



Financial Data Exchange Comments
Docket No. CFPB-2020-0034 - *Consumer Access to Financial Records*
Consumer Financial Protection Bureau (CFPB)

The Financial Data Exchange, LLC (FDX) is pleased to provide comments to the Consumer Financial Protection Bureau (CFPB) Advanced Notice of Proposed Rulemaking (ANPR) requesting information related to consumer access to financial records and the development of regulations to implement Section 1033 of the Dodd-Frank Act.

These comments are intended to address many of the questions posed in the CFPB's ANPR from the insight and perspective FDX has gained as an industry standards body with diverse membership¹ from every corner of the user-permissioned financial data ecosystem. FDX's comments are also intended to inform the CFPB about the progress, maturity, and overall benefits of neutral market-led technical standards to enable end-users² to access, share, and use their own financial data. Specifically, FDX seeks to highlight the success of market-led standards to date and the breadth of participation among all market entities in this work. FDX also strives to convey a detailed view of FDX's mission, structure, and vision as an example of how even competing entities across the spectrum of financial services can join together to implement common, interoperable, and royalty-free technical standards that maintain innovation in the marketplace while elevating user control and experience. Finally, FDX wishes to submit that a market-led approach is best suited to develop, implement, promote, and certify technical standards for user-permissioned data sharing in the United States.

About FDX

FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to unifying the financial industry around a common, interoperable, royalty-free standard for the secure and convenient access of permissioned consumer and business financial data, aptly named the FDX Application Programming Interface (FDX API). FDX is currently comprised of 167 financial data providers (i.e., "Data Holder"³ or financial institutions)⁴, data recipients (i.e., "Data User"⁵ or third-party financial

¹ [FDX Members](#)

² From *FDX Taxonomy of Permissioned Data Sharing v. 1.0*: End Users: include consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data. Consumers: are end users acting in their personal capacity. Full Taxonomy in Appendix.

³ Reference to definition of "[Data Holder](#)" from CFPB Consumer Access to Financial Records ANPR.

⁴ From *FDX Taxonomy of Permissioned Data Sharing v. 1.0*: Data Providers: the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages. Full Taxonomy in Appendix.

⁵ Reference to definition of "[Data User](#)" from CFPB Consumer Access to Financial Records ANPR.

technology companies or fintechs)⁶, data access platforms (i.e., data aggregators⁷ and ecosystem utilities)⁸, consumer groups, financial industry groups and other permissioned parties in the user-permissioned financial data ecosystem. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

FDX exists chiefly to promote, enhance, and seek broad adoption of the FDX API technical standard (formerly the Durable Data API – DDA), which allows for users within the financial data ecosystem to be securely authenticated without the sharing or storing of their login credentials with third parties. Through broad adoption of the FDX API, screen scraping (the retrieval of financial account information with a user’s provided login credentials) will eventually come to an end, and the flow of user-permissioned data between banks, aggregators, fintech applications, payments, and online lending, for example, will be more secure and reliable. This standard has been under the stewardship of the FS-ISAC and many of the largest financial services organizations in the US have begun implementing this standard in the last several years⁹.

Scope of FDX Comments

FDX is barred by its charter from taking positions on legislative and regulatory policy issues. Consequently, FDX is not able to provide comment on questions or parts of questions in the ANPR that relate to specific regulatory decisions or actions. However, FDX does engage in “educational advocacy” to ensure that regulators, legislators, and policymakers are educated and fully aware of the work FDX is doing, the way this work interacts with certain policies and regulations, and the way innovations across the financial services ecosystem are giving consumers and businesses the ability to securely use and share their financial data. As a market-led standards body, FDX also advocates for technical specifications and standards designed and implemented by the financial services industry for user-permissioned data sharing as opposed to regulatory or government mandated technical standards.

Overall, and considering the potential shift of the regulatory landscape around user-permissioned data sharing, FDX believes it is important to provide the CFPB with its views on the wide range of issues covered in the ANPR, and for the CFPB to have a clear view of how FDX works and the progress it has made to develop and drive adoption of neutral market-led technical standards for consumer data sharing. FDX also believes that industry-led efforts to develop and promote technical standards for

⁶ From *FDX Taxonomy of Permissioned Data Sharing v. 1.0: Data Recipients*: service companies, applications (financial apps), financial institutions, products, and services where End Users (on their own or through their End User Delegates) manage or act on their finances, whether actively managing their finances (such as moving money or applying for credit) or passively doing so (such as garnering recommendations or insights). Full Taxonomy in Appendix.

⁷ Reference to definition of “Data Aggregator” from CFPB Consumer Access to Financial Records ANPR.

⁸ From *FDX Taxonomy of Permissioned Data Sharing v. 1.0: Data Access Platforms*: intermediaries that facilitate financial data access, transit, storage and/or permissioning on behalf of Data Recipients or End Users, also commonly referred to as “Data Aggregators”. In some cases, Data Access Platforms do not have a direct relationship with the End User. The data may be passed through without modification or may be normalized in line with permitted objectives (e.g., parsed for readability or used to confirm other data). Data Access Platforms should not be misidentified with parties who do not obtain End Users’ consent but gather data, sometimes referred to as Data Brokers or Data Harvesters. Full Taxonomy in Appendix.

⁹ Examples of some publicly announced data sharing agreements mentioning FDX API listed as Appendix B.

financial services are as important as ever because they are able to keep pace with rapid marketplace innovations in a way that regulatory or government mandated approaches often cannot.

Historical Snapshot of Standardization of User-Permissioned Data Sharing

Over the last two decades, significant innovation in financial services has been driven by end user demand for online financial management services, payments, credit decisioning and more that requires access to and sharing of financial data. While these new financial technology tools are often provided by companies that are not affiliated with an end user's primary financial institution, financial institutions themselves also offer financial technology products and services to their customers.

To utilize these third-party services, users need the ability to be authenticated so they can authorize access to their financial data from their financial institutions to other financial data parties in a convenient, secure, and reliable manner.

In order to give these parties access to their financial records, end users have historically provided their login credentials to financial applications or data access platforms (known as credential-based access). In most cases, financial apps do not store a user's login credentials, but instead pass these credentials via an Application Programming Interface (API) to the data access platform. The financial application or data access platform can then access the financial institution website and retrieve the users' data (this process is known as screen scraping).

While credential-based access and screen scraping have provided a pathway for consumers to use and share their own financial data to date, this legacy technology is inefficient and places stress on financial institutions due to the number of automated logins. Finally, and most importantly, this method of consumer authentication and data access requires the sharing of sensitive consumer login credentials and provides limited consumer control over the amount of data consumers share with third parties.

Fortunately, market adoption of a more efficient and secure method of data sharing began a few years ago and should eventually replace shared login credentials and screen scraping in most scenarios. Specifically, tokenized access, in concert with API-based data collection, allows a user to be securely authenticated by their own financial institution and authorize the data provider to supply only the data they want to share. In fact, APIs make user-permissioned data sharing easier, more accurate and more secure. Not only do they remove credential sharing and provide dedicated data access, but APIs provide the ability for data providers to give consumers control over the type of data that is shared, with whom, for how long and for what purpose.

While the advent of APIs for financial data sharing has begun to change the user-permissioned data landscape, there was still a missing element – standardization. In fact, without standard APIs and additional standardization of authentication, authorization, certification, user experience and consent guidelines, financial institutions, financial data access providers and fintech applications and services will remain fragmented – using incompatible APIs, processes and even definitions of how a user is able to permission use of their own financial data.

Accordingly, FDX was born out of a desire among all entities in the user-permissioned financial data ecosystem to have standardized APIs available for all user-permissioned financial data.

FDX Comments

Rather than seeking to answer each individual question in the ANPR, which would likely involve duplicative and overlapping content, most of FDX's comments will be organized thematically with reference to questions in the ANPR where we believe the theme or content provides an appropriate response. In addition to specific comment themes and specific answers, FDX's comments are guided by the following core tenets:

- FDX submits that a non-profit and market-led technical standards body is best positioned to unify the financial industry around common, interoperable, royalty-free technical standards for user-permissioned data sharing.
- FDX technical standards can be tailored to accommodate regulatory requirements. FDX is, by charter, neutral on the “what” of regulatory policy in this area and rather seeks to implement technical standards to accomplish the “how” of user-permissioned data sharing in a way that is responsive to market needs as well as any legal or regulatory compliance requirements.
- FDX will not differentiate views between authorized or direct data access. The broad ecosystem of entities that power user-permissioned data sharing, and that make up FDX's membership, use both direct and authorized methods of data access to allow consumers to authorize the sharing and third-party use of their financial data. In addition, both approaches are reflected in FDX's standards and market deliverables, and since the shared data is the same in both methods of access, FDX believes the difference lies in the implementation of transparency, traceability, control, and security standards, rather than distinctions that exist due to the method of data access.
- Due to rapid innovation in the marketplace, industry roles within the user-permissioned data sharing ecosystem continue to evolve and often overlap. Entities generally occupy roles as user-permissioned data providers, data access platforms and data recipients as directed by the consumer or business. That said, some of these entities can occupy multiple roles at the same time. These ever-changing dynamics highlight the need for neutral market-led standards that are able to adapt to market innovations for the benefit of the end-user rather than attempting to tie specific entities to specific roles in a way that could chill market innovation and evolution or possibly compromise the End User's experience or service options.
- FDX uses the term “End User” to encompass consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data¹⁰. FDX recognizes that End Users may also delegate persons or entities, such as End Users' CPAs, brokers, fiduciaries, and other advisors to act on the End Users' behalf to

¹⁰ From FDX *Taxonomy of Permissioned Data Sharing v. 1.0*: End Users: include consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data. Consumers: are end users acting in their personal capacity. End User Delegates: refers to delegated persons or entities, such as End Users' CPAs, brokers, fiduciaries, and other advisors, who have been authorized by the End User to grant permission to share and receive the End Users' Financial Account Information on the End Users' behalf. Full Taxonomy in Appendix.

access and share financial data. FDX's Taxonomy of Permissioned Data Sharing¹¹ (included in the Appendix) defines these delegates simply as those who have been authorized by the End User to grant permission to share and receive the End Users' Financial Account Information on the End Users' behalf.

Consumer Centrality & Benefit - 5 Principles of User-Permissioned Data Sharing

Corresponding ANPR Questions: 1, 3, 4, 13, 26, 27, 41, 46

FDX believes accessible, user-permissioned financial data sharing inherently gives consumers control of their data. Such an approach empowers End Users to better understand, leverage, and benefit from their own financial data and improve their financial lives. A consumer-centric approach also facilitates access to financial data that can improve financial literacy, financial decisions, and financial convenience.

In order to deliver a system of financial data sharing that provides these consumer benefits, FDX believes five core principles must be present to ensure that all participants in the user-permissioned data sharing ecosystem serve the needs of consumers. These are:

- 1.) **Control** - Consumers should be able to permission their financial data for services or applications.
 - All entities within the user-permissioned financial data ecosystem should provide clear, intuitive navigation and information to consumers, allowing informed decision making on sharing financial data.
 - Consumers should have the ability through easy, intuitive interfaces, to effortlessly grant, modify and revoke access to their financial data for applications or services they desire to use.
- 2.) **Access** – End Users should have access to their data and the ability to determine which entities will have access to their data.
 - Intuitive navigation: The authentication process should avoid unnecessary steps or language that delays, interrupts, or impedes access.
 - Speed of access: Hand-off between parties and systems should be convenient, smooth, secure, and efficient. Time-consuming or confusing experiences represent a barrier and frustrate consumers.
 - Responsible Access: Consumers should provide informed consent (with the ability to revoke that consent) for any and all access granted to entities within the user-permissioned financial data ecosystem. These entities will then only have access for the purposes for which the consent was provided.
- 3.) **Transparency** - Individuals using financial services should know how, when, and for what purpose their data is used. Only data that is required to provide such services should be shared with the organization providing the service.
 - Consumers should be able to view who they have permissioned, as outlined above in "Control."

¹¹ FDX Taxonomy of Permissioned Data Sharing v. 1.0 listed as Appendix A

- When permissioning a new service, consumers should be fully informed regarding what their data is used for, how long the service can access that data, who it is used by, and under which terms the service is provided.
- 4.) **Traceability** - All data transfers should be traceable. Consumers should have a complete view of all entities within the user-permissioned financial data ecosystem that are involved in the data sharing flow.
- Data users (organizations and service providers) should know each step the data takes in order to permit the consumers to follow the path for each data flow. Data flows should be easily traceable and logged as the data traverses (i.e., from the financial data provider through the financial data access platform and to the financial data recipient) in order to aid the pinpointing of potential errors or suspicious connections.
 - Traceability may be used to support operational efficiencies and remediation activities. Additionally, it may also result in the faster detection and response to potential errors and suspicious traffic, as well as helping to pinpoint the source of the issue.
- 5.) **Security** - Financial data parties should follow industry best cybersecurity practices across the whole of their organization for safety and privacy of data during access and transport and when that data is at rest.
- All entities within the user-permissioned financial data ecosystem need to provide clear definitions on data usage and privacy, permitting consumers to make educated decisions.
 - All entities involved in the data-sharing ecosystem must have appropriate security policies and practices in place. These practices should reflect best-in class standards and be improved upon continuously.
 - Security should empower consumer control, access, transparency, and traceability and should not be implemented in a manner that introduces friction points or other features that contravene these principles.



Based on these 5 Core Principles, and specific to a few questions within CFPB's ANPR, FDX also submits the following:

- ❖ The ability for consumers to access, control and share their own financial data, whether via authorized or direct access, is the central pillar upon which FDX is built. Simply put, FDX's goal is to develop, promote and seek broad adoption of neutral market-led technical standards that enable the most secure and transparent consumer data access possible while preserving the ability for the market to continue to innovate and utilize the best technological approaches for data sharing.
- ❖ FDX believes that all five core principles work together to provide consumers with superior permissioned data sharing and align the marketplace with consumer expectations and understanding. Specifically, consumers expect and demand access to their own data to use, share and leverage to their financial benefit. Consumers also expect that they alone have control of how their data is permissioned, shared, used, or accessed, as well as having the ability to revoke such choices. Consumers also expect to be clearly informed about who has access to their data, what purpose it will be used for and for how long. Finally, consumers fully expect that their data will be transferred as needed in a secure manner, and that if there is an issue that results in loss, that they will be made whole.
- ❖ When a system of financial data sharing appropriately provides these five principles, consumer benefits derived from accessing, sharing, and using their own financial data is significant. Whether from better personal financial management, access to wider and better credit services, more efficient processes for account and asset verification, more accurate information, streamlined accounting and bookkeeping, quicker tax preparation or myriad other data access use cases, consumers are benefitting in the form of cost savings, efficiency and enhanced financial awareness.

Innovation & Small Market Participants

Corresponding ANPR Questions: 2, 4, 6, 7, 8, 10, 11, 13, 46

Financial data sharing innovations continue to accelerate with the increase in end users' demand for online financial management services, payments, credit decisioning and other applications that may require access to and sharing of financial data. And FDX believes that innovation in financial services is being enhanced via common, interoperable, royalty-free, and market-led technical standards. Such market-led standardization provides foundational requirements for entities seeking to serve the market for user-permissioned data sharing, whether via direct or authorized data access. A non-profit industry standards body like FDX also brings together a vibrant, and diverse ecosystem of financial services providers whose distinct perspectives lead to more robust understanding of consumer need and demand.

Finally, FDX believes that market-led technical standards based on consumer protection principles, rather than prescriptive regulations, are more likely to benefit consumers by enabling rapid, nimble, and tailored adaptation that responds to the accelerating pace of change in financial technology.

To illustrate this point, consider that FDX membership encompasses the full spectrum of entities and stakeholders involved in user-permissioned data sharing including financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups, industry utilities, service providers, other permissioned parties and even individual academics and experts in the field. In addition to the broad spectrum of FDX's membership, the organization also maintains a diversity in size of organizations: from small community financial institutions and credit unions to some of the world's largest banks, from consumer groups to core technology providers, from start-up fintechs to leading data aggregators.

Of specific interest to both FDX and CFPB, innovation must be considered through the lens of these small entities.

Small financial institutions face challenges in the current consumer data sharing ecosystem due to both financial and technological constraints. Core technology providers often supply products and services so that the customers of these small financial institutions can use the same technology tools and have the same user experiences as larger financial institutions. However, absent a common standard, proprietary technology implementations take time to develop, and small financial institutions simply do not have the resources to build these solutions themselves. In a similar manner, small fintechs can face capital formation challenges and may have difficulty bringing new and innovative solutions to market amid an oft siloed and diverse financial services landscape.

It is in view of these challenges where standards bodies like FDX can make such a huge difference for small entities. In their most elemental form, common interoperable standards provide a framework for common and interoperable API-based data sharing services, tools, and protections that even the smallest financial institutions can offer their customers. Such standards also assist other small market entities by lowering common barriers and by bringing the full spectrum of the financial services ecosystem together in one place and making participation and engagement very affordable. In addition, a common standard, in concert with a working group structure and standardization of data use cases, allows any entity, regardless of size, to bring innovative models forward that can be defined quickly and implemented in the marketplace rapidly so that consumers can use their own financial data in new and innovative ways. And the same rationale applies to developers who can build from a universal standard.

In sum, innovation in user-permissioned financial data sharing continues apace. In addition, common technical standards allow entities of all sizes within the financial data ecosystem to use the same standard and process for a given product or service so that end-user demand for innovative financial services can be met with the same tools.

Structure & Details of US Market-Led Technical Standards Body

Corresponding ANPR Questions: 4, 5, 8, 13, 46

As mentioned in the introduction, FDX is an international, non-profit organization operating in the US and Canada that is dedicated to unifying the entire financial services ecosystem around a common, interoperable, royalty-free standard for the secure and convenient access of user-permissioned financial data that is aptly named the FDX Application Programming Interface (FDX API).

FDX believes the following important organization details about FDX can inform CFPB's deliberations on this ANPR:

- FDX is currently comprised of 167 financial data providers (i.e., financial institutions), data recipients (i.e., third-party financial technology companies or fintechs), data access platforms (i.e., data aggregators and ecosystem utilities), consumer groups, financial industry groups and other permissioned parties in the user-permissioned financial data ecosystem. More than half of FDX members are fintechs and non-banks.
- FDX technical standards can be tailored to accommodate any regulatory or legal requirements in a given jurisdiction. FDX is, by charter, neutral on policy and seeks to implement technical standards to accomplish the “means and methods” of user-permissioned data sharing in a way that is responsive to market needs as well as any legal or regulatory compliance requirements. FDX will ensure its standards meet any principles or requirements that the CFPB may place on user-permissioned data access.
- Since the most recent FDX member survey on adoption and implementation of the FDX API, over 12 million US consumers have been transitioned from screen scraping to a version of the FDX API. FDX estimates that data access and sharing for between 65-85 million US consumers is still provided through shared login credentials and screen scraping.
- FDX's organizational structure includes a balanced board of financial institutions (FIs), financial industry groups and non-financial institutions (Non-FIs)/fintechs as well as an observer-level board seat for consumer advocacy groups.
- Every FDX member organization, regardless of size, type, or dues, has a single and equal vote in Working Groups and Task Forces where most of the FDX work is accomplished. In this, FDX abides by the mantra of “Best idea wins,” irrespective of firm size or type. The FDX board voting structure is also balanced by giving different market segments equivalent voting representation by requiring a super-majority of board members across industry sectors to agree on major decisions.
- The FDX API specification itself is free for any organization to download and use and membership starts with a no-cost tier for non-profit consumer advocacy groups and an affordable and revenue-based structure for all other entities.
- FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

In addition to the FDX board, FDX is comprised of Committees, Working Groups and Taskforces that report to the FDX board and work diligently to continue to develop and improve the FDX API with active and ongoing participation from member organizations. And while diversity of members and robust participation gives FDX the ability to seek standardization that works across the financial industry, these formal structures of work and the same balanced leadership structure (all groups are led by a FI and a

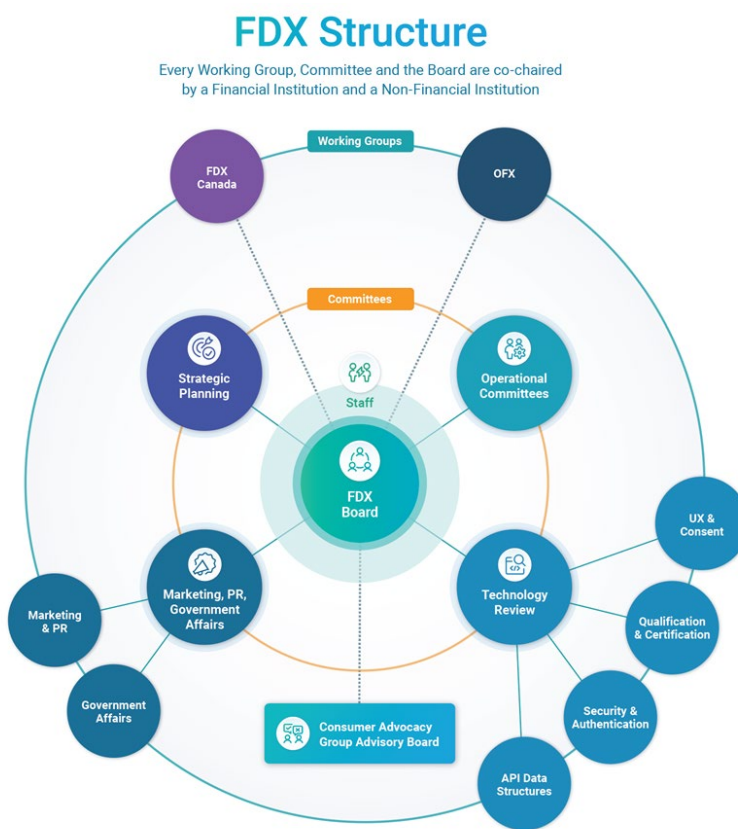
non-FI Co-Chairs), ensure that FDX standards consider all needs of the marketplace. Some of the FDX Committees, Working Groups and Taskforces include:

- 1.) Technical Review Committee: tasked with the ongoing maintenance and improvement of the FDX API technical specification, along with adopting or building other technical solutions to promote FDX objectives. The Technical Review Committee oversees several working groups to achieve these goals.
- 2.) APIs/Data Structures Working Group: tasked with creating programs and processes that will certify proper implementation of the FDX API standard, ensuring interoperability.
- 3.) Security & Authentication Working Group: tasked with the design of appropriate security and authentication protocols and related matters.

- 4.) FDX Canada Working Group: comprised of Canadian financial industry participants working within FDX to help ensure that uniquely Canadian market requirements are accurately reflected in the development and maintenance of the global FDX API standard.

- 5.) Consumer Advocacy Group Advisory Board: composed of non-profit consumer advocacy groups who elect from among themselves a board level observer. The consumer advocacy members provide input and recommendations at the working group and board level to ensure that consumer needs, security, experiences, and rights are kept at the forefront of FDX’s decision making process.

- 6.) User Experience/Consent Working Group: focused on best practices for user experience, consent matters and user engagement. The working group works closely with the Consumer Advocacy Group Advisory Board to improve standards, specifications, best practices relating to the consumer experience.
- 7.) Marketing, Public Relations and Government Affairs Working Groups: responsible for all communications functions of the organization including government affairs, public relations, and internal member communications as well as overseeing membership, marketing and FDX events.
- 8.) Open Financial Exchange: OFX joined FDX in 2019 as an independent working group tasked with maintaining and evolving the OFX standard as necessary to support the existing OFX



implementations, while leveraging the use cases and work between the OFX and FDX standards and providing a migration path to FDX for OFX users wishing to migrate.

FDX Deliverables to the Marketplace

Corresponding ANPR Questions: 20, 26, 27, 28, 32, 42, 43, 46

FDX launched a little over two years ago. In that time, FDX has delivered key standards, guidelines, and best practices into the marketplace. Here are a few of the key FDX deliverables to date and those anticipated in the near future:

- 1.) **FDX API Specification:** Currently at version 4.5, the FDX API is the foundation of FDX data sharing standardization and offers consumers the ability to access over 500 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive Open Finance standards in the world. The FDX API is designed to enhance interoperability and performance for the full range of both currently defined use cases as well as those anticipated in the future. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity and represents a global best-in-class solution set for user-permissioned data sharing that limits the risk of data inaccuracy.

- 2.) **User Experience & Consent Guidelines:** As adoption and implementation of the FDX API expands, these guidelines are the product of months of work and significant consumer testing and are intended to accelerate design decision-making during implementation of data sharing experiences. The User Experience & Consent Guidelines also seek to align user-permissioned financial data sharing with consumer understanding, preferences, and expectations. These guidelines specify what information and control must be given to end users to ensure consistent data sharing experience regardless of where their data is held or who they are seeking to share it with. Specifically, concepts such as financial data sharing, data flow, and data clusters, followed by specific user experience guidelines for an end user grant consent journey for financial data sharing are defined in this documentation. Eventually, FDX certification will involve compliance with User Experience requirements and the guidelines will be tailored to each FDX defined Use Case.

- 3.) **Taxonomy of Permissioned Data Sharing** In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX maintains a set of common terminology to be used as a taxonomy for the ecosystem. This documentation also includes a conceptual flow model to show how End Users interact with different participants within the current ecosystem that is evolving from legacy to new technology. The Taxonomy document¹² also provides a cursory comparison of similar terminology in the permissioned data sharing space among other parties such as the US Department of Treasury, US Consumer Financial Protection Bureau, and other key parties in the financial services industry.

¹² FDX Taxonomy of Permissioned Data Sharing v. 1.0 listed as Appendix A

- 4.) **Use Cases:** Use Cases are consumer-permissioned scenarios that help users minimize and limit the amount of data they share by defining the minimum amount of data elements that are needed for a given product or service as reasonably understood by the authorizing consumer. FDX use cases do not limit data access. Rather, they allow the financial services ecosystem to identify appropriately minimized and certifiable data sets needed to power an application and then utilize an industry-led standard like the FDX API to deploy and increase adoption of these use cases. In addition, FDX use cases offer the user-permissioned financial data ecosystem a pathway to quickly define and implement new or innovative use cases with the entire financial industry in a way that lowers barriers for new products and services. So far, FDX has approved a Personal Financial Management (PFM) use case and expects to define and certify specific use cases in the future, such as credit management and servicing, account verification, tax preparation and others.

- 5.) **Developing a Certification Program:** Creating a standard alone cannot promote, drive adoption, or guarantee adherence to the standard. A qualification and certification program are needed to ensure common implementation and interoperability of any technical standard and further limits the risk of data inaccuracy. Products (i.e., programs, services, and apps for consumer permissioned financial data sharing) can be approved by a certification program to test the technical compatibility/interoperability, prior to being marketed as a compliant product, or getting access to certain intellectual property rights. Work continues on FDX's certification platform, and FDX recently released foundational requirements covering availability, performance, and security that implementations of the specification must meet to apply for a FDX use case certification.

- 6.) **Global Registry:** An authoritative registry of trusted entities is needed to help the user-permissioned financial data marketplace clearly identify ever evolving technologies and new market entrants, as well as the web of often proprietary, incomplete, and incompatible technical standards that complicate the market today. Such a registry will enable those entities operating within the FDX and other ecosystems to reliably identify and verify trusted organizations and acts as a market incentive to all entities to ensure the accuracy of the data itself, as well as the transfer or exchange of that data. This registry will also support high volume and high velocity transactions, and interoperability across a variety of financial services, industry sectors and jurisdictions. In addition, a registry will provide assurance regarding reliability and repeatability of the performance of data, traceability, transparency, and trust in FDX Certification(s), accelerates the adoption of standards, and serves to bind the ecosystem players to each other. FDX intends the Global Registry to act as a non-profit, non-commercial, technology agnostic, multi-tenant, cross-sector, authoritative international resource as well as a center of technical excellence.

Lessons Learned – Examining Other Jurisdictions

Corresponding ANPR Questions: 5, 46

It is still early days for open banking and open finance markets around the world. The regulatory experience of a few jurisdictions can offer some guidance to the CFPB. That said, FDX comments here are limited to regulatory approaches to technical standards rather than regulations pertaining to financial data access rights.

The UK, European Union, Australia, Mexico, and Brazil are pursuing regulatory approaches to technical standards for user-permissioned financial data sharing and data access. Such a regulatory-driven approach is common in these jurisdictions because these markets tend to have a single financial regulator and a concentrated banking market (i.e., 9 major banks in the UK, 4 in Australia, 4 in Mexico, etc.). The resulting technical standards often apply to a significant portion of the market all at once. However, without an ecosystem approach that considers the needs of a large and complex market, and its diverse participants (especially important in the US with over 14,000 financial institutions), such technical standards can be ill-fitting to smaller market participants. In addition, regulatory driven standards in these jurisdictions have required significant technical resources and have incurred substantial start up and opportunity costs. Finally, and most importantly, regulatory standards in these jurisdictions have become more akin to regulatory compliance - meeting regulatory minimums – rather than standards that seek to address the full market, prioritize, or solve market problems, or that are able to adapt to market needs. The result has been standards that cover limited financial data elements, and adoption and utilization rates that are below market-led approaches like FDX despite the weight of a government mandate and significant public resources.

As for a specific example, the government mandated approach in the UK is led by the Open Banking Implementation Entity (OBIE), which was created by the UK's Competition and Markets Authority, funded by a special assessment on large banks, and chartered with creating software standards and industry guidelines that drive competition and innovation in UK retail banking. It was driven by privacy concerns and the need to create more competition. The OBIE technical approach was twofold: to build functional APIs to cover account information and payments in partnership with the 9 largest banks and develop security controls with the OpenID Foundation. While operating with a significantly smaller population than the US, Open Banking in the UK reached 2 million consumers by September 2020. In comparison, FDX's voluntary and market-led approach in the US reached 12 million consumers by the same time with no regulatory mandate, government resources or the benefit of a multi-year head start.

In reviewing other jurisdictions, FDX encourages the CFPB to also take note of negative impacts that fixed deadlines have had on adoption of and compliance to technical standards. Specifically, FDX encourages CFPB to consider the fixed deadline approach in these jurisdictions compared to a market driven approach that allows solutions to be piloted methodically by market entities and then implemented organically in an organization's normal technical product development and change calendar.

FDX suggests the CFPB also consider the experience of other market-led approaches to financial technology innovation like online banking, mobile banking, and the EMV (EuroPay, Mastercard, Visa) chip replacing the magnetic stripe on cards. All of these significant technological transitions in financial

services moved forward without government mandates or artificial timelines. Further, outside the fintech sector – examples like Bluetooth, Fast Identity Online (FIDO), Universal Serial Bus (USB) and the Payment Card Industry Data Security Standard (PCI DSS) show how market-driven solutions have been successful.

In sum, FDX submits that regulatory mandated technical standards for user-permissioned financial data sharing in foreign jurisdictions have underperformed compared to market-led standards in the US and are ill-suited to the unique dynamics of the US financial regulatory system and market. Compliance to regulatory standards has been expensive in terms of public resources, time and for some new and small companies in terms of technical integration and opportunity costs. Compliance requirements can also prove to be inflexible to dynamic market needs. In addition, they are often not suited to small market players and have been adopted at a rate lower than market-led standards. On the other hand, market-led standards developed by organizations like FDX are not dependent on government mandated funding, allow the market to set the scope and direction of its work and prioritizes market needs with a democratic approach that is open to all ecosystem participants.

Addressing Specific ANPR Questions about Technical Standards

Corresponding ANPR Questions: 5, 10, 13, 14, 15, 16, 23, 24, 28, 42 & 43

FDX wishes to respond specifically to several questions contained in the ANPR related to either market-led technical standards or questions where FDX believes market-led technical standards are best suited to address an issue or question.

Overall, FDX firmly believes that market-led standards are best suited to define the technical aspects of user-permissioned data sharing in the US market. FDX believes it would be a mistake for the CFPB to attempt to define technical standards in any way. Regulatory-led or government mandated technical standards related to financial data sharing and open banking have proven to be limited in scope, time consuming and unable to adapt quickly to market conditions and technological changes. Also, government mandated technical standards have the potential to significantly slow or freeze innovations because technical standards become a compliance exercise rather than an attempt to define standards that are responsive to market needs and consumer demand.

On the other hand, common, interoperable, royalty-free, and market-led technical standards not only maintain accessibility and innovation in the financial services industry but propel them forward. Specifically, common market-led standards level the playing field and lower the barriers to entry for market entities of all shapes and sizes because the cost and efficiency of connecting to implementations of the same standard across the ecosystem is much lower than a multitude of proprietary standards. Open market-led standards are also able to be continually adapted with balanced input from all market participants. Finally, and by their very nature, market-led technical standards adapt to the needs of the market. Whether it is a new product and service that technical standards need to address or new technologies that should be implemented, market-led technical standards are never wed to one approach, one technology or one market segment. They grow, mature, and change with the market and with consumer demand.

Questions & Answers

- 10. Should the Bureau expect data access ecosystem participants to develop and adopt multilateral rules applicable to authorized data access? How should the Bureau expect any such rules to impact competition and innovation and how should the Bureau take account of any such impacts in implementing section 1033?**

FDX Answer:

As stated previously, FDX does not differentiate its standards between authorized or direct data access, since FDX members, and the marketplace in general, use both methods of data access to ensure consumers are able to connect to, permission and use their financial data. Instead, and because the shared data is the same, FDX is delivering technical standards, certification, and industry best practices (market deliverables listed above) that focus on the control, access, transparency, traceability, and security standards for the data so that user experience can be the same across the market.

That said, the CFPB should absolutely expect data access ecosystem participants to develop and adopt multilateral rules and standards that govern the technical aspects of data access, and FDX is doing so. Examples of this work include the recently defined Personal Financial Management (PFM) Use Case, User Experience and Security guidelines, a technical specification that covers all forms of financial data, a Certification platform that will provide objective measures of conformance, and work with other standards bodies around the world like the OpenID foundation to provide global interoperability.

- 13. To what extent should the Bureau expect broad-based standard-setting work by authorized data access ecosystem participants to enable and facilitate authorized data access? What favorable or unfavorable impacts to competition and innovation should the Bureau anticipate from such work? How should implementation of section 1033 access rights take account of such broad-based standard-setting by system participants?**

FDX Answer:

The CFPB should expect the US financial industry to continue to develop and enhance technical standards for user-permissioned data sharing through FDX. In just a little over two years, FDX not only has significant momentum with 167 members and over 12 million US consumers converted from screen scraping to the FDX API, but it is also best positioned to continue unifying the financial industry around its common, interoperable, and royalty-free technical standards. FDX can make this claim because it has the broad commitment and participation of its members from across the financial data ecosystem, including financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups, industry utilities, service providers, other permissioned parties and even individual academics and experts in the field.

FDX also wishes to make the CFPB aware of the way FDX standards refer to and build upon the work of other existing global standards organizations like the Internet Engineering Task Force (IETF), the Open ID Foundation (OpenID), National Institute of Standards and Technology (NIST) and the FIDO Alliance (FIDO). In other words, FDX does not seek to “reinvent the wheel” where existing open

standards exist and instead seeks to provide technical standards that provide foundational global interoperability for a financial services industry that is increasingly borderless and regulatory structures that vary between jurisdictions. Indeed, technical harmonization around the globe, especially on privacy, security, and authentication, is critically important and FDX is actively engaged with and following other global open banking and open finance regimes around the world.

Additionally, FDX technical standards can be tailored to accommodate any regulatory or legal requirements in a given jurisdiction. FDX standards are not intended to answer every question or solve every issue in the marketplace (i.e., whether the CFPB should develop regulations to implement Section 1033 of the Dodd-Frank Act). However, FDX seeks to implement technical standards to accomplish the “means and methods” of user-permissioned data sharing in a way that is responsive to market needs as well as any legal or regulatory compliance requirements that may be put in place in the US.

Finally, and as stated earlier, FDX believes that market-led technical standards for user-permissioned data sharing are the best path forward to expand market participation and innovation in the United States. Such standards provide a level playing field for all market participants, so that entities of all sizes can compete with the same tools, and so that even the smallest financial institutions can offer their customers the same API-based data sharing services, tools and protections that are provided by larger financial institutions. Market-led technical standards, in concert with a working group structure and standardization of data use cases, also allows any fintech firm to bring innovative models forward that can be defined quickly and implemented in the marketplace rapidly so that consumers can use their own financial data in new and innovative ways. Additionally, market-led technical standards offer the ability to achieve nimble adaptations to changing market conditions. And finally, without a common, open, interoperable, and standardized API, along with additional standardization of authentication, authorization, certification, user experience and consent guidelines, financial institutions, financial data access providers and fintech applications and services will remain fragmented – using incompatible APIs, processes and even definitions of how a user is able to permission use of their own financial data. Such an outcome slows innovation, fragments user experience, limits market participants and typically tilts the market towards large, well-capitalized incumbents.

14. Should the Bureau seek to encourage broad-based standard setting work by authorized data access ecosystem participants? If so, how should it do so?

FDX Answer:

FDX not only believes CFPB should encourage continued standard setting by all market participants in the user-permissioned data sharing ecosystem by considering ways it can acknowledge, reference, and point to FDX standards in the marketplace, but FDX notes that the 1033 statute actually directs the CFPB to “promote the development and use of standardized formats.” In other words, FDX submits that the proper question is not whether the Bureau should seek to encourage broad-based standard setting work, but rather how the CFPB should encourage this work.

In one sense, the very nature of many market-led technical standards bodies is to exist and operate outside of a regulatory structure. And yet, ecosystems developing and certifying technical standards

often face a “catch 22” of sorts. On one hand, market entities want to maintain independence in technical standards work, but on the other hand, these entities desire a supportive acknowledgement or reference from regulators to show approval of the standards themselves and the direction of the work. In fact, regulatory acknowledgements provide significant value. They provide a sense of stability in the work and standards themselves, and such references can also help an industry coalesce around common interoperable standards rather than pursue a multitude of proprietary implementations. This is especially helpful to smaller entities as discussed above.

In addition to prior US Government references to industry-led technical standards for data sharing¹³, FDX recently noticed one instance of regulatory encouragement of market-led standards when the Financial Stability Oversight Council's (FSOC) annual report recommended that member agencies support adoption and use of standards in mortgage data, including consistent terms, definitions, and data quality controls. This recommendation pointed to the Mortgage Industry Standards Maintenance Organization (MISMO) and serves as a prime example of the type of regulatory reference or acknowledgement that helps market participants, especially those across a diverse and competitive ecosystem, continue to collaborate and coalesce around common industry standards. Similarly, the Appendix E of the Fair Credit Reporting Act (FCRA) *Interagency Guidelines Concerning the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies* states that information should be furnished in a manner than is designed to minimize the likelihood of errors and should "be furnished in a standardized and clearly understandable form and manner and with a date specifying the time period to which the information pertains."

Considering this, FDX would like to submit three specific recommendations for the CFPB to consider as it thinks about how to encourage standards work:

- 1.) **Reference & Acknowledgement** - FDX encourages the CFPB to think about ways it can explicitly endorse or reference technical standards and certification organizations and the work it is doing. Further, such endorsements or references should flow throughout the organization - from the CFPB Director down to those within the CFPB tasked with regulatory oversight and enforcement - so that everyone at the CFPB who encounters an implementation of a certified standard within the ecosystem has the ability to understand how the standard works and what it means. In this, FDX encourages the CFPB to even consider how standards and certification bodies might be able to provide training materials on their standards so that CFPB officials are up to speed on the latest versions and certifications of a technical standard in the marketplace.
- 2.) **Clarity** - CFPB may consider ways it can provide regulatory clarity that can assist standards work. Especially in a digital world, where engineers can only code to 1 or 0, or where conformance testing often exists in a binary state (pass or fail), regulatory clarity is extremely important. For

¹³ “Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators. A potential solution should address data sharing, security, and liability. Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers’ access to their data.” – U.S. Dept. of The Treasury, [“A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation”](#) July 2018

example, and while FDX cannot comment on specific policy or regulations, if there is a particular domain that the CFPB feels should be in a technical scope of an industry led body like FDX, then we would welcome that input and the industry, and their technical teams can work together to meet those requirements.

- 3.) **Harmonization** - Given CFPB's sole authority to promulgate regulations to implement Section 1033 of the Dodd-Frank Act, FDX encourages CFPB to coordinate with other financial regulators and harmonize and streamline requirements where possible so that industry standards are not caught between competing, overlapping or disjointed regulations.

15. What steps should the Bureau take to prescribe standards applicable to covered persons to promote the development and use of standardized formats for information that can be obtained by means of section 1033 data access rights? What form should such standards take? Should these standards differ depending on whether data is accessed directly by the consumer or through an authorized entity?

FDX Answer:

FDX submits that Section 1033 requires the Bureau to address standardized formats for data. However, the statute does not direct the Bureau to promulgate actual standardized formats for data sharing or data exchange. Instead, the statute directs the CFPB to “prescribe standards applicable to covered persons to promote the development and use of standardized formats for information...”¹⁴

With this in mind, FDX believes the statute intends CFPB to pursue a principles-based approach that will provide guidance to market-led technical standards like FDX as we continue to develop and promote adoption of common, interoperable, royalty-free standards for the secure and convenient access of permissioned consumer and business financial data.

Market-led technical standards like the FDX API can accommodate regulatory or legal requirements that are promulgated in a given jurisdiction. And consistent with previous answers, FDX welcomes principles-based CFPB guidance and regulatory clarity where market confusion and friction exist or where standards are unable to solve an issue. That said, FDX discourages the CFPB from pursuing actual regulatory technical standards in any form and for any access method for many of the reasons stated previously. Instead, FDX encourage CFPB to engage with industry standards and encourage continued work where the industry can arrive at common and interoperable standards.

Per this question, FDX also wants to make the CFPB aware of FDX's annual strategy survey that gives all FDX members, who represent the financial services ecosystem, the ability to be heard and direct the organization's work towards the highest priority issues in the marketplace. These surveys ensure that industry standards work remains agile and adaptive. FDX may also soon explore surveys that allow non-FDX members to weigh in on issues that need attention and standardization to ensure that FDX is responsive to all market issues in the user-permissioned data ecosystem.

¹⁴ [§5533\(d\)](#)

16. What steps, if any, should the Bureau take to promote particular mechanisms of authorized data access? If some mechanisms are more beneficial (or as beneficial but at lower cost to consumers), what are the obstacles to further adoption of such mechanisms, and what steps should the Bureau take to mitigate such obstacles?

FDX Answer:

FDX's core mission is to rapidly transition the user-permissioned financial data ecosystem away from shared user login credentials and screen scraping and to tokenized authentication and API-based data collection through the FDX API. As noted above, 12 million US consumers have already been converted from screen scraping to the FDX API. And eventually, through broad adoption of the FDX API standards, screen scraping will come to an end, and the flow of user-permissioned data between banks, aggregators, fintech applications, payments and online lending will be more secure and reliable.

FDX is unable to take a position on whether the CFPB should act or promulgate regulations related to particular methods of user-permissioned data access. However, FDX does wish to highlight that progress is being made, and that like other industry-wide technological transitions (i.e., EMV Chip Card), this work takes time. FDX also wishes to highlight the plight of small, community-based, financial institutions who are reliant on core technology providers to provide API-based solutions before they can transition away from screen scraping. Finally, FDX notes that its work to standardize security, user experience, data profiles and use cases is a critical element of the financial data ecosystem's ability to transition from screen scraping to APIs.

23. Should the Bureau propose to address the operational reliability of authorized data access, and if so, how, and why? Should the Bureau consider any different ways to address the operational reliability of direct access, and if so, how, and why?

FDX Answer:

The market has been addressing operational reliability of partners for years via a variety of methods. FDX believes that the measurement and evaluation of a given data access point's availability, responsiveness, and quality is a matter for the two parties exchanging data to determine. As they both serve the same customer (the end user) they both have a strong market incentive to optimize a given data connection's success metrics.

FDX, as a neutral non-profit standards body with no commercial interests, can be a forum where the industry can jointly define and report on the common metrics and formats for availability, responsiveness, and quality.

24. How should the Bureau ensure that any implementation of section 1033 access rights does not promote or require the use of particular access (or other) technologies?

FDX Answer:

FDX encourages the CFPB to support (as described above) and show restraint and defer to industry and market-led technical standards to ensure that the government is not in the position of promoting or requiring the use of particular access methods or technologies in the user-permissioned data ecosystem. FDX also encourages CFPB regulations to promote the use of standard formatting and refer to the FDX technical specification as one example of an acceptable standard.

In the same way the market eventually phased out legacy technology in favor of newer technology in other industries (i.e., cassette tapes and CDs giving way to Bluetooth and streaming in automobiles), the CFPB should expect the same natural market transition to occur with user-permissioned data sharing. Changing consumer demand and expectations, changing cyber risks, along with cost and efficiency of delivering products and services to meet such consumer demand and the advent of common market-led standards, will ensure that the market, instead of the government, chooses the best technology and data access methods going forward at any given time.

28. What tools can market participants provide consumers to align consumer expectations and preferences with the actual movement, use, storage, and persistence of authorized data? What steps, if any, should the Bureau take to improve the effectiveness of such tools?

FDX Answer:

FDX wishes to highlight two previously referenced FDX market deliverables as examples of tools the marketplace is already providing through FDX to align consumer expectations and preferences with the actual movement, use, storage, and persistence of authorized data - User Experience & Consent Guidelines and Use Cases.

The FDX User Experience & Consent Guidelines are the product of significant consumer testing and seek to make user-permissioned data access and sharing more consistent and familiar for users while also striving to align all market participants with consumer expectations around transparency, control, and ease of the process for permissioning financial data for use with fintech apps. Similarly, FDX Use Cases align the marketplace with the consumer expectation to share their financial data only for the product or service they initiated data sharing with in the first place. Use cases accomplish this by helping users minimize the amount of data they share by defining only the data elements that are needed for a given product or service.

In addition to acknowledging these tools, FDX also wishes to highlight previous statements about the importance of regulatory engagement, acknowledgement, and reference of such market-led work. The tools themselves are best developed and implemented by the ecosystem and market-led technical standards bodies, however, they can be benefitted by support and engagement from

regulators to ensure that the tools are meeting needs appropriately and to increase adoption of standards.

- 42. Are there risks that some data holders may not have adequate market incentives or legal requirements to ensure that the consumer data they provide to consumers or authorized third parties is accurate and that they correct inaccuracies when they occur?**

COMBINED

- 43. What risks of data inaccuracy are introduced as a result of the data access ecosystem? Do data users and data aggregators have adequate market incentives or legal requirements to ensure that the consumer data they use is accurate or sufficiently accurate for the purposes to which it is put? If your answer varies by the type of use to which consumer data is put, please explain why that is the case. How can data users and data aggregators act on such incentives, to the extent that they exist? To what extent have they so acted to this point or should be expected to so act going forward?**

FDX Answer:

As the user-permissioned financial data ecosystem continues to coalesce around market-led technical standards like FDX, the market incentives, and frankly, market penalties, that ecosystem participants face to provide accurate consumer financial data are only increasing. In other words, as common technical standards provide a level playing field, entities that are not providing accurate data will be weeded out of the marketplace. Further, tools like FDX certification and FDX's principle of providing traceability for all user-permissioned financial data will help provide a baseline of quality and consistency in the marketplace and identify the source of errors when and if they do occur.

FDX is unable to comment on whether further legal or regulatory requirements may be needed to enhance data accuracy.

Conclusion:

User-permissioned financial data access and sharing has brought immense disruption, innovation, and market participation to the financial services landscape in the US. And this upheaval has raised legitimate questions about consumer rights to access financial data.

Thankfully, many market issues are currently being addressed through common, interoperable, royalty-free, and neutral market-led technical standards that are especially valuable when new technologies and innovations shift the marketplace faster than policymakers and regulators can adapt.

Different jurisdictions around the world have engaged user-permissioned data sharing with different regulatory approaches, but the consistent need in every environment is a common standard. Indeed, the technical harmonization between these jurisdictions, especially on security and authentication, bears out this very tenet. With this in mind, FDX believes that its market-led standards are best suited to define the technical aspects of user-permissioned data sharing in the US market.

FDX welcomes continued engagement with the CFPB on these issues.

Appendix

- A. FDX Taxonomy of Permissioned Data Sharing**
- B. Publicly Announced Data Sharing Agreements Mentioning FDX API**

Appendix A: FDX Taxonomy of Permissioned Data v. 1.0

Published December 2020 – Initial Document Release

Legal Notice:

Financial Data Exchange is a standards body and adopts this Taxonomy of Permissioned Data Sharing for general use among industry stakeholders. Many of the terms, however, are subject to additional guidance under prevailing laws, industry norms, and/or governmental regulations. While referencing certain laws that may be applicable, readers, users, members, or any other parties should seek legal advice of counsel relating to their particular practices and applicable laws in the jurisdictions where they do business. See FDX's complete Legal Disclaimer located at <http://www.financialdataexchange.org> for other applicable disclaimers.

Introduction:

The Financial Data Exchange (FDX) is a technical standards body composed of financial institutions, financial technology companies, data aggregators, consumer groups and industry trade associations participating in the user-permissioned financial data ecosystem. Entities in this ecosystem occupy roles as user-permissioned data providers, data access platforms and data recipients as directed by the consumer or business. Some of these entities can occupy multiple roles at the same time. FDX seeks the development and promotion of a common, interoperable, and royalty-free standard – the FDX API - to facilitate the secure exchange of financial information and accelerate innovation while giving consumers or businesses greater control of their data and better awareness of how it is being used.

In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX proposes the following set of common terminology to be used as a taxonomy. FDX is also providing a conceptual flow model to show how End Users interact with different participants within the current ecosystem that is evolving from legacy to new technology. This document also provides a cursory comparison of similar terminology in the permissioned data sharing space among other parties such as the US Department of Treasury, US Consumer Financial Protection Bureau, and other key parties in the financial services industry. Additional markets outside the U.S. were reviewed for informational purposes, for example the “Consumer-Directed Finance” report of the Canadian Minister’s Advisory Committee on Open Banking, Australian Consumer Data Standards and the European Banking Authority (EBA).

FDX has adopted the taxonomy of terms set forth herein in all of its documents, artifacts and specifications moving forward. FDX is a standards body and also adopts this taxonomy for general use among its members, industry stakeholders, and others as normative. This implies that improper use of a term constitutes a blocking event that requires correction. For example, a Request for Comment (RFC) may be declined for improper use of a term. The same applies to all other documents being published, such as marketing materials or sanctioned newsroom articles. Many of the terms, however, are subject to additional guidance under prevailing laws, industry norms, and/or governmental regulations.

FDX welcomes comments and suggestions to its proposed taxonomy. Please send your comments to info@FinancialDataExchange.Org. Additionally, FDX will update this Taxonomy of terms from time to time and change the version and date specified above with each new revision.

Permissioned Data Sharing Taxonomy

Consumers: are end users acting in their personal capacity.

End Users: include consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data.

End User Delegates: refers to delegated persons or entities, such as End Users' CPAs, brokers, fiduciaries and other advisors, who have been authorized by the End User to grant permission to share and receive the End Users' Financial Account Information on the End Users' behalf.

Data Providers: the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages.

Data Recipients: service companies, applications (financial apps), financial institutions, products and services where End Users (on their own or through their End User Delegates) manage or act on their finances, whether actively managing their finances (such as moving money or applying for credit) or passively doing so (such as garnering recommendations or insights).

Data Access Platforms: intermediaries that facilitate financial data access, transit, storage and/or permissioning on behalf of Data Recipients or End Users, also commonly referred to as "Data Aggregators". In some cases, Data Access Platforms do not have a direct relationship with the End User. The data may be passed through without modification or may be normalized in line with permitted objectives (e.g., parsed for readability or used to confirm other data). Data Access Platforms should not be misidentified with parties who do not obtain End Users' consent but gather data, sometimes referred to as Data Brokers or Data Harvesters.

Account Credentials: any data used to identify and authenticate the End User to the Data Provider (such as username (I.D.), passwords (and possibly password hints and answers)) in order to gain access to the End Users' Financial Account Information.

Financial Account Information: the financial accounts, statuses, histories, balances and holdings, plus transactions reflecting monetary and financial actions directly sourced from Data Providers.

Derived Financial Data: consists of observations, data profiles, analysis or models derived from Financial Account Information.

Customer Identity Data: information about the End User that can be used to uniquely identify such End User.

Fintech: the word, is a combination of "financial technology" and often refers to a financial technology company that offers automated tools to End Users to use their financial data.

Screen Scraping (aka Data Scraping and Web Scraping): a method for the retrieval of Financial Account Information typically using an End User's Account Credentials (provided by End Users to a third party to obtain their Financial Account Information as though the End Users were connecting to the Data Provider). The modality of such access is often, but not limited to, from an HTML (hypertext markup language) page via electronic means (usually via automated script) but can also be from terminal emulation, API, or other interface.

Strong Customer Authentication (SCA) prescribes the use of two or more of these factors (known as **Multi Factor Authentication (MFA)**):

- Type 1 – Something you know – passwords, PINs, code words, etc.
- Type 2 – Something you have – typically smart phones, token devices, etc.
- Type 3 – Something you are – Biometrics (e.g., fingerprints, facial recognition, iris or retina scans).

End User Authentication: Process by which the End User’s access to Financial Account Information is authenticated by the Data Provider. This is accomplished via different mechanisms:

- Legacy tech (aka *Account Credentials-based access*) – the Data Access Platform or Data Recipient typically stores the End User’s Account Credentials and authenticates access to accounts with the Data Provider on behalf of the End User. Such access is typically limited to Type 1 authentication factors (see authentication factors above).
- Modern tech (aka *tokenized access*) –The End User authenticates directly with the Data Provider. **Note:** End Users do not provide their Account Credentials to either the Data Recipient or the Data Access Platform in this model.

End User Authorization: Process by which the End Users consent to share their Financial Account Information with Data Access Platforms or Data Recipients:

- Legacy tech (aka *Account Credentials based access*) – the End Users provide their Account Credentials to the Data Recipient and/or the Data Access Platform for access to the Data Provider on behalf of the End User. The resulting Consent can only be revoked at the Data Recipient or the Data Access Platform.
- Modern tech (aka *tokenized access*) – The End Users authorize the Data Providers directly to share their Financial Account Information with the Data Recipients and/or the Data Access Platforms. In addition to consent revocation at the Data Recipient and Data Access Platform, this also permits the Data Provider to manage the End User Consent and allows the End User to revoke it at the Data Provider.

Permissioning: the end-to-end process of granting, managing, and revoking Consent for data access.

Consent: In the permissioning process, Consent encapsulates the scope (duration, data, and use) of what is being shared as a result of the affirmative action of the end user.

Permission Dashboard: a digital experience that enables the End User to view the status of the permissions they’ve granted, and the parties or processes accessing data.

Revocation: the process or act of ending or removing permission for access.

Open Finance/Open Banking: While these terms are evolving and are often used interchangeably, they generally refer to an End User’s ability to access and share their own financial data. Different terms are often linked to the presence or lack of regulation, whether they be government-regulated financial data sharing regimes, market driven systems of End User permissioned data sharing or some hybrid of

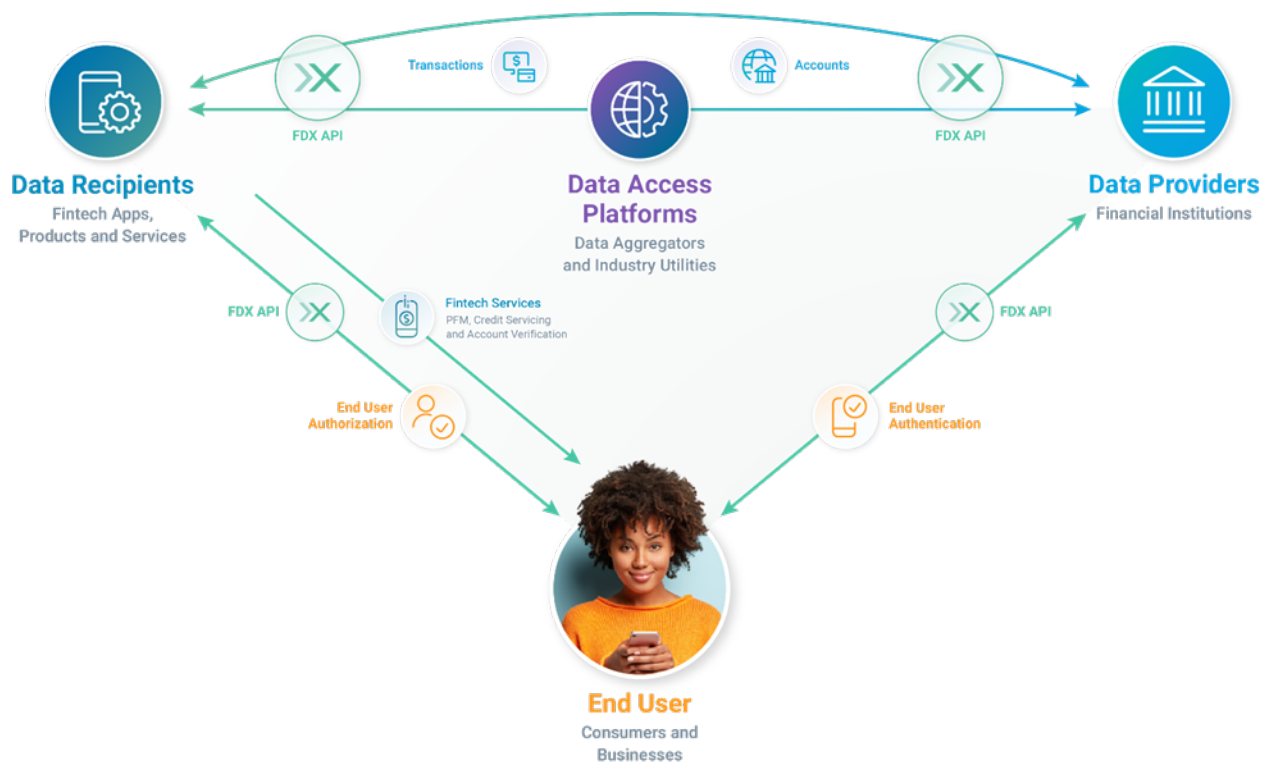
the two. Other similar terms include consumer directed finance, connected banking or permissioned data sharing.

Other Financial Data Sharing Terminology

Data Brokers: collect personal information from public and private records and provide this information to public and private sector entities for many purposes, from marketing to law enforcement and homeland security purposes.

Data Harvesters: use communication and information services, including applications (apps), to collect data from End Users and provide the data or derived digital products to third parties.

Conceptual Flow: End Users permission Data Providers to share their Financial Account Information with Data Recipients as shown below.



Suggested Taxonomy Reconciliation

Many of the participants in this space have offered differing definitions for each party and as such, there is often confusion in the ecosystem about what party and action is being discussed.

The table below attempts to reconcile the actors and actions in permissioned data sharing to respective parties' terms for them.

	End User	Data Recipient	Data Access Platform	Data Provider	Financial Account Information	Customer Identity Data
CFPB	Consumer	Permissioned Parties / Consumer-Permissioned Providers	Account Aggregators	Consumer Financial Account Providers	Consumer Financial Account Data	Non-Financial Consumer Account Data
US Department of Treasury	Consumer	Consumer Fintech Application Providers	Data Aggregators	Financial Services Companies / Financial Services Firms		
European Banking Authority (EBA)	Consumer	Account Information Service Providers (AISP)	Account Information Service Providers (AISP)	Account-Servicing Payment Service Providers (ASPSP)	Sensitive Payment Data	

The goal of this taxonomy and cross-referencing of terminology in the permissioned data sharing space will allow all parties to communicate more accurately about this space.

The following appendices note the sources of these definitions: US Consumer Financial Protection Bureau, US Treasury, European Banking Authority.

FDX Taxonomy Appendix 1: Consumer Financial Protection Bureau Definitions

Source: October 18, 2017 publication Consumer-authorized financial data sharing and aggregation

https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf

Source: Request for Information Regarding Consumer Access to Financial Records (Nov. 14, 2016) [81 Fed. Reg. 83806, 83808-09 (Nov. 22, 2016)]

<https://www.govinfo.gov/content/pkg/FR-2016-11-22/pdf/2016-28086.pdf>

- **consumer financial account data** is consumer financial account and account-related information.
- **consumer-permissioned access** is consumer access to such information, including access by entities acting with consumer permission.
- **consumer-permissioned account data** is account information that is obtained via consumer-permissioned access.
- **non-financial consumer account data** is data held by companies that offer consumers non-financial products and services.
- **consumer account data** refers collectively to both consumer financial account data and non-financial consumer account data.

- **consumer financial account providers** are entities that control or possess data about consumer use of their products and services.
- **consumer-permissioned providers** or **permissioned parties** are entities that rely, at least in part, on consumer-permissioned access to consumer financial account data.
 - Note: consumer-permissioned providers are third-party providers and do not themselves count as consumer-permissioned providers by virtue of using the account data that they already hold to deliver additional services to customers.
- **account aggregators** are entities that obtain consumer financial account data directly from consumer financial account providers for consumer-permissioned providers.
- **Consumer** is an individual or an agent, trustee, or representative acting on behalf of an individual per Dodd-Frank Act “covered person” in detail at 12 U.S.C. 5481(6).
- **account aggregation** or **data aggregation** is the process of accessing consumer account data.

FDX Taxonomy Appendix 2: Consumer Financial Protection Bureau Definitions

Source: July 2018 publication *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation*

<https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf>

- **Data aggregation** generally refers to any process in which information from one or more sources is compiled and standardized into a summary form.
- **Consumers** are the individuals who are users of financial services and the principal providers of the information collected by financial service companies.
- **Financial services companies** or **financial services firms** include banks, mutual funds, insurance companies, broker-dealers, wealth management firms, and other financial institutions that provide traditional retail banking, depository, credit, brokerage, investment, and other account management services to consumers. These companies are the sources of consumer financial account and transaction data.
- **Data aggregators** are the firms that access, aggregate, share, and store consumer financial account and transaction data they acquire through connections to financial services companies.
- **consumer fintech application providers** are the firms that access consumer financial account and transaction data, either from data aggregators or financial services companies, in order to provide value-added products and services to consumers.
- **fintech applications** are the websites or mobile apps created by consumer fintech application providers for consumers to access value-added products and services either from data aggregators or financial services companies.
- **Screen-scraping** is acquiring financial account and transaction data either manually or through specialized software.
- **API [Application Programming Interface]** is a clearly specified program that links two or more systems and that enables a well-defined communication and data exchange between them in order to run applications and other software.

- **Covered Person [Under Section 1002(6) of Dodd-Frank [12 U.S.C. § 5481(6)]]** is defined as “any person that engages in offering or providing a consumer financial product or service,” and any affiliate of such a person, if the affiliate acts as a service provider to that person.

FDX Taxonomy Appendix 3: European Banking Authority

PSD2 - Payment Services Directive 2 Title I Article 4 (Selected definitions excerpted here)

<https://eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/8701>

- **(10) ‘payment service user’** means a natural or legal person making use of a payment service in the capacity of payer, payee, or both;
- **(11) ‘payment service provider’** means a body referred to in Article 1(1) or a natural or legal person benefiting from an exemption pursuant to Article 32 or 33; (aka Third Party Payment Service Provider TPP);
- **(12) ‘payment account’** means an account held in the name of one or more payment service users which is used for the execution of payment transactions;
- **(15) ‘payment initiation service’ (PIS)** means a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;
- **(16) ‘account information service’ (AIS)** means an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;
- **(17) ‘account servicing payment service provider’ (ASPSP)** means a payment service provider providing and maintaining a payment account for a payer;
- **(18) ‘payment initiation service provider’ (PISP)** means a payment service provider pursuing business activities as referred to in point (7) of Annex I;
- **(19) ‘account information service provider’ (AISP)** means a payment service provider pursuing business activities as referred to in point (8) of Annex I;
- **(20) ‘consumer’** means a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his or her trade, business or profession;
- **(29) ‘authentication’** means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user’s personalized security credentials;
- **(30) ‘strong customer authentication’** means an authentication based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

- **(31) ‘personalized security credentials’** means personalized features provided by the payment service provider to a payment service user for the purposes of authentication;
- **(32) ‘sensitive payment data’** means data, including personalized security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data;
- **(38) ‘agent’** means a natural or legal person who acts on behalf of a payment institution in providing payment services;

FDX Taxonomy Appendix 4: Canadian Standing Senate Committee on Banking, Trade and Commerce

The following are selected definitions from the Canadian Standing Senate Committee on Banking, Trade and Commerce.

Source: June 2019 publication: *Open Banking: What it means for you*

https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_SS-11_Report_Final_E.pdf

- **Application programming interface (API):** An application programming interface (API) is a software intermediary that allows two applications to talk to each other. It acts as a universal access point by which information is retrieved from a database. APIs are the main technological mechanism by which data would be securely shared between a bank and a third-party provider in an open banking framework.
- **Consumer Data Right:** The right of Australian consumers to have control over their data. The right will be implemented sector-by-sector, beginning in the banking, energy and telecommunications sectors.
- **Financial Data Portability:** Financial data portability is the ability of consumers to direct that their personal financial information be shared with another organization.
- **Fintech:** Fintech refers to both the innovative ideas being developed into financial services technologies and applications, as well as the businesses that are offering these services. While fintech usually refers to independent financial services businesses, banks also offer fintech applications.
- **General Data Protection Regulation (GDPR):** The GDPR is the European Union (EU)’s privacy and data protection legislation which came into effect in 2018. It sets out several privacy rights for individuals, including the right to obtain one’s personal data from a company and send it to a third party and the right to have personal information erased and no longer shared with third parties.
- **Open Banking:** Open banking generally refers to a framework to give customers access to and control over their financial data. In most countries, open banking has two elements: financial data portability and payments initiation.
- **Open Data:** Open Data is structured data that is machine-readable, freely shared, used and built on without restrictions. One of the goals of an open data initiative is to enable computer-to-

computer transfer of information using a universal access point, called an API, to retrieve information from a database.

- **Payments Initiation:** Payments initiation is the enabling of payments directly from a bank account using a smartphone app, as an alternative to credit and debit card payments.
- **Screen Scraping:** Screen scraping is the process by which certain smartphone apps access banking data. Some fintech companies will use a customer's online banking login credentials to access the customer's bank account in order to collect and store the customer's account information and transaction history.
- **Third-party providers:** Third-party providers are those businesses that would be requesting customer banking information from banks in a Canadian open banking system. Initially, these businesses would likely be financial technology or "fintech" companies and other banks.

Appendix B: Examples of Publicly Announced Data Sharing Agreements Featuring the FDX API

- [Finicity Announces Secure Data Access Agreement with Brex](#) - December 18, 2020.
- [“Akoya and U.S. Bank team up to accelerate safe, secure, and transparent consumer-permissioned financial data access”](#) - November 16, 2020.
- [“Finicity and BMO Harris Bank Finalize Secure Data Access Agreement”](#) - November 12, 2020.
- [“Wells Fargo and Envestnet | Yodlee Sign Data Exchange Agreement”](#) - September 24, 2020
- [“FINICITY FINALIZES SECURE DIRECT DATA AGREEMENT WITH CHARLES SCHWAB”](#) - September 18, 2020.
- [“TD enters into North American data-access agreement with Intuit”](#) - September 2, 2020.
- [“TD enters into North American data-access agreement with Finicity”](#) – August 7, 2020.
- [“U.S. Bank and Fiserv sign agreement to simplify data exchange between customers and applications”](#) – March 9, 2020.
- [“Envestnet | Yodlee and JPMorgan Chase Sign Data Agreement to Enhance Consumer Data Protections, Bolster Overall Data Connectivity and Reliability”](#) – December 5, 2019.
- [“U.S. Bank signs agreements with top data aggregators and fintechs, bolstering API efforts”](#) – September 23, 2019.
- [“Wells Fargo and Plaid Sign Data Exchange Agreement”](#) – September 19, 2019