization Request (PAR) with the attributes of the requested data access, and sends this to the Data Provider.
- The Data Recipient then redirects the account-holding customer to the bank for authentication and authorization through an OAuth 2.0 Authorization Code grant.
- On completion of authentication and authorization, the Data Recipient can request an Access Token at the Data Providers Token endpoint to be used for data retrieval.

Pushed Authorization Request (PAR) is an OAuth 2.0 profile and an optional element of FAPI 1.0 Advanced, already adopted by many global open finance frameworks such as the Australian Consumer Data Right (CDR) and the UAE Open Finance Framework (OFF).

Although the Pushed Authorization Request (PAR) standard is optional within the FAPI 1.0 Advanced profile, the FDX security standard declares it is mandatory. PAR Requests allow the Data Recipient to send the payload of the Authorization request to the Data Provider's PAR Endpoint before initiating the Data Recipient Authorization process. The Redirect URI returned is then used in the subsequent call to the Data Provider's Authorization Endpoint.

PAR provides heightened security for transmitting Authorization request details as the payload is sent to a secure, backend URL, protecting sensitive information that would otherwise be sent in the browser.

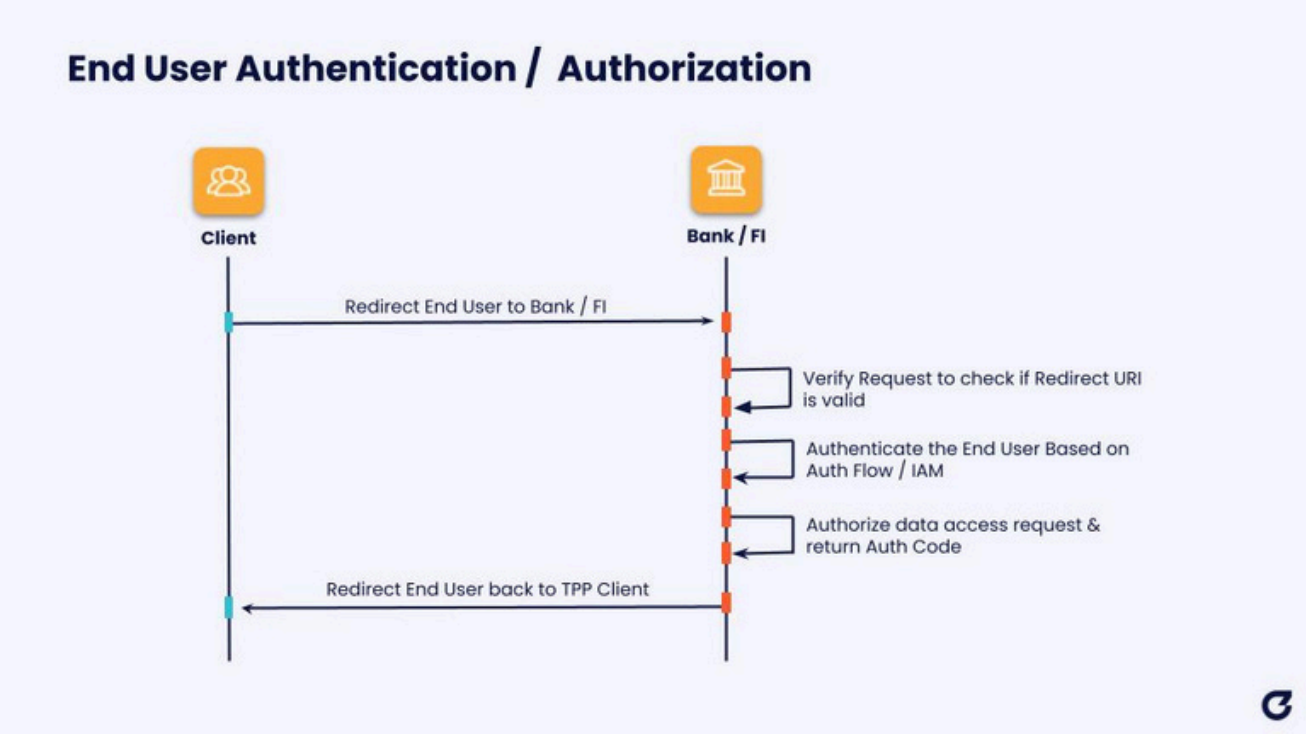


Once the PAR Request is completed, the Data Recipient invokes an Authorization Request to obtain an Access Token based on an Authorization Code grant type. In the context of FDX, the key features of the requested authorization are:

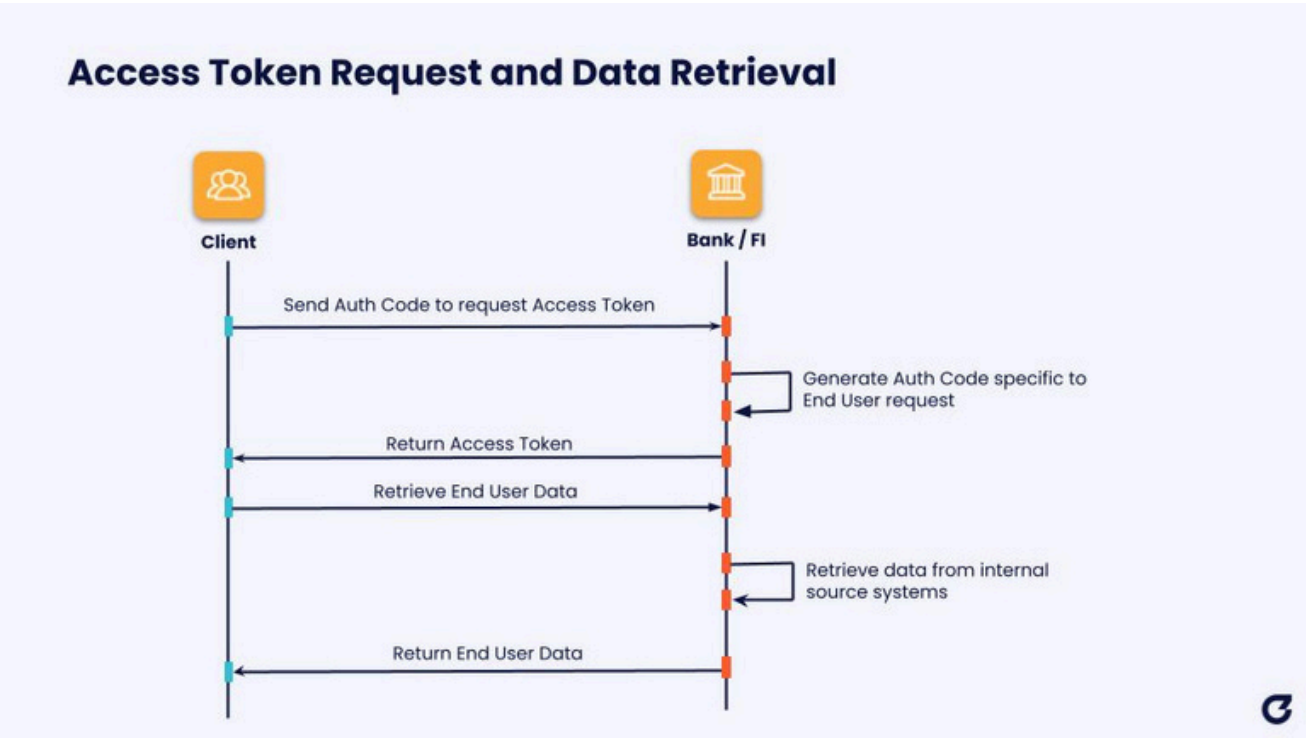
- Data Recipient Client Type: FAPI 1.0 Advanced only supports confidential clients and explicitly rejects the use of shared client secrets.
- PAR Request URI: The request URI uniquely identifies the scopes of data access to be approved by the user.
- Redirection Endpoint: Used by the Data Provider to redirect the user back to the Data Recipient once the authorization has been completed.

Successful Data Recipient Authorization Requests will trigger redirection of the consumer (i.e. user) to the Data Provider's Auth Service in order to perform End User Authentication and confirm Authorization of the consent. End User Authorization requests can only result in a successful initiation of the user interaction if the Client and the associated PAR Request URI can be validated, and if the redirection endpoint specified matches the details registered by the Data Recipient with the Data Provider.

Successful completion of the user interaction will result in the Data Recipient receiving an Authorization Code. At no point does the Data Recipient have access to the internal authentication / authorization flow provided by the Data Provider to the user.



The final stage of the authorization process involves a Data Recipient submitting a request to the Data Provider's Token Endpoint, using the Authorization Code in order to receive an Access Token and optional Refresh Token. The Access Token response received by the Data Provider will identify the scope of access granted by the Data Provider to the Data Recipient, and provide the Access Token lifetime in seconds. The Client can then use this Access Token in subsequent API calls to retrieve End User Data. This data is the actual covered data provided by the standardized API, such as account or transaction details.



05. Addressing Consumer Experience and User Interfaces

Both the proposed Section 1033 ruling and the core principles of open banking necessitate the development of front-end interfaces able to support certain features. For Data Providers, this can be thought of in terms of two types of user – Data Recipients, meaning the third party participants using the consumers' data to enable certain use cases; and End Users, meaning the consumers themselves, using the third party's apps or tools.

Consumers / End Users

When approving data sharing arrangements between Data Providers and Data Recipients, End Users should be able to perform several key functions in order to authorize access to their personal financial data:

- Authentication
- Confirmation of Consent
- Management of Authorized Consents

In open banking standards, including FDX, these functions are often described in the User Experience Guidelines. The remainder of this section will address each in turn.

1. A*uthentication*

FAPI and other open banking API security standards do not typically define explicit technical requirements for authentication of the end user, relying on existing mechanisms implemented by the account-holding bank with high-level requirements like the use of multi-factor authentication (MFA). However, consumer authentication is a formal requirement of the Section 1033 ruling and is an implied necessity under the OAuth 2.0 authorisation framework.

In order to achieve both a consistent user experience and a high level of security, Data Providers are likely to provide the same authentication process and login credentials used for general access to online or mobile banking when authenticating users.

This will normally also mean that MFA is implemented, as it is often part of online banking already, with biometrics used as a strong indicator of customer identity. MFA takes place during Authorization Code flow, when the End User is redirected to the Data Providers Authorization Server to authenticate and authorize access.

2. Confirmation of Consent

Confirmation of consent is not a formal requirement of Section 1033. However, Data Providers are encouraged to confirm with the End User the following information regarding a consent:

- The account(s) to which the Data Recipient is seeking access.
- The categories of covered data the Data Recipient is requesting to access.
- The identity of the Data Recipient issuing the request on their behalf.

From a user experience perspective, the Data Provider needs a mechanism to retrieve a list of the user's accounts and the scope of access requested by the Data Recipient, which the Data Provider will present to the user in their digital channels. In the FDX standard, the scope of data to be shared is uniquely identified by the PAR Request URI provided by the Data Provider to the Data Recipient.

The Data Recipient uses the PAR Request URI as an argument during Authorization Code flow, which enables the Data Provider to verify the consent. Presenting the consent to the consumer to confirm within the digital channel ensures the consumer has a final opportunity to review the details associated with the consent before they authorize data access and are redirected back to the Data Recipient. As above, the consent should include details on the identity of the Data Recipient, the specific accounts being covered, and the respective data being shared.

3. Consent Dashboard

Another common user experience (UX) function within open banking is the ability to manage authorized consents often referred to as a 'consent dashboard'. Section 1033 encourages Data Providers to provide consent management capabilities, including a consent dashboard, provided that this does not in any way discourage the user from maintaining authorized access to data and utilizing Data Recipient services.

Section 1033 also references 'adherence to industry standards' in respect to consent dashboards as a way to provide evidence that consent revocation mechanisms provided do not present a hindrance to Data Recipients
FDX provides detailed UX guidance giving a general overview of how Data Providers (and Data Recipients) should present consent-related information to users in their digital channels, which includes consent dashboard functionality. FDX also provides guidance on permissions language linking specific OAuth 2.0 authorization scopes to more user-friendly descriptions of what these data scopes mean to the end user.

Under the FDX UX guidelines, which match industry conventions, a consent dashboard should able to provide the following core capabilities:

- View a summary of all consents.
- View consent details for a single consent.
- Revoke a consent.

The consent details presented to the user should at a minimum specify information such as the Data Recipient details, the accounts authorized for data sharing, the scopes of data being shared and the sharing duration. Other capabilities like bulk consent management are capabilities that can enhance the customer experience, and Data Providers may consider adding them in order to improve usability.

Developer Portal

Data Providers are obliged under Section 1033 to provide developer documentation. This documentation acts as a specialized channel for providing developers at a Data Recipient with all the information they require to integrate with a Data Provider's APIs.

A Data Provider's developer portal should meet several requirements, including but not necessarily limited to the following:

- Provide an easy-to-use experience for developers.
- Align with other developer documentation published by the Data Provider.
- Accurately describe the integration requirements of using their APIs.
- Remain consistent with the Data Provider's APIs as new versions are published.
- Providing information on how to access technical support.

Many FI's already provide non-regulated third party integration capabilities. The accepted industry principles and capabilities of good developer documentation are applicable here, namely well described APIs, helpful developer tools, detailed documentation, and any other means to provide a good-quality developer experience (DX).

06. Securely Accessing Consumer Data as a Third Party

Once consent has been established and the third party Data Recipient has a valid Access Token, access to Section 1033 covered data is secured by a variety of common API and network security mechanisms including:

- MTLS
- Granular consent
- Use of digital signatures / signing certificates
- Masking and/or Tokenization

Securing Access to Section 1033 Consumer Data

MTLS provides transport layer security, implemented using certificates trusted by both the Data Recipient and Data Provider. This will provide a secure communication channel, in a similar way to other FAPI endpoints, and even in instances where FAPI is not being used.

Once a valid connection is established, a Data Recipient will rely on an Access Token with the corresponding authorization scopes in order to access a Data Provider's resource endpoints. Access tokens can be generated only via the OAuth 2.0 consent authorization flow, and the Data Provider will be able to verify the authorisation scopes through introspection against the stored consents for the registered user, using the Access token to correlate the corresponding Consent ID.

All requests for data access will additionally be secured using digital signatures**.** Participants can implement payload signing, based on the provisions of the standards, using agreed upon signing keys shared for verification using mechanisms such as JSON Web Key Sets (JWKS).

Additional measures that can be implemented include masking of sensitive data. Sensitive data typically includes Personally Identifiable Information (PII), such as bank account or credit card numbers. PII can be provided in masked or tokenized format, to ensure that it is not unnecessarily shared by the Data Provider to the Data Recipient. Masking or tokenization is implemented where there is not a genuine use case for sharing the sensitive data, therefore adhering to the principle of data minimization.

The Section 1033 ruling enshrines regulated access for Data Recipients to certain categories of consumer data, as defined by the CFPB. The high-level categories described by the CFPB can be qualified into one of the following:

- Personal Data
- Account Data
- Product Data

Data Providers **must** make covered data available in a standardized format, which should either be based on a widely accepted standard for data sharing, or a designated industry standard from a designated standard setting body, such as FDX.

The remainder of this section goes through each of these three data categories in turn, describing the API operations which need to be supported as per the FDX API specification. Note that the operations described below are not exhaustive of what is covered by FDX, but rather indicative of what a data request via FDX would look like.

Personal Data

Assuming a Data Recipient can be identified by the Data Provider, and has the consumer's explicit consent, they are able to access the consumer's data using an Access Token. FDX provides a Customer API, allowing Data Recipients to obtain either granular or high-level information on the customers associated with a consumer financial account:

- GET /customers
- GET /customers/{customerId}

These endpoints return standardized response schemas containing personal data attributes such as Name, Address, Date Of Birth, Government IDs and Contact Details. This allows Data Recipients and Data Access Platforms (also known as Data Aggregators) to facilitate various forms of Identity Verification use cases whereby many Data Providers implement the same, standardized high-quality data outputs via open banking APIs.

Account Data

Probably the most critical component of data access for authorized Data Recipients is the ability to retrieve consumer account data from the Data Provider, such as detailed information on the balances and transactions from the payment accounts owned by the user. This is facilitated within the FDX standards by APIs such as:

- GET /Accounts
- GET /Accounts/{AccountId}
- GET /Accounts/{AccountId}/Transactions

Many open banking use cases rely on the ability for Data Recipients to get an aggregated view of the consumer's financial life using information from one or more Data Providers for a single consumer. Use cases include verifying affordability in the context of lending, or providing automated financial management tools and tailored financial advice.

FDX provides detailed API response schemas linked to the specific type of consumer financial account – for example, Deposit, Line of Credit, Investment and Business Accounts.
As regards Payments data, Section 1033 requires that all the information 'necessary to

complete a payment' be made available; however, a payment initiation API similar to that in other regions is not in scope. For its part, the FDX specification does include some limited Payments capabilities, but these are not likely to be required for certification.

Product Data

Covered data under the Section 1033 ruling extends to details on the product information associated with the account type, such as reward programs, terms and conditions, fees and overdraft arrangements.

When this information is coupled with the consumer's account data, this facilitates further potential use cases for Data Recipients and Data Access Platforms, such as product marketplaces and account switching services.

Note that, as of this writing, the FDX specification includes fields for Annual Percentage Rate (APR) and Annual Percentage Yield (APY) as part of the Accounts API, but does not include an API specification for generalized product information or terms and conditions. However, these may be added in the future based on member demands.

07. Operational Impacts and future considerations

Regardless of which standard is used for compliance with Section 1033, FDX or otherwise, one aspect of meeting operational requirements will be implementing version controls to support ongoing upgrades. By example, FDX is now on its fourth 'major' version (6.X) since absorbing the Durable Data API (DDA) initiative in late 2018. Keeping up with new specification versions and adopting best-practices for versioning will be a major consideration for participants when considering how to implement open banking APIs.

Alongside versioning, there are also specific, non-functional technical requirements for participants to consider when designing API interfaces facilitating consumer data sharing. The Section 1033 ruling requires interface performance to be 'commercially reasonable' and includes a minimum availability requirement of 99.5%. In a commercial sense, this is likely to mean that third party API interfaces must be at least as performant as the mobile or web channels banks provide to consumers when performing the same activities directly. This approach sets an important baseline for fostering fair competition.

In practice, from an API management perspective, this means open finance APIs should be subject to various types of performance testing in advance of their release to ensure commercial viability for authorized Data Recipients. Data Providers must also share availability data with the CFPB, so they should consider an API management solution that provides management information reporting as a core capability. Under Section 1033, Data Providers must also retain records related to API responses for at least 3 years, so a robust audit capability must be considered a core requirement of managing their APIs.

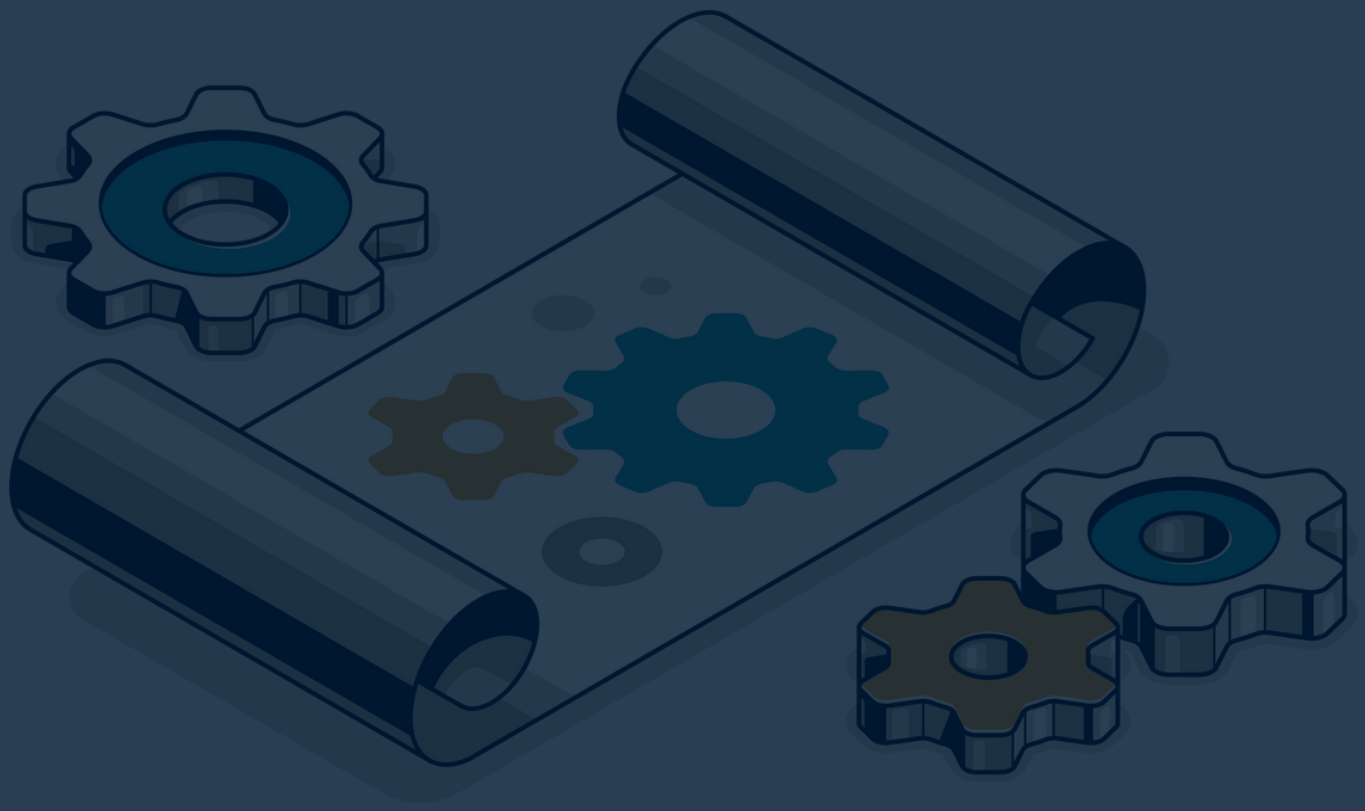
The Section 1033 ruling only covers third party access to certain categories of consumer data. However, the wider open finance model and associated API security profile brings to the fore a variety of commercial API opportunities and future use cases for both Data Recipients and Data Providers. The FDX API already supports access to alternative data sets, such as Tax and Payroll information, and payment initiation has already been identified by the CFPB as a future enhancement to the regulatory framework.

When considering the larger implications of open banking, US financial institutions and their respective technology teams are best served to think of compliance with Section 1033 as just the beginning. As it has in other jurisdictions, American open banking is likely to evolve and grow over the coming years, presenting countless new opportunities. Banks, financial institutions and other holders of personal financial data are strongly encouraged to look beyond compliance as they consider their broader open banking strategies.

08. Working with Ozone API

Ozone API provides a turnkey open finance platform which supports all the open banking standards and regulatory frameworks in the world. We already support the core standards underpinning open banking in the US, including the FDX data specifications, as well as the latest version of FAPI 1.0 Advanced and other security standards included in the FDX security specification. Open banking / finance standards will continue to evolve in the US far beyond the initial CFPB Section 1033 ruling and the current version of FDX, so working with a partner who understands how to build, maintain, and leverage open finance standards for commercial benefit is critical.

Working with Ozone API gives Data Providers of all stripes a strategic advantage, both when it comes to generating revenue from open banking APIs and managing the costs associated with delivery, all based on a solution that is proven at scale with banks globally and designed to ensure fast and simple integration with your existing technology. Through our award-winning Ozone API platform, we provide a suite of components tailor-made to support businesses aiming to achieve open banking regulatory compliance, while positioning them to go well beyond. With Ozone API, you can truly unlock the power of open finance.



ozone API

Technical Guide to CFPB Section 1033

Get in touch: www.ozoneapi.com