From:	Tom Carpenter <tcarpenter@financialdataexchange.org>
Sent:	Tuesday, October 19, 2021 2:19 PM
To:	Comments
Subject:	[EXTERNAL MESSAGE] FDIC RIN 3064-ZA26 - Financial Data Exchange Comments to Proposed Interagency Guidance on Managing Risks Associated with Third-Party Relationships
Attachments:	FDX Comments - Proposed Interagency Guidance on Managing Risks Associated with Third-Party Relationships.pdf

Comments from the Financial Data Exchange (FDX)

Tom Carpenter
Director, Public Affairs & Marketing
tcarpenter@financialdataexchange.org
202-577-3035

Financial Data Exchange Comments
Proposed Interagency Guidance on Managing Risks Associated with Third-Party Relationships
FDIC RIN 3064-ZA26 & Docket ID OCC-2021-0011

The Financial Data Exchange, LLC (FDX) is pleased to provide comments to the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, "the agencies") on the proposed interagency guidance on managing risks associated with third-party relationships.

FDX's comments are intended to address the guidance in general and to respond to two specific questions posed by the agencies. These comments are drawn from the insight and perspective FDX has gained as an industry standards body with diverse membership[1] across the financial services ecosystem. FDX specifically wishes to provide the agencies 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, FDX's comments are intended to inform the agencies about the progress and maturity of FDX since its launch less than 3 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.

---

[1] FDX Members

[2] 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 C.

[3] 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 C.

[4] 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 C.

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 196 data recipients like fintech companies, data providers like financial institutions, and data access platforms like 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).

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. Many of the largest financial services organizations in the US have begun implementing this standard in the last several years[5].

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 guidance 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.

Considering this, and in the context of the ever-changing roles and relationships between different financial services entities in the process of user-permissioned financial data sharing, FDX believes it is important to provide the agencies with a perspective on how the ecosystem works and answer two specific questions in the proposal:

- What other aspects of third-party relationships, if any, should the guidance consider?
- In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?

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

[5] Examples of some publicly announced data sharing agreements mentioning FDX API listed as Appendix D.

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, 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

FDX seeks to provide the agencies its general perspective on third party relationships within the user-permissioned data sharing marketplace and answer the following questions. FDX also seeks to contextualize its comments with background on FDX's structure and work.

1. **What other aspects of third-party relationships, if any, should the guidance consider?**

Roles:

FDX defines four key roles within user-permissioned data sharing, End Users, Data Providers, Data Access Platforms and Data Recipients (defined below and with full FDX Taxonomy definitions in Appendix C). And while each of these roles have traditionally been played by specific market actors, today's user-permissioned data ecosystem involves financial services firms often playing many of these roles, and sometimes simultaneously. With this in mind, FDX standards are focused on the role itself rather than the type of entity performing said role. In this, FDX encourages agencies to consider how a role-based approach could impact the way third-party guidance might apply to entities involved in consumer permissioned data sharing so that interagency guidance is able to maintain flexibility as the ecosystem continues to evolve and innovate.

- **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.

Balancing Data Access & Third Parties

FDX notes many variables in user-permissioned data sharing within the context of managing risks associated with third-party relationships.

First, 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. 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.

Secondly, FDX recognizes that financial institutions are required to maintain sound risk management strategies including addressing consumer protection, information security, and other operational risks. And that until this proposed interagency guidance, uniform and consistent principles on third-party risk management have been lacking.

Thirdly, consumer demand and the ecosystem's desire to serve customers adds further complexity to this balance. Consumers have come to expect and demand access to their own data to use, share and leverage to their financial benefit. And 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. Additionally, consumers expect to be provided with clear information about who has access to their data, what purpose it will be used for and for how long. Finally, consumers expect that their data will be transferred as needed in a secure manner.

Evolving Responsibilities

As stated earlier, consumer data access entities in the user-permissioned data sharing marketplace generally occupy roles as data providers, data access platforms and data recipients as directed by the end user. Traditionally, 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.

However, rapid innovation in just the last few years means that the entities who play these roles continue to evolve and often overlap. Further, some of these entities can occupy multiple roles at the same time.

- 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.

FDX can't comment on the specific regulatory aspects of business arrangements between financial institutions, data aggregators and fintech applications. However, in consideration of the ever-changing dynamics listed above and with an understanding of user-permissioned data sharing that is truly consumer-centric, FDX believes the agencies must consider user-permissioned data sharing uniquely from the more traditional way banking organizations utilize third parties for products, services, and activities. Specifically, FDX submits that third-party guidance must balance the need for 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, with the need for consumers to be able to access and share their own financial data with data recipients who may have no relationship with the data provider. In addition, agencies must ensure third-party guidance is flexible enough to adapt to market innovations and user demand.

2. **In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?**

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 API standards. In fact, common API standards like the FDX API offer superior security and end-user control. Further, market-led efforts bring together a vibrant and diverse ecosystem of financial services providers that gives the market varied perspectives that lead to a more robust understanding of consumer need and demand.

With this in mind, FDX encourages agencies to consider how third-party guidance might prioritize the adoption of APIs and reduce structural disincentives that might delay adoption and implementation of APIs. Specifically, and as a way to offer clarity to organizations working with standard-setting organizations, FDX believes agencies can and should do more to acknowledge that common and interoperable API standards and tokenized authentication make consumer-permissioned data sharing easier, more accurate, and more secure than credential-based access and screen scraping, including incorporating these benefits into third-party risk assessment standards to ensure that there are no inadvertent disincentives for financial institutions that wish to transition from credential-based access and screen scraping to APIs. For example, FDX found recent Federal Financial Institutions Examination Council (FFIEC) guidance on "Authentication and Access to Financial Institution Services and Systems"[6] lacking in the way it failed to differentiate between the security and risk profiles of credential-based screen scraping versus tokenized API-based data sharing. FDX thus encourages the agencies to illustrate this critical distinction in third-party guidance as a way to promote API adoption. FDX also encourages agencies to acknowledge and reference the role industry standards can play, as other agencies have,[7] and to consider roles standards might play in current and future evaluation of third-party relationships.

---

[6] https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf

[7] The U.S. Dept. of The Treasury's 2018 report entitled, "A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation" stated, ""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."

The Financial Stability Oversight Council's (FSOC) annual report in 2020 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)

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

On one hand, 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. Market entities want to maintain independence in technical standards work, but these entities also 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.

While FDX has not defined industry standards for business arrangement due diligence between data providers, data access providers and data recipients, future FDX certification of FDX API implementations and adherence to FDX standards and guidelines should be used in third-party evaluations in the future. Specifically, certified testing of the implementation of FDX's specifications, processes, and tools ensure that user-permissioned data sharing is secure, transparent, traceable and keeps the consumer in control. Additionally, regulatory acknowledgement of industry standards efforts could propel further industry standardization of different aspects of business arrangements in user-permissioned data sharing.

Considering this, FDX would like to submit three specific recommendations for the agencies to consider in third-party guidance:

1.) **Reference & Acknowledgement** - FDX encourages agencies to think about ways they can explicitly endorse or reference technical standards and certification organizations and the work they are doing. Specifically, FDX encourages agencies to evaluate Incorporation by Reference[8] as a possible tool to feature and include applicable industry-led standards work in third-party guidance. Such endorsements or references should also flow throughout the agencies - from the agency leads down to those tasked with regulatory oversight and enforcement within the agencies. Further, agencies should partner with standards and certification bodies to provide training materials on their standards so that agency officials are up to speed on the latest versions and certifications of a technical standard in the marketplace. Such deep understanding within agencies gives examiners who encounter an implementation of a certified industry standard the ability to understand how the standard works and what it means.

2.) **Engagement** – Agencies may want to consider ways to conduct regulatory engagement in areas where standards work may be beneficial. 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 alignment with industry standards can be extremely important. For example, and while FDX cannot comment on specific policy or regulations, if there is a particular domain that the agencies would like to see technical standards address, then FDX welcomes that input, and the industry and their technical teams can work together to meet those requirements.

---

understandable form and manner and with a date specifying the time period to which the information pertains." The industry specification METRO and later METRO2 was leveraged to accomplish this.

[8] https://www.federalregister.gov/reader-aids/office-of-the-federal-register-blog/2011/02/what-is-incorporation-by-reference

3.) **Harmonization** – FDX applauds the Fed, the OCC and the FDIC working together on this guidance and encourages further coordination with other regulators like the Consumer Financial Protection Bureau (CFPB) to harmonize and streamline requirements where possible so that industry standards are not caught between competing, overlapping or disjointed regulations.

Structure & Details of the Financial Data Exchange

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.

Below are a few of the notable FDX Committees Working Groups and Task Forces with the full list included as Appendix B.

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 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

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.) FDX API Specification: 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.) 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 document[9] 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.) Global Registry: 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 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.) Use Cases: 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 FDX use cases do not limit consumer data access. 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.) 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

[9] FDX Taxonomy of Permissioned Data Sharing v. 1.0 listed as Appendix C

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.) Annual Strategic Survey: 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.

Conclusion:

Third party relationships are inherent to user-permissioned financial sharing. And yet, it is clear that user permissioned data sharing adds significant complexity to the traditional understanding of third-party risk management. Specifically, (i) the advent of financial services entities often playing more than one of the four key roles within the user-permissioned data sharing ecosystem (End Users, Data Providers, Data Access Platforms and Data Recipients), (ii) the requirements on financial institutions to maintain sound risk management strategies, and (iii) the increasing consumer demand to access, share and leverage their own data for their financial benefit, all combine to challenge the current manner that banking organizations utilize third parties for products, services, and activities. FDX thus encourages agencies to consider how a role-based approach could impact the way third-party guidance might apply to entities involved in consumer permissioned data sharing so that interagency guidance is able to maintain flexibility as the ecosystem continues to evolve and innovate.

FDX also encourages agencies to consider how third-party guidance might prioritize the adoption of APIs and reduce structural disincentives that could delay adoption and implementation of APIs for user-permissioned data sharing. Specifically, FDX suggests an increased agency acknowledgement and reference of the role industry standards might play in current and future evaluation of third-party relationships as well as examining other areas where engagement and harmonization can better align the regulatory view of third-party relationships in financial services with innovations that are taking place in the market.

FDX is encouraged by the coordination of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) on this interagency guidance and looks forward to engaging with the agencies on these matters in the future.

Appendices

A. **FDX Five Principles of Consumer Data Sharing**
B. **FDX Committees, Working Groups & Task Forces**
C. **FDX Taxonomy of Permissioned Data Sharing 1.1**
D. **Publicly Announced Data Sharing Agreements Mentioning FDX API**

Appendix A: 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.
    - 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.

Appendix B: FDX Committees, Working Groups & 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.

Appendix C: FDX Taxonomy of Permissioned Data v. 1.1

Published May 2021

Legal Notice:

Financial Data Exchange, LLC (FDX) 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 interpretations 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, LLC (FDX) is a technical standards body composed of financial institutions, financial technology companies, data access platforms (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 and 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 U.S. Department of Treasury, U.S. 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 interpretations 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 Permissioned Data Sharing from time to time and change the version and date specified above with each new revision.

Taxonomy of Permissioned Data Sharing

Consumers: are end users acting in their personal capacity.

End Users: includes 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 or authorize transactions with Data Recipients.

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), 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[5] or Data Harvesters.

End User 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 User's 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.[2,3,4]

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.

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.

Consent: The permission granted by an End User to a Data Provider to share the End User's data to a Data Recipient. Consent is held by the Data Recipient to access/store/use data to provide services to the End User.

Grant Consent: The act of establishing permission by an End User to a Data Provider to share the End User's data to Data Recipient.

Consent Duration: The agreed upon time frame for the length of Consent, such as time-based, persistent, or one-time. Refer to the User Experience Guidelines document for the current definition of each duration.

Authorized Accounts: Accounts held at the Data Provider to which an End User grants access under the Consent.

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

Consent Dashboard: a digital experience that enables the End User to view the status of or take action on the Consents they've granted and the parties or processes accessing data.

Consent Status: The current state of the Consent as either Active, Revoked, or Expired.

View Consent: The ability to or action by an End User to review Consent that they have granted.

Manage Consent: The ability to or action by an End User to update or make changes to Consent that they have granted.

Active Consent: Granted Consent that is not expired or revoked. This is the only state in which data can be shared or actions can be taken on behalf of the End User.

Revoked Consent: An inactive state caused by the explicit removal of Consent before expiration. Once revoked, the Data Provider shall no longer share any data with the specified Data Recipient.

Expired Consent: An inactive state caused by the occurrence of a time limit and was not renewed. Once expired, the Data Provider shall no longer share any data with the specified Data Recipient.

Data Cluster: A group of data elements that communicate to an End User the scope of data to be shared under a consent.

Consent Scope: The specification that defines what data is requested, between whom, its purpose, and duration for a specific consent granted by an End User.

Application: The software product or service provided by a data recipient that is used by the End User.

Consent API: The application programming interface that transmits Consent Scope data.

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[5].

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.

Sources

[1] Government Accountability Office, Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace (GAO-13-663) (Dec. 18, 2013) (full-text).

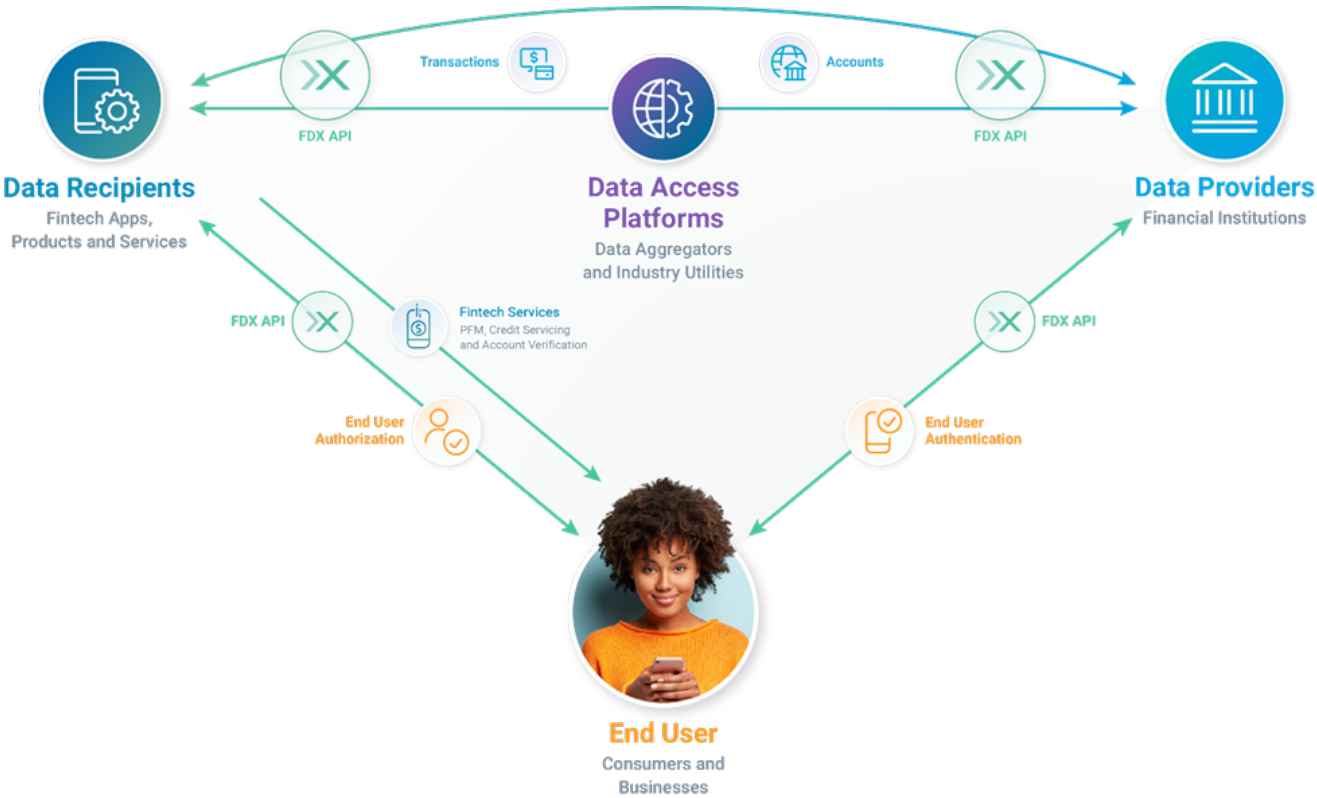
[2] https://www.techopedia.com/definition/16597/screen-scraping

[3] https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712

[4] https://en.wikipedia.org/wiki/Web_scraping

[5] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1202

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



Money Movement Taxonomy

Money Movement: The process to execute a digital payment or transfer. This may include forms of digital execution such as digital or crypto currencies, but does not include paper-based and coin-based methods such as paper checks and physical currencies.

Payment Service Provider (PSP)/Payment Processor: financial institution or entity that connects to payment networks (e.g., ACH, Visa, MasterCard, SWIFT) for the End User to move money via payment initiators.

- **PSP APIs** expose payment services to an End User Application (**payment initiator**) by a payments services provider (e.g., a bank) that provide:
    - Capabilities to a payment user to setup and initiate payments\
    - Capabilities to a business payee to collect credit, debit, or account / routing numbers, such that the payment is then initiated as debit by the merchant to the payer's account. These are called **Merchant Services**.

- **Payment Network Access APIs** expose access to payment rails to payment service providers. These are not subject to the same tokenized access needs as the PSP APIs. Only authorized, regulated providers are able to access such APIs.

Payment Access Platforms: Intermediaries that facilitate payment initiation services on behalf of payment initiators.

Payment Initiator: Service companies, Applications (financial apps), financial institutions, products and services where End Users (on their own or through their End User Delegates) facilitate sending payment instructions to a Payment Service Provider (PSP).

Payment Initiation: A process by which a Payment Initiator sends payment instructions to a Payment Service Provider.

Bill Payment: The process for paying a bill electronically.

Biller: Entity that requests payment owed by the end-user for a product or service.

Payee: The End User who is the financial beneficiary of a payment.

Payer: The End User who is the financial source of a payment.

Payment network: The industry legal and technology infrastructure that facilitates the execution of payment instructions and settlement among Payment Service Providers.

Payment: An instrument for transferring money between a payer and payee.

Immediate Payment: A Payment that cannot be cancelled. Funds are expected to be executed as soon as possible by the involved parties (Payer, Payee, and Payment network).

Scheduled Payment: A future dated Payment.

Recurring Payment: A series of regularly occurring Payments.

Transfer: The movement of funds from one account to another account owned by the same entity.

Internal Transfer: A Transfer of funds between accounts owned by the same legal entity at a single financial institution.

External Transfer: A Transfer of funds between accounts owned by the same legal entity held at different financial institutions.

Scheduled Transfer: A future dated Transfer.

Recurring Transfer: A series of regularly occurring Transfers.

Merchant: A specific type of a payee, typically a business from which goods or services are rendered.

Payment/Transfer Status: The current state of a transaction provided by the Payment Service Provider, such as the success or failure of the Payment/Transfer request.

FDX Certification Taxonomy

Application Form: A set of documentation (questionnaire/survey) provided by the Certification Applicant when applying for FDX Certification.

Certification: Conformance with an FDX-defined Use Case.

Certification Applicants: Any Data Provider, Data Recipient, or Data Access Platform who wish to be certified against the requested qualification criteria.

Certification Case: A test case that is only applicable to Certification.

Certified Entity: A Data Provider, Data Recipient, or Data Access Platform that has received FDX Certification.

Certifying Entity or Certifier: An entity, or person(s) who qualify the applicant and certify against stated requirements. FDX is the ultimate certifying entity although it may rely on self-qualification or industry-accepted qualification tests.

Certification Expiry: An organization's Certification may expire if it does not re-certify for conditions that require re-certification, such as an elapsed time period, implementation update, or FDX specification update.

Certification Model: The methodology for attestation to conformance with FDX-defined Use Cases and related technical standards, including the application Certification process and post-certification monitoring.

Certification Tool: A utility that performs the necessary validations to score/assess the Certification Applicant against Certification criteria.

Certification Test Suite: A collection of tests used to validate a Certification Applicant's server implementation.

Conformance Monitoring: Post certification monitoring of a Certified Entity to confirm that software deployed in production meets agreed conformance standards for FDX certification.

Common Call Compliance: Required FDX endpoint functionality to achieve Certification for all Data Providers, regardless of the Use Case(s) to be validated.

Data Samples: Depersonalized "real" or synthetic JSON responses that are representative of a particular data set.

FDX Certification "Badge": Iconography that may be used to advertise FDX Certification.

FDX Certification: FDX-awarded certification that can be displayed by the Certified Entity (e.g., "Certified" for Financial Data read-only).

FDX Registry: A directory of ecosystem participants, members and non-members, with their organization information, application information, FDX technical conformance status, and reference to certain other registrations or certifications they may have.

Data Provider Products: Data Provider accounts offered to their clients. These may have a specific Data Provider marketing brand (e.g., "Premier", "Platinum") moniker used directly with their customers and easily recognizable under their own secure online portals.

Provider Implementation Data List: A list of FDX API entities and elements supported by the Data Provider.

Reference Implementation Server: An example implementation of all FDX Data Provider endpoints.

Use Case: The minimum data set required to fulfill a business purpose as defined by FDX.

Use Case Certification: Compliance with a data set as required by the applied Use Case(s), as well as operational and security requirements for the same.

Use Case Data List: A list of FDX API entities and elements deemed as required to meet an FDX-defined Use Case.

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.

Entity	End User	Data Recipient	Data Access Platform	Data Provider	Financial Account Information
CFPB	Consumer	Data User	Data User/ Data Aggregators	Data Holder	Consumer Financial 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.

Appendix 1: Consumer Financial Protection Bureau Definitions

Source: October 22, 2020, publication *Consumer Financial Protection Bureau Dodd-Frank* Section 10-33 Advanced Notice of Proposed Rulemaking (ANPR)

https://files.consumerfinance.gov/f/documents/cfpb_section-1033-dodd-frank_advance-notice-proposed-rulemaking_2020-10.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 data** (**consumer data**): "information in the control or possession of [a] covered person concerning a consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account, including costs, charges and usage data."
- **Consumer data access**: authorized data access and direct access.
- **Authorized data**: data initially sourced from a data holder as a result of authorized data access.
- **Authorized data access** (**consumer-authorized data access**): third-party access to consumer financial data pursuant to the relevant consumer's authorization.
- **Authorized entities**: entities or persons with authorized data access to particular consumer financial data.
- **Data aggregator** (**aggregator**): means an entity that supports data users and/or data holders in enabling authorized data access.
- **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).
- **Data holder**: a covered person with control or possession of consumer financial data.
- **Data user**: a third party that uses consumer-authorized data access to provide either (1) products or services to the authorizing consumer or (2) services used by entities that provide products or services to the authorizing consumer.
- **Direct access**: direct access by the individual consumer to consumer data rather than by an authorized entity.

Appendix 2: US Treasury Definitions

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

https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi..... 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 acquir[ing] 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.

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) '**consume**r' 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 personalised security credentials;

(30) '**strong customer authentication'** means an authentication based on the use of two or more elements categorised 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) '**personalised security credentials'** means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;

(32) '**sensitive payment data'** means data, including personalised 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;

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 D: 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