Testimony of Tom Carpenter
Director of Public Affairs, Financial Data Exchange (FDX)

Before the United States House Committee on Financial Services
Task Force on Financial Technology

Hearing entitled "Preserving the Right of Consumers to Access Personal Financial Data"

Tuesday September 21, 2021
Rayburn House Office Building, Room 2128

Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Davidson, and Members of the Task Force on Financial Technology, thank you for the opportunity to testify at today's hearing. My name is Tom Carpenter and I serve as the Director of Public Affairs for the Financial Data Exchange (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 over 200 data recipients like fintech companies, data providers like financial institutions, and data access platforms like data aggregators, as well as consumer groups, payment networks, financial industry groups and other stakeholders in the user-permissioned financial data ecosystem. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

In essence, FDX operates as a Bluetooth-like specification to enable API-based financial data sharing with fintech services. Just like Bluetooth, FDX has brought together diverse financial industry players from banks to fintechs, data aggregators to consumer groups, payment networks to industry associations and many stakeholders in between to define a common API standard so that the financial industry is not fragmented into a maze of proprietary standards. Just like Bluetooth offers consumers the ability to use different consumer electronic products in an interoperable manner, regardless of manufacturer, FDX is defining a common standard so that sharing and moving financial data between financial institutions, fintechs and intermediaries is seamless, secure, transparent, consumer centric, and not dependent on where one banks or which fintech app they choose to use. And most importantly, through implementation of the FDX API, users within the financial data ecosystem are able to be securely authenticated without the sharing or storing of their login credentials with third parties. In fact, through broad adoption of the FDX API, screen scraping, or 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.

The good news today is that FDX is not just an attempt at such industry standardization and transition to API-based financial data sharing. Rather, and less than three years since its founding, FDX is a roaring success. FDX has surpassed 200 members that all work through FDX's over 30 different working groups and task forces to continue developing and enhancing the FDX standards. The FDX API itself is being implemented broadly across the financial services industry and will soon be certified for required data elements, technical conformance and availability. The FDX API is currently used by 22 million consumer accounts in the US and Canada for financial data sharing. Further, the FDX API currently defines over 620 unique financial data elements that consumers can access, share and leverage for their own financial benefit, making it one of the most robust open finance APIs in the world today.

Scope of Testimony:

My testimony today is drawn from the insight and perspective FDX has gained as an industry standards body with diverse membership[1] across the financial services ecosystem. In this, my hope is to provide the Task Force with a vantagepoint into the relationships between financial data providers[2] (i.e., financial institutions and banking organizations), data recipients[3] (i.e., third-party financial technology companies or fintechs) and data access platforms[4] (i.e., data aggregators and ecosystem intermediaries) in relation to user-permissioned financial data sharing. In addition, my testimony is intended to inform the Task Force about the progress and maturity of FDX since its launch less than three years ago, including a detailed view of FDX's mission, structure, and vision to implement common, interoperable, and royalty-free technical standards for user-permissioned financial data sharing.

As a technical standards body, FDX is currently barred from taking positions on most legislative and regulatory policy issues. 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.

---

[1] FDX Members

[2] From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: Data Providers: the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages.

[3] From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: Data Recipients: service companies, applications (financial apps), Fintechs, 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).

[4] From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: 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 may 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 Brokers5 or Data Harvesters.

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.

Ultimately, FDX believes open banking or open finance has two halves – a "What" and a "How." The "what" is often determined by legal agreements between financial services entities or defined in legislation or regulation. The "what" encompasses many of the decisions and guidance about financial data rights, determinations about what constitutes derived data and the way different entities and roles within data sharing are regulated.

On the other hand, the "how" of open banking or open finance involves the technical means and methods that enable the full scope of user-permissioned financial data to be securely shared and transmitted between data providers, data access platforms and data recipients. This "how" is where FDX is succeeding in defining a common, interoperable and royalty-free API standard and accompanying guidance so that financial data sharing is consumer-centric, complete, secure and uniform regardless of where a user banks, what financial services they access or what fintech apps they may choose to use.

Considering this, and in the context of the ever-changing roles and relationships between different financial services entities involved in financial data sharing, FDX believes it is important to provide the task force with a perspective on how user-permissioned financial data sharing is actually working in the market today.

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 and are increasingly on the receiving end of financial data from other financial institutions as directed by their customers.

To utilize these 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, different data scopes, processes and even definitions for 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 that can replace the need for screen scraping for the same user-permissioned financial data elements.

Key Points for the Task Force:

In an effort to provide the task force with thoughts on issues as requested in testimony for this hearing, I would like to list a few key points that I believe are critical for the task force to understand and consider related to the current state of consumer data sharing, industry standardization and the benefits that permissioned financial data sharing is delivering to consumers and small businesses.

Five 5 Principles of Consumer Data Sharing

The ability for consumers to access and share the entirety of their own financial data, whether via authorized or direct access, is the central pillar upon which FDX is built. And 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 greater consumer protection and full 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.

2.) **Access** – End Users should have access to their data and the ability to determine which entities will have access to their data.

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.

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.

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.

Benefit of user-permissioned data sharing:

Before anyone coined the term open banking or open finance, consumer demand for budgeting, payments, digital lending, importing tax data and other fintech applications served as a catalyst for the innovative and diverse financial services marketplace we have in the U.S. today. And consumers are the beneficiaries of this competition and innovation because they now have more choices, great efficiency and lower costs for financial services. Some specific benefits of consumer permissioned financial data sharing include:

1.) **Enhanced transparency into one's financial circumstances** - Put simply, the ability to access and share the full extent of a consumer's financial data now allows consumers to actually see their money, debt, investments and bills all in one place which allows for better management and more informed financial decision making.

2.) **Expansion of credit access and lower cost of credit** - Financial data sharing is accomplishing a long-held goal of this Committee by broadening credit access to thin-file or no-file borrowers because lenders are able to determine credit worthiness from cash flow data when a traditional credit score is limited or incomplete.

3.) **Increased financial literacy and utilization of financial data** – Financial data sharing is giving consumers the same powerful tool that many companies have utilized for years – Big Data. And while the notion of big data often has a negative connotation, when a consumer has the reins of all of their own data, they are able to better understand their own financial lives and use it to leverage better financial outcomes.

4.) **Lower Costs** – The provision of digital and automated financial services tools help consumers manage their money, including by avoiding overdraft fees and lowering lending costs due to more efficient processes, a better determination of credit worthiness, better rates and lower fee products.

Distinction of User-Permissioned Financial Data Sharing vs Data Collection & Data Harvesting

It is important for the task force and regulators to consider a bright line distinction between user-permissioned financial data sharing, and activity undertaken by actors like data brokers or data

harvesters. From an FDX standpoint, I want to stress to the Task Force that all financial data used and accessed through the FDX API standard must be user permissioned. In other words, no financial records will be accessed without a consumer's full permission and control. This contrasts sharply with practices where data about consumers is collected and/or sold without express consumer consent, consumer control or consumer awareness. This distinction is important as the Task Force and Committee consider privacy questions about financial services activities involving consumer financial data.

Technical Standards Best Left to Industry

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 Congress or the CFPB to attempt to define technical standards in any way.

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. 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.

In addition, FDX technical standards can be tailored to accommodate any regulatory or legal requirements in a given jurisdiction. As mentioned, FDX is neutral on policy issues 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 Congress or the CFPB may place on user-permissioned data access.

FDX also wishes to make the Task Force 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.

But don't just take my word for it. I encourage the Task Force to 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.

Alternatively, 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.

It is also important to consider the market dynamics of jurisdictions pursuing regulated or government mandated standards. Often these markets 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, multiple financial regulators 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.

Shifting Roles within Consumer Permissioned Data Sharing

FDX defines four key roles within user-permissioned data sharing, End Users, Data Providers, Data Access Platforms and Data Recipients.

- **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.
- **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), fintechs, 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 may 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.

While each of these roles have traditionally been played by specific market actors (financial institutions have played the role of data providers, data aggregators and other intermediaries have played the role of data access platforms and fintechs have played the role of data recipients), today's user-permissioned

data ecosystem involves financial services firms often playing many of these roles, and sometimes simultaneously. For example:

- Financial institutions increasingly play the role as both data providers and data recipients when their customers seek access to account data from other financial institutions or seek credit that may involve cross-institution data sharing.
- The role of a data access platform has expanded to include different industry utilities, intermediaries and approaches. In addition, some data aggregators are serving functions for financial institutions to allow for more seamless data sharing experiences, like managing end-user permissions and obtaining consent.
- While still in its infancy, even fintech apps may soon move beyond the role of data recipients and into the role of data providers with two-way data sharing or reciprocity that provides a flow of fintech data back to financial institutions.

With this in mind, FDX standards are focused on the role itself rather than the type of entity performing said role and FDX encourages future Task Force considerations around consumer data sharing to also consider the role in the ecosystem versus the type of entity playing it.

Views on CFPB Rulemaking

FDX submitted comments[5] to the Consumer Financial Protection Bureau's (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. In addition, FDX was mentioned or referenced in relation to how the financial industry is creating technical standards in almost half of the comments the CFPB received on the ANPR.

While FDX is unable to comment on specific elements of potential CFPB rulemaking, or even if CFPB should proceed with rulemaking at all, I would like to submit the following contextual thoughts:

- FDX believes that the ability for consumers to access, control and share all of their own financial data, whether via authorized or direct access, in a transparent, traceable and secure manner is paramount.

- FDX believes that consumers expect full access to their own data to use, share and leverage to their financial benefit. We believe that consumers also expect that they alone should have control of how their data is permissioned, shared, used, or accessed, as well as having the ability to revoke such choices. We believe that consumers expect to be clearly informed about who has access to their data, what purpose it will be used for and for how long it will be used. Finally, we believe 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.

- FDX believes that when a system of financial data sharing appropriately provides FDX's Five Principles (Control, Access, Transparency, Traceability and Security), consumers benefit in the

---

[5] https://www.regulations.gov/comment/CFPB-2020-0034-0019

form of cost savings, transparency, efficiency, control, enhanced financial awareness and security.

- FDX believes 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. Such market-led standards, such as the FDX API, can be tailored to accommodate regulatory requirements and 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 the CFPB and other regulators can and should do more to prioritize the adoption of common and interoperable APIs and reduce structural disincentives that might delay adoption and implementation of APIs. This includes formal reference or acknowledgement of market-led standards to show approval of the standards themselves and the direction of the work. This is especially important for smaller entities. Such support also includes better training and understanding from the top of the agencies down to those involved in examination and regulatory enforcement so that all are aware of how standards are being implemented and used in the marketplace.

- FDX believes that regulatory modernization must prioritize harmonization. FDX encourages regulators to work together where possible so that industry standards are not caught between competing, overlapping or disjointed requirements.

- FDX believes that public policy around consumer data sharing must balance the need for consumers to be able to access and share the full extent of their own financial data with data recipients who may have no relationship with the data provider with data providers, like banking organizations, to maintain sound risk management practices, conduct activities in a safe and sound manner, and remain consistent with applicable laws and regulations.

- FDX believes that rapid innovation in the marketplace and evolving and overlapping industry roles within the user-permissioned data sharing ecosystem means that policy must consider addressing the role that is being played rather than focusing on a specific market segment or entity playing the role.

Conclusion:

As the Director of Public Affairs for the Financial Data Exchange, I am thankful for the opportunity to provide testimony to the Task Force today. I believe it is important for Task Force Members to be aware of the policy issues inherent to user-permissioned financial data sharing, but also the immense progress that the industry has made in regard to technical standards which enable this data sharing, and which are powering the transition from screen scraping to interoperable APIs. I welcome your questions.

Appendices

A. **Structure & Details of the Financial Data Exchange**
B. **FDX Five Principles of Consumer Data Sharing**
C. **Publicly Announced Data Sharing Agreements Mentioning FDX API**

Appendix A: Structure & Details of the Financial Data Exchange

In less than three years, FDX not only has significant momentum with over 200 members and over 22 million 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, investment 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.

As a technical standards body, FDX's members develop, enhance and adapt the FDX API and accompanying standards via a board of directors and over 30 different committees, working groups and task forces. FDX maintains fairness by ensuring that its membership is diverse and that all market segments within the larger ecosystem have the opportunity to participate in the work. FDX also employs a balanced leadership approach across all work streams with each committee, working group and task force co-chaired by a financial institution and a non-financial institution. Finally, every FDX member organization, regardless of size, type, or dues, has a single and equal vote.

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.

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.

Below is a list of FDX's Committees Working Groups and Task Forces

Committees

Audit & Finance	Assists the Board in discharging its responsibilities relating to independent oversight, financial reporting, budget, internal controls and procedures and related matters. It performs both an audit and a finance role.
Compensation	Determines FDX's overall compensation structure, policies and programs, as well as oversees compensation of FDX's Managing Director, other executives and key employees.
Executive Steering (ESC)	The ESC is comprised of nine sustaining members, with a similar industry representation to the Board, that has the authority of the Board (subject to certain restrictions and override authority of the Board) and meets monthly. The FDX Board has ultimate authority with respect to any decisions of the ESC.

Marketing, PR & Government Affairs	Shares FDX stories and milestones, and seeks to increase membership in FDX by raising awareness of the benefits of FDX's common interoperable standard.
Technical Review (TRC)	Provides technical oversight to all working groups, including technical standards, versioning, and related matters. The TRC's role involves oversight and alignment of artifacts produced by technical working groups.

Working Groups

API & Data Structures	Maintains, revises, and releases the API and data specification. In addition, provides any necessary artifacts in support thereof, such as meta data, dictionaries and use cases.
Canada	Assesses the potential for use of the FDX API in Canada, recommends any changes to the FDX API that may be required for use in Canada, and if suitable, advocate the use of the FDX API in Canada.
Consumer Advocacy Group Advisory Board	Composed of Consumer Advocacy Groups, this group provides advisory services to the FDX Board and Working Groups on a mutually agreed upon basis.
Global Summit	Oversees the planning and execution of all FDX biannual Global Summits. Determines the topics, speakers, presenters, schedules, formats, and appropriate venues for each summit.
Marketing & Public Relations	Addresses all topics related to Marketing and Public Relations matters. This includes raising awareness of the benefits of FDX standards and other goals of the Marketing, PR & Govt Affairs Committee.
OFX	Provides on-going support and enhancements as needed to the OFX specification and associated services, in a secure and user-controlled manner.
Qualification & Certification	Develops and maintains the FDX product certification program, Foundational Certification, to ensure technical interoperability among FDX member organizations. Further, it oversees the development of an FDX Directory and Registry.
Security & Authentication	Develops and maintains the FDX API Security Model and standards, and related artifacts in support thereof.
U.S. Government Affairs	Amplifies the efforts of the Marketing & Government Affairs Committee in its educational and outreach efforts with governmental bodies (regulatory, appointed and elected).
User Experience	Develops industry guidelines and best practices for the user experience when sharing and accessing their financial data. The overall goal is a consistent user interface across the industry driven by FDX's core principles.

Standing Task Forces

API Governance & Authoring	Task force to oversee documentation authoring process so RFC author proposals are formulated in line with the authoring strategy.
Canadian Government and Regulatory Engagement	Task force to guide the educational engagement of FDX and its members with government representatives, policymakers, regulators, and industry stakeholders in Canada.
Canadian Technical	Task force to oversee all technical work for Canada, to align FDX technical specifications for application in the Canadian market, and to make recommendations to other FDX working groups.
Consent API	Task force to develop supporting Consent API to synchronize the consent experience and enable transmission and presentation of consistent data sharing consent between entities in the ecosystem.
Consent Management & Consent Dashboard	Task force to author User Experience for consent management, consent parameters and consent revocation in consent dashboards.
Governance and Oversight	Task force to oversee overlapping task force issues within User Experience and help the working group determine prioritization.
Money Movement Planning	Task to incorporate money movement and payment capabilities into the FDX API including features, user experience, security, interoperability and certification.
Sensitive Data Solutions	Task force to develop a solution for use cases requiring use of sensitive data that satisfies the use case while maintaining security and privacy.
Strategic Planning	Task force to develop the strategy, annual plan and priorities for all FDX activities and working groups that will deliver on the FDX mission.
Tax Forms	Task force to develop FDX formatted tax forms and schemas and transition providers away from using legacy tax data formats.
Taxonomy	Task force to author and publish updates to FDX Taxonomy for use within FDX and to inform external stakeholders.
Use Case Development & Maintenance	Task force to explore and develop user-permissioned data sharing use cases.
User Journeys	Task force to author consent flow and use case journeys for evolving the User Experience Guidelines.
User Experience Research	Task force to evaluate needs, execute and report out on user experience research.

Special Purpose Task Forces

App Registration	Task force of the Security & Authentication working group to explore scalability issues related to Recipient Application Registration between Data Access Platforms and Providers and to explore standards for Provider Automated Application Registrations.

Cryptocurrency	Task force of the API working group to develop attributes and modifications allowing FDX use for cryptocurrency portfolios, transactions, exchanges and tax reporting.
Fraud Monitoring	Task force of the API working group to build fraud monitoring and controls into the FDX specification including modeling use case-based fraud scenarios, data required for suspicious activity and fraud reporting.
Data Clusters	Task force of the User Experience working group to determine data cluster grouping, consumer understanding, visual treatment and mapping to use cases. The task force will also define consent object, enabling consent grant management and requirements for consent API technology.
Certification Model	Task force of the Qualifications & Certification working group to develop FDX's Certification model 1.0.
Directory	Task force of the Qualifications & Certification working group to create and maintain an FDX Registry of membership, technical conformance and relevant parties.
Notifications	Task force of the API working group to define the notification framework and specify security guidelines, specifications, document use cases and operation best practices for event notification.
Testing & Tooling	Task force of the Qualifications & Certification working group to develop test suites for FDX certification.
Intermediary Identity	Task force of the Security working group to specify modifications and methods to use the OAuth framework so that Data Access Platforms are able to perform functions for Data Recipients like end-user transparency, registration and traceability functions.
FAPI & FDX API Security Profile Harmonization	Task force of the Security and Authentication working group to identify elements of FAPI specification for FDX to deem normative and to establish reference to FAPI certification as a requirement for FDX certification.
Recipient Certification Requirements	Task force of the Qualifications & Certification working group to determine expectations and responsibilities of data recipients and what must be provided for certification.

FDX Deliverables to the Marketplace

Since its launch in 2018, 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.) <u>FDX API Specification</u>: Currently at version 4.6 (with FDX API 5.0 anticipated release before the end of October 2021), the FDX API is the foundation of FDX data sharing standardization and offers consumers the ability to access over 620 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.) <u>User Experience & Consent Guidelines</u>: 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.) <u>Taxonomy of Permissioned Data Sharing:</u> 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 document[6] 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.

4.) <u>Global Registry</u>: FDX is currently building an authoritative registry of trusted entities 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. The FDX Global 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 interoperability across a variety of financial services, industry sectors and jurisdictions. In addition, the FDX registry will provide information 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

---

[6] FDX Taxonomy of Permissioned Data Sharing v. 1.1 listed as Appendix C

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.

5.) <u>Certification Use Cases</u>: FDX use cases are testable data profiles that measure functional capability of an API against a broad business use of financial data. FDX defines these data profiles as a means of establishing functional baselines that APIs must meet to be considered useful by data consumers, but <u>FDX use cases do not limit consumer data access</u>. In fact, FDX encourages sharing of other data even when not defined in use cases as necessary to meet innovation and business goals. FDX recommends that any such sharing be in line with FDX's five principles of financial data sharing – Control, Access, Transparency, Traceability and Security (CATTS). So far, FDX has approved Personal Financial Management (PFM) and Credit Management and Servicing (to support credit decisioning and scoring) use cases. It expects to define and certify specific use cases in the future, such as money movement, account verification, tax preparation and fraud reporting.

6.) <u>Developing a Certification Program</u>: 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.

7.) <u>Annual Strategic Survey</u>: FDX's annual strategy survey gives FDX members 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.

Appendix B: FDX Five Principles of Consumer Data Sharing

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."
   - 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.

- o 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.

- o 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.
- o 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.
- o 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.

Control
End users should be able to permission their financial data for services or applications.

Security
Entities should follow industry best cybersecurity practices for safety and privacy of data during access and transport and when that data is at rest.

Access
End users should have access to their data and the ability to determine which entities will have access to their data.

Traceability
All data transfers should be traceable. End users should have a complete view of all entities that are involved in the data-sharing flow.

Transparency
End users using financial services should know how, when, and for what purpose their data is used and only data that is required to provide such services should be shared with the organization providing the service.

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

- [TD Bank joins the Akoya Data Access Network to accelerate Open Finance](#) – Sept 13, 2021
- [Pentadata Announces Open Finance Integration with Akoya –](#) July 29, 2021
- [Wells Fargo joins the Akoya Data Access Network to advance API-based financial data aggregation](#) – June 22, 2021
- [Capital One and Plaid Announce New Data Sharing Agreement](#) – June 8, 2021
- [Jack Henry and Akoya Offer 4.8 Million Financial Institution Customers API-Based Access to Their Financial Data](#) - May 10, 2021
- [Jack Henry-Finicity partner to empower community financial institutions with open banking capabilities](#) - May 5, 2021
- [Akoya adds JPMorgan Chase to its Data Access Network –](#) February 17, 2021
- [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 Finicity](#) – August 7, 2020
- [TD enters into North American data-access agreement with Intuit](#) – September 2, 2020
- [Financial Institutions Can Empower Consumers to Securely Share Their Data with New Aggregation Solution from Fiserv](#) - September 3, 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
- [Envestnet | Yodlee and Charles Schwab Enter Financial Data Access Agreement](#) – April 16, 2020
- [Charles Schwab Reinforces Its Commitment to Customer Data Protection](#) – April 16, 2020
- [Wells Fargo Surpasses One Billion API Calls](#) – February 11, 2020
- [JPMorgan Chase, Envestnet l Yodlee Sign Agreement to Increase Customers' Control of Their Data](#) – December 5, 2019
- [Plaid Signs Data Agreement with JPMorgan Chase](#) – October 22, 2018