FINANCIAL™ DATA EXCHANGE

Taxonomy of Permissioned Data Sharing

Version 1.4
December 2022

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.

Revision History

Document Version	Notes	Date
1.0	Initial Document Release This document was created as a result of FDX RFC 0016 and incorporates the full contents of the RFC for public release.	**December 2020**
1.1	This version was created as a result of FDX RFC 0065 and incorporates the full contents of the RFC for public release.	**May 2021**
1.2	This version was created as a result of FDX RFC 0162 and incorporates the full contents of the RFC for public release.	**October 2021**
1.3	This version was created as a result of FDX RFC 0200 and incorporates the full contents of the RFC for public release.	**May 2022**
1.4	This version was created as a result of FDX RFC 0241 and incorporates the full contents of the RFC for public release.	**December 2022**

Contents

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.

Credentials: any data used to identify the End User to the Data Provider, such as a username and password pair, to gain access to the End User's Financial Account Information.

Unique Customer Record (aka **Consumer Account)**: One Credential per direct connection to a Data Provider from a Data Access Platform or a directly-connected Data Recipient.

Financial Account Information: the financial accounts, statuses, histories, statements, 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.

Government ID Number: Any government-issued unique identifying number for a person or other recognized entity, such as a Social Security Number (SSN), Social Insurance Number (SIN), Employer Identification Number (EIN) or Tax ID Number (TIN).

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 User gives permission to a Data Provider 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 or via Data Access Platforms to share their Financial Account Information with the Data Recipients. In addition to consent management and 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.

Business Purpose: The service being provided by the data recipient for which data access is needed.

Consent: The permission granted by an End User to share their data from a Data Provider to a Data Recipient. Consent may be held by the Data Provider, Data Access Platform, or the Data Recipient as defined by the bilateral agreement(s) for the entities involved.

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

End User Notification: Any communication to an end user, such as email or text, that a data sharing event has occurred.

Event Notification: The notification of a specific event generated by one entity to inform another.

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

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].

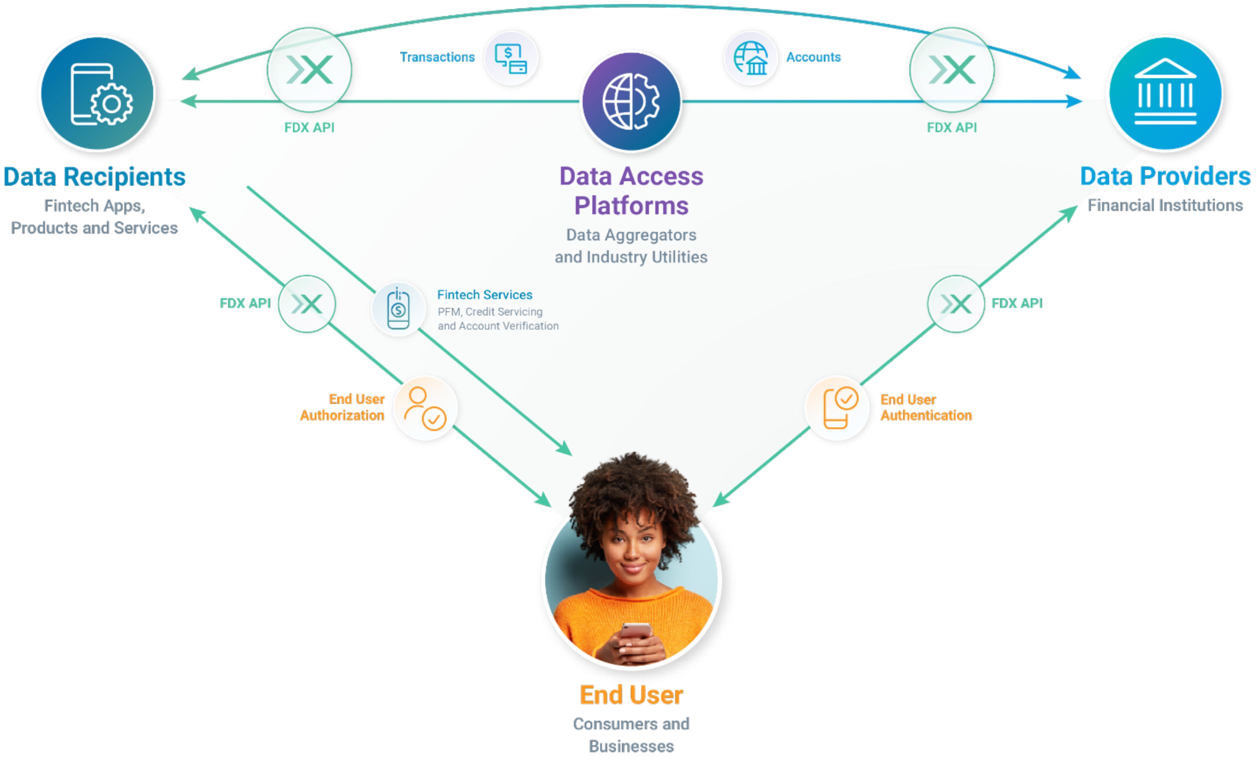
Data Harvesters: use communication and information services, including applications (apps), to collect data from End Users and provide the data or derived digital products to third parties.

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:



Consent and User Experience Taxonomy

Consent Issuer: The entity that generates a Consent when granted by the End User. The Consent Issuer may also respond to requests to provide Consent details.

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

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.

Authorized Accounts: Accounts held at the Data Provider to which an End User permits access under the Consent. (Accounts, and other resources, are declared scopes.)

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. (Duration is a declared scope.)

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

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.

Consent Revocation: An action to revoke consent that can occur at a Data Provider, Data Recipient, or Data Access Platform via a Consent Dashboard or another experience. Can be initiated by the end user or by an involved party.

Consent Dashboard: A digital experience that enables the End User to view, edit, or revoke the Consents they've granted and the parties or processes accessing data.

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.