CFPB Questions extracted from document https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf	page	
The CFPB requests comment on the procedures it should use to recognize Standard-setting bodies. For example, the CFPB requests comment on whether it should recognize a given body before, after, or at about the same time as the body seeks to issue a qualified industry Standard or whether the recognition procedures should be flexible enough to accommodate all of those possibilities.	50	In the opinion of the OIDF the procedures for recognition of qualified standards setting bodies should be flexible enough that they are able to deal with organisations that are curating standards in various stages of their lifecycle. It would seem appropriate to recognise standards setting bodies that already have relevant industry standards or are recognised in their domain as leading development of standards that, although perhaps not complete, are sufficiently mature for implementation and that there is a desire/need among a number of in scope organisations to adopt as part of their solution to meet the CFPB rules. The verification that a standards setting body does meet the requirements defined in 1033.141 should be kept fairly lightweight, with perhaps a self-asserted questionnaire that is subsequently signed and published with a supporting appeals/objections process available to interested parties.
The CFPB requests comment on how to provide guidance and, in particular, on how to ensure that the substance is consistent with the provisions of this proposed rule, as finalized.	50	A pre-defined checklist with opportunity for providing supporting evidence would seem appropriate. Ensuring that the substance is consistent would be well served by requiring that self-asserted qualified standards bodies are required to make such assertions a matter of public record and that there is a corresponding appeals/objections process.
The CFPB requests comment on whether the proposed basic account verification information category would accommodate or unduly interfere with beneficial consumer use cases today. Given privacy and security concerns about unintentionally covering other kinds of information that are not typically shared today,	64	Inclusion of account information would seem to be useful in some cases but could also lead to inappropriate uses of the Open Banking rules. This extension to the scope starts to overlap with pure-play digital identity services potentially affecting that market but also risking a form of implied identity assurance becoming used in the wider market, it may also lead to inappropriate data sharing. In other markets digital identity attributes have not been included in the Open Banking scope and it has not obviously impeded adoption while allowing for more focussed rule making to be possible around provision of digital identity attributes, and mitigating risk of conflict or overlap with digital identity sharing rules and regulations. The OIDF would suggest further wording that clarifies the intent of the CFPB rule-making in relation to the proposed basic account verification information category and to make more explicit the use cases that are in and out of scope of the rulemaking.
, the CFPB also requests comment on whether it is appropriate to limit this category to only a few specific pieces of information.	64	It is possible to not have any requirement to provide any account verification information under the scope of Open Banking rule making and other jurisdictions have that situation. This allows for other rules and regulations to cover this digital identity information and for providers to make their own decisions about what they wish to provide in this regard.
The CFPB requests comment on whether a definition is needed and whether format should be defined to mean the specifications for data fields, status codes, communication protocols, or other elements to ensure third party systems can communicate with the developer interface.	77	The OpenID Foundation strongly encourages the CFPB to not conflate "data formats" with "communication protocols". We believe the CFPB and US consumers would be better served by having both as equally important but separate components and that both "data formats" and "communication protocols" should be implemented using Qualified Industry Standards. "Status codes" may exist in both depending whether the status code relates to an aspect of "communication protocol" or an element of the data.
The CFPB requests comment specifically on what role qualified industry Standards should have, if any, regarding the quantitative minimum performance specification set forth in the final rule.	79	Depending on the scope of "minimum performance specification" this question may have various ranges of answer. If "minimum performance specification" relates only to the amount of time it takes for any provider to respond to a request then the role of the qualified industry standard is fairly clear however it may be that there are "performance" requirements relating to an number of other metrics including but not limited to: - the percentage of requests that succeed -vs- fail - the percentage of requests that correctly implement required security controls -vs- do not - the percentage of requests that correctly conform to any qualified industry standards for data format or communication protocol

...the third party ‘passes’ the consumer directly to the data provider, who authenticates the consumer using the consumer’s digital banking credentials, and then provides the third party with a secure access token.The CFPB seeks comment on whether and, if so, how the proposed rule should address this practice.	87	The OpenID Foundation is a strong proponent of this approach and that is essentially the solution that the FAPI security profiles describe and are implemented in other countries' existing Open Banking solutions including UK, Brazil, Saudi Arabia and Australia. The underlying reason for the adoption of the FAPI security profile in other countries is that it is the best known implementation of that apprach and it has been tested both in an academic cyber-security context and through real world implementation by banks and third parties in multiple countries with all the attendant review and testing procedures. It also provides sufficient detail that correct implementations based on a specific variant will be interoperable with each other. Regarding whether and how the proposed rule should address this practice, the OIDF would suggest that the requirements are made clear... 1. That there is a Qualified Industry Standard used when implementing the "communication protocol" used between the Data Providers and the Third Parties 2. That the third party should not need (and never have) access to any credential issued to the consumer by the data provider (as that needs to kept as a secret between the consumer and the data provider) in order to use the standard "communication protocol" 3. That the qualified industry standard should be designed and implemented in a way that mitigates clearly defined risks and threats (e.g. https://openid.net/specs/fapi-2_0-attacker-model-ID2.html) 4. There should be tools to test that the communications protocol defined in the qualified industry standard has been correctly implemented.
the CFPB declines to propose a general policies-and-procedures requirement for data security but seeks comment on such a requirement.	89	Some available communication protocol standards (such as the FAPI security profiles of OpenID Connect) have a significant proportion of their content focussed delivering strong data security controls for the interactions involved in the Communication Protocol. So while the OIDF understands that a general set of requirements for data security could be counterproductive it would be important that there are security countermeasures contained within Qualified Industry Standards that are deployed. The suggested requirement for a qualified industry standard for communication protocol is particularly relevant to this topic and should have a generalised requirement to mitigate security risks and be explicit about the security risks that are mitigated.
The CFPB requests comment on additional ways to harmonize the risk management obligations of data providers with CFPA section 1033’s data access right for consumers and authorized third parties. Risk management may entail a variety of practices and risk management Standards could be defined through several sources, including prudential guidance, other Federal government Standards, or qualified industry Standards.	94	Risk management is a wide topic and clearly requires many components to understand and appropriately mitigate risks. One component of risk management that the CFPB should include relates to the various security risks associated with the sharing of information and granting of access to services by data providers. The "communication protocol" aspect of an Open Banking ecosystem is a key point of control from a security perspective and the OIDF provides an open standard that has been proven to work in other Open Banking ecosystems. The FAPI security profile includes not just robust security controls, but also clear documentation of the specific technical risks that are mitigated, academic analysis of the protocol, that demonstrates those risks are mitigated by the FAPI specifications, and tools to allow implementers to test their implementations for conformance to the specification. As a set these capabilities provide a significant mitigation of risks in that part of the overall Open Banking landscape. Additionally the FAPI security profiles of OpenID Connect allow for a controlled set of interactions, permitting data providers to be confident that the consumer is interactively involved and informed about what is going on, allows for the secure delivery of access tokens to the third party and if necessary enables the data provider to request consent from the consumer that they wish to share data or access to servicves with a specific third party.

The CFPB requests comment on whether developing such a credential could reduce diligence costs for both data providers and third parties and increase compliance certainty for data providers with respect to the proposed rule.	98	The OpenID Foundation has had direct experience of contributing to such credentials and has advocated for them in other jurisdictions, we have also seen cases where an environment has started out without any such credential and moved to establish them. The underlying reason for having a credential is multi-faceted but mainly relates to two things. 1. Interoperability 2. Security If interoperability is delivered between Third Parties and multiple Data Providers it enables Third Parties to re-use integration code, reducing their costs. If a Qualified Industry Standard for the "communication protocol" is required then the liklihood of Data Providers having access to off-the-shelf software is greater enabling them to have greater choice of implementation approach and potentially a faster time to deliver a secure interoperable solution. Security can also be enhanced through the use of a well adopted and mature Qualified Industry Standard for the "communication protocol" as the risk of design mistakes is reduced due to the very wide review and implementation experience that standard will have already been through. Correct implementation of the required standards significantly increases the liklihood of both of those outcomes and a credential backed by standardised empirical testing can significantly increase the liklihood of a coprrect implementation being delivered. This incidentally reduces the cost for both Data Providers and Third Parties as they do not need to implement nearly as much of their own testing tools to ensure their implementation is as designed.
The CFPB also requests comment on the steps necessary to develop such a credential and how the CFPB or other regulators could support such efforts.	98	There are a numer of approaches to this across the previous implementations of Open Banking. Based on that experience it is common for there to be several credentials that entities need to achieve before they can participate. The three domains of Business, Legal and Technical would seem a good starting point and for each of these domains a number of rules may be needed (the focus of this consultation). These rules should have some level of associated Conformance and Certification process associated with them, these processes will be delivered with a combination of people, process and technology. The OpenID Foundation focusses on specific technical standards and provides open source conformance tools and a corresponding service that delivers self-service conformance testing and the ability to publically self-certify conformance. This is used in several jurisdictions as one component of the wider set of credentials needed by data providers and third parties to participate. The OIDF conformance and certification service can be delivered directly to individual ecosystem members or delivered via an OpenID Foundation certified partner at an ecosystem level.
The CFPB seeks comment on how the proposed rule could further facilitate compliance and reduce due diligence costs for both data providers and third parties while adequately ensuring the security of consumer data.	102	One aspect of security of consumer data is the security of that data in transit between the data provider and the third party. The OpenID Foundation provides the FAPI specification specifically to enable that sort of secure data sharing between parties on behalf of consumers. The very existance of a mature and well tested "communication protocol" of this nature will reduce costs for implementers as the work to invent this has een done and has been "battle tested". Additionally, the maturity of the FAPI specs means that off-the-shelf software and services are available that can deliver a significant proportion on an implementation for either a data provider or third party. There is also readily available conformance tooling that implementers can use to check that their implementation is functioning as per the specifications and this includes verification that quite a number of known bad cases are correctly handled, several of these these "known bad" cases have been developed in response to previous implementation errors in other jurisdictions. Having a ready made conformance tool and service further reduces the due diligence costs as there is a significantly reduced need to develop test scenarios or or test tooling for these scenarios. Conformance tooling provided by the OIDF covers both ends of the "communication protocol" i.e. data provider and third party

The CFPB requests comment on whether clarifications are needed regarding what information would be sufficient to confirm the third party has followed the authorization procedures in the context of automated requests received through a developer interface.	107	The OpenID Foundation provides the FAPI specifications in part to enable the authorization to be handled in such a way that the Data Provider can be very confident that the request is originating from a third party that is appropriately authorized and that the exchange of messages in that process have not been subverted by another unauthorized entity. The FAPI specs on top of OpenID Connect provide a "Communications Protocol" that allows the third party to pass Consumer interaction to the Data Provider for appropriate authentication and authorization and get a secure access token back that can only be used by that third party to access that consumer's data and services when accessing the developer interface.
The CFPB seeks comment on whether the final rule should instead permit data providers to confirm this information with the consumer only where reasonably necessary. Under this alternative approach, if technology were to evolve such that data providers could reasonably confirm this information without asking the consumer to confirm it, the rule might no longer permit data providers to ask consumers to confirm this information.	108	Open Banking data providers need to be able to perform some sort of confirmation for two reasons: 1. demonstrate that they have granular control over access to consumer data 2. provide granularity to the consumer that is not possible without the insight the data provider alone has (e.g. account selection). It may be possible to implement some sort of externalised consent service but the consequence of this is that an additional party would be needed that has access to data provider information before consumer authorization can be completed. It is more common for the implementation to allow some long lived authorization such that the third party is permitted to use a Secure Access Token over an extended period without recourse to a confirmation process every time. Open Banking implementations that use the OpenID Foundation specifications usually use the long lived authorization option but there is nothing preventing the other options working with OpenID Foundation specs.
The CFPB seeks comment on whether it should indicate that conformance to a specific Standard or a qualified industry Standard would be relevant indicia for a data provider’s compliance with the machine-readability requirement in proposed § 1033.341(a)(2).	115	The OpenID Foundation would encourage the use of conformance testing across the various standards domains required by the draft rules and for the additional "communication protocol" standard domain discussed elsewhere in this document. There are myriad ways that machine readability can be achieved but it is in the interests of third parties that the number of different standards adopted by Data Providers are kept to a fairly low number as this reduces the integration work needed and thus the cost. It is also important that implementation of standards are done correctly to keep the integration code as consistent as possile across providers.
Additionally, the CFPB seeks comment on whether it should issue rules or guidance that would make it easier for third parties and other members of the public to identify a particular data provider’s information.	115	Making generally available the necessary parameters to allow a third party to connect to a developer interface would be appropriate. It would seem contradictory to have the situation where initial connection required a human interface for technical connection parameters before then having the developer interface used by applications. Note it may be appropriate to have a human workflow to authorize third party access to the ecosystem as a whole and that is implemented in other jurisdictions.

The CFPB requests comment on whether the authorization procedures in proposed § 1033.401 would be sufficient to ensure that a third party is acting on behalf of a consumer in obtaining access to covered data or whether the CFPB should consider alternative procedures.	131	The OIDF would suggest that authorization is presented to the Consumer by the Data Provider and not the third party for several reasons. 1. The Data Provider is in a position to offer the detail of what has been requested and clarify any details that the third party does not have visability of at that point in the exchange. 2. The Data Provider can have certainty that the Consumer has indeed been presented with correct information about the data and services that were requested. 3. The Consumer has direct control through their intreraction with the Data Provider and can provide their informed consent. 4. The security of data and services provided can be maintained while allowing third parties to access resources that they have been explicitly granted access to by the Consumer linked to those accounts. The FAPI specs on top of OpenID Connect provide a "communications protocol" that allows the third party to pass the Consumer interaction to the Data Provider requesting access to Consumer data or services and allows for appropriate authentication and authorization to be performed. The Third Party gets a secure access token back that can only be used by that third party to access that consumer's data and services when accessing the developer interface.
The CFPB also requests comment on whether the authorization disclosure, including the statement that the third party will comply with certain third party obligations, is sufficient to ensure that the consumer would be able provide express informed consent for the third party to access covered data on behalf of the consumer.	132	It would seem challenging to rely solely on the proposed authorization disclosure for various reasons. 1. The Third Party my not have enough information available to them before actually requesting data to present a precise authorization description to the Consumer 2. There is a risk that the Third Party mis-identifies the Consumer and presents an authorization disclosure for the wrong Data Provider customer, ultimately getting access to and presenting information from one consumer to another 3. Without prior knowledge of details of the Consumer's accounts third parties will have a choice of presenting overly broadly scoped authorization requests to consumers or having a multi-stage journey to establish an accurate picture of the authorization they need resulting in a poor user experience 4. The Data Provider will have no way of knowing whether the authorization disclosure is what was presented to the Consumer and will have no way of knowing if an incorrect Authorization Disclosure is incorrect due to an error or malicious action so it will e very difficult for their security, fraud and risk responsibilities to be fulfilled in relation to the Developer interface
The CFPB seeks comment on any obstacles to including the proposed authorization disclosure content and on whether additional content is needed to ensure consumers have enough information to provide informed consent. Specifically, the CFPB seeks comment on whether the rule should include any additional requirements to ensure: (1) the consumer can identify the third party and data aggregator, such as by requiring inclusion of legal names, trade names, or both; (2) the description of the consumer's requested product or service is narrowly tailored and specific such that it accurately describes the particular product or service that the consumer has requested; (3) the consumer can locate the third party obligations, such as by requiring a link to the text of proposed § 1033.421; and (4) the consumer can readily understand what types of data will be accessed, such as by requiring third parties to refer to the covered data they will access using the categories in proposed § 1033.211.	136	With regard to the second point in this question, it is likely that this narrowly tailored and specific requirement will a significant challenge to achieve before the third party requests data from the data provider. The Third party will not have visability of which accounts and services the specific customer has with a given Data Provider before requesting information from the Data Provider. There is also a risk that the Third Party mis-identifies the Consumer and presents information about the wrong consumer (whether due to accident or some malicious actor), risking access to and presentation of information about one consumer to another. Both of these points would seem to be a significant obstacle to the origination of authentication information from the third party. We would also suggest that there is a missing element in this question which would be the "purpose" of the authorization. It may be very informative to the consumer at some point in the future if a given authorization has a "purpose" element attached to it as a reminder of why this data access was authorized. This will be particularly relevant to long lived authorizations but potentially when looking back at the history of authorizations.

The CFPB seeks comment on whether there are technology-based solutions that could apply the appropriate proposed third party requirements automatically. For example, the CFPB seeks comment on whether such solutions are available that could assist third parties with automatically terminating access after the third party's authorization has ended or with limiting the use of covered data consistent with the limitation described in proposed. If such solutions are available, the CFPB requests comment on whether to require third parties to integrate these capabilities.	140	Implementations based on FAPI and OpenID Connect standards already enables features such as this. With other Open Banking implementations that use FAPI & OpenID Connect the narrow tailoring of access given to the Secure Access Token includes an expiry time. It is also possible using a technology component called "Grant Management" for the third party to communicate to the Data Provider that the access authorised by the Consumer should be revoked earlier than the expiry time of the Secure Access Token or the long lived authorization data maintained by the Data Provider.