Financial Data Exchange Response to Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights Consumer Financial Protection Bureau (CFPB)

Financial Data Exchange, LLC (FDX) is pleased to provide this response to the Consumer Financial Protection Bureau (CFPB) proposals and questions in its October 27, 2022, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights (the "Materials").

Part III D.2. ii. of the Materials reference the CFPB's view that industry-led standards (such as FDX) are "a positive development" and the questions thereunder seek input on how the "CFPB can promote the development of industry standards."[1] As the leading technical standards body in the industry for sharing permissioned financial data, rather than respond to the questions specifically, FDX believes it is important to take this opportunity to demonstrate that the voluntary development of industry led standards (specifically by FDX) has been more successful than any government imposed standards and that the development of a new, government mandated standard is not necessary. Through the development, adoption, and constant improvement of the FDX API (defined hereafter), FDX and its members have made significant progress transitioning from credential "screen scraping" to the FDX API, with over 42 million consumer accounts using the FDX API as of Fall 2022.[2]

FDX's response is intended to inform the CFPB about the progress, maturity, and overall benefits of neutral industry-led technical standards to enable end-users[3] to access, share, and use their own financial data.[4] Specifically, FDX seeks to highlight the success of industry-led standards to date and the breadth of participation among all market entities in this work. FDX also strives to convey a detailed view of FDX's mission, structure, and vision as an example of how competing entities across the spectrum of financial services can join together toward a common goal to implement common, interoperable, and royalty-free technical standards that maintain innovation in the marketplace while elevating user control and experience. Finally, FDX wishes to submit that an industry-led approach is best suited to develop, implement, promote, and certify technical standards for user-permissioned data sharing in the United States.

---

[1] Consumer Financial Protection Bureau (2022, Oct. 27). *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights*: *Outline of Proposals and Alternatives under Consideration* p.32.
[2] Almost all of FDX Financial Institution (FI) members are using or plan to use FDX API; more than 42 million consumer accounts are on FDX API as of Fall 2022; and the FDX API averaged 99.91% availability with more than 3.5 billion API calls per month.
[3] Financial Data Exchange (2020). *FDX Taxonomy of Permissioned Data Sharing v. 1.4*. End Users: include consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data. Consumers: end users acting in their personal capacity. See Appendix A for complete taxonomy.
[4] Financial Data Exchange (2022, Dec.). *Experience Guidelines v. 2.2.* See Appendix B made available to the industry for guidance on the implementation of an end user's consent journey consistent with the FDX API.

About FDX

FDX has achieved significant growth and marketplace adoption since its launch just over four years ago. FDX's diverse membership[5] has grown across every sector of the user-permissioned financial data ecosystem. FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to unifying the financial services industry around a common, interoperable, royalty-free standard for the secure and convenient access of user-permissioned financial data, aptly named the FDX Application Programming Interface (FDX API). The FDX API is continuously improving and adding features with scheduled updates in the Spring and Fall of each year (FDX API 5.2 is the current version as of the Fall 2022 Release). Updates are based on member prioritization surveys, planned certification goals, member requests for improvements and to ensure the FDX API can assist regulated parties comply with changes to rules and regulations. FDX is currently comprised of ~230 financial data providers (i.e., "Data Holder"[6] or financial institutions),[7], data recipients (i.e., "Data User"[8] or third-party financial technology companies or fintechs),[9] data access platforms (i.e., data aggregators[10] and ecosystem utilities),[11] consumer groups, nonprofit entities, financial services industry groups and other permissioned parties in the user-permissioned financial data ecosystem. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

FDX exists primarily to promote, enhance, and seek broad adoption of the FDX API technical standard, 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, credential-based screen scraping will eventually cease, and the flow of user-permissioned data between banks, aggregators, fintech applications, payments, and online lending, for example, will be more secure and reliable. This standard has been under the stewardship of the FS-ISAC with adoption across many of the largest financial services organizations in the US over the last several years[12].

---

[5] FDX Members

[6] Reference to definition of "Data Holder" from CFPB Consumer Access to Financial Records Advance Notice of Proposed Rulemaking dated November 6, 2020 (the "2020 ANPR").

[7] From *FDX Taxonomy of Permissioned Data Sharing v. 1.4*: Data Providers: the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages. Full Taxonomy in Appendix A.

[8] Reference to definition of "Data User" from CFPB Consumer Access to Financial Records 2020 ANPR.

[9] From *FDX Taxonomy of Permissioned Data Sharing v. 1.4*: 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 A.

[10] Reference to definition of "Data Aggregator" from CFPB Consumer Access to Financial Records 2020 ANPR.

[11] From *FDX Taxonomy of Permissioned Data Sharing v. 1.4*: 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 A.

[12] Examples of some publicly announced data sharing agreements mentioning FDX API (see Appendix C) and known development portals (see Appendix D) demonstrate the depth with which the U.S. financial services industry is embracing the FDX API and working with each other to grow adoption.

Scope of FDX Comments

FDX is a neutral industry-led technical standards body and does not take positions on legislative and regulatory policy issues other than promoting an industry developed technical standard over a government mandated technical standard. Consequently, FDX is solely commenting on topics in the Materials that are neutral in impact to different FDX membership groups. Additionally, FDX is not addressing questions relating to the financial, cost and time impacts specific regulatory implications would have – these questions are better answered by our members and other small business entities. FDX's only comment on cost impacts that any regulations may have is to emphasize that the FDX API is made available free of charge for members and non-members of FDX which will help minimize the cost of compliance that any new regulations may entail. While any technical implementation will incur costs to market participants, the more parties that are required to adopt APIs (such as the FDX API), the lower the total cost would become as more competitors enter the marketplace, competing to implement competitive APIs with the numerous financial market participants.

As a result, FDX's response is more informative in nature in support of the CFPB's view that industry-led standards are "a positive development"[13] and to emphasize the benefits of an industry led standard over a government mandated standard. While FDX itself is not a targeted small business for the detailed input sought by the CFPB in its SBREFA impact analysis, a substantial portion of FDX's membership includes small entities as defined by the CFPB (which include data providers, designated third parties, etc.). The FDX API is a free standard that was created to reduce costs, promote interoperability, increase security and simplify the sharing of user-permissioned data for all sizes of businesses (which can be even more beneficial for small, start-up business by lowering compliance costs and the barriers to entry).

FDX is also responding to ensure that regulators, legislators, and policymakers are fully aware of the work FDX is doing, how 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 an industry-led standards body, FDX also advocates for technical specifications and standards to be designed and implemented by the financial services industry for user-permissioned data sharing as opposed to regulatory or government mandated technical standards.

Overall, and considering the potential shift of the regulatory landscape around user-permissioned data sharing, FDX believes it is important to provide the CFPB with a clear view of how FDX works and the progress it has made to develop and drive adoption of neutral industry-led technical standards for consumer data sharing. FDX also believes that industry-led efforts to develop and promote technical standards for financial services are as important as ever because they are able to keep pace with rapid marketplace innovations and emerging security threats in a way that regulatory or government mandated approaches often cannot.

FDX is now in the process of implementing a certification standard for organizations to certify that, from a technical point of view, such organizations can meet the requirements set forth in the specified FDX API certification classifications. FDX certification relates to the certification of technical standards which intend to compliment, and in no way conflicts with, the CFPB, OCC, FDIC, Federal Reserve, and other government bodies' role in overseeing FDX accredited companies for compliance with applicable law and regulation.

[13] Small Business Advisory Review Panel For Required Rulemaking On Personal Financial Data Rights, October 27, 2022, p.32.

Historical Snapshot of Standardization of User-Permissioned Data Sharing

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

To utilize these third-party services, end 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. Furthermore, in the hands or bad actors, access to an end user's credentials can facilitate fraudulent activities.

Fortunately, market adoption of a more efficient and secure method of data sharing began a few years ago and should eventually replace credential-based screen scraping in most scenarios. Specifically, tokenized access, in concert with API-based data collection, allows consumers to provide authorization to share only the data needed for a given product or service to their own financial institution, a data access platform or a data recipient. 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 consumers to have more 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 along with standardization of authentication, authorization, certification, user experience and consent guidelines, capabilities across financial institutions, financial data access providers and fintech applications and services will remain fragmented – using incompatible APIs, processes and definitions of how a user is able to permission use of their financial data.

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

For the avoidance of doubt, FDX was formed to unify the financial services industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data with *consumer permissioned* financial data access. FDX does not address access to personal financial information that is obtained without the consent of the end uses (such as "data brokers" and

"data harvesters"). Any such "non-permissioned" access is deemed "out of scope" and not considered by FDX or addressed in the FDX API.

* * * * *

FDX Informational Response

FDX's comments are guided by the following core tenets:

- FDX submits that a non-profit, industry-led technical standards body is best positioned to unify the financial services industry around common, interoperable, royalty-free technical standards for user-permissioned data sharing and that the development of any new, government mandated standard is not necessary. Importantly, FDX's ~230 members are diverse in size and type and includes members from all sectors of the user-permissioned financial data ecosystem.
- FDX technical standards can be tailored to accommodate regulatory requirements. FDX is neutral on the "what" of regulatory policy in this area and rather seeks to implement technical standards to accomplish the "how" of user-permissioned data sharing in a way that is responsive to ongoing market needs as well as any shifts in legal and regulatory compliance requirements.
- FDX desires to use this opportunity to demonstrate some of the successes and achievements since its launch just over four years ago, as well as to describe FDX's continued growth goals and commitment to meet the needs of the financial services industry and its customers.

FDX believes accessible, user-permissioned financial data sharing inherently gives consumers control of their data. This consumer-centric approach empowers end users to better understand, leverage, and benefit from their own financial data and improve their financial lives. It further 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 all participants in the user-permissioned data sharing ecosystem serve the needs of consumers.[14] These are:

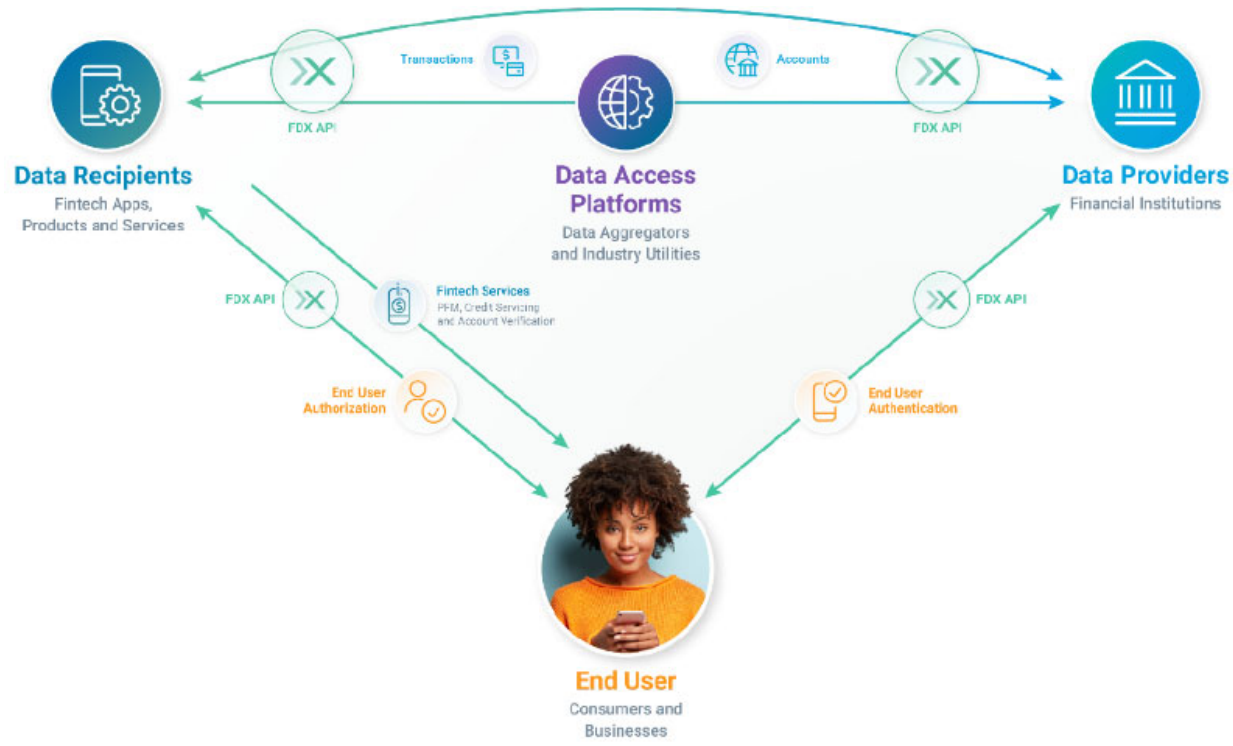
1.) **Control** - Consumers should be able to permission their financial data for services or applications.
    - All entities within the user-permissioned financial data ecosystem should provide clear, intuitive navigation and information to consumers, allowing informed decision making when sharing 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.

[14] Derived from Consumer Financial Protection Bureau (2017, Oct .18). Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation . These FDX core principles are intended to cover all nine listed by the CFPB through a broader reading of the FDX five core principles.

    - 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 cybersecurity best practices across the whole of their organization for safety and privacy of data during access, in transit and at rest.
    - All entities within the user-permissioned financial data ecosystem need to provide clear definitions on data usage and privacy, permitting consumers to make educated decisions.
    - All entities involved in the data-sharing ecosystem must have appropriate security policies and practices in place. These practices should reflect best-in-class standards and be improved upon continuously.
    - Security should empower consumer control, access, transparency, and traceability and should not be implemented in a manner that introduces friction points or other features that contravene these principles.

Based on these five Core Principles, FDX also submits the following:

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



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. FDX believes that innovation in financial services is being enhanced via common, interoperable, royalty-free, and industry-led technical standards. Such industry-led standardization provides foundational requirements for entities seeking to serve the market for user-permissioned data sharing, whether via direct or authorized data access. A non-profit industry standards body like FDX also brings together a vibrant, and diverse ecosystem of financial services providers whose distinct perspectives lead to more robust understanding of consumer need and demand.

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

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

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

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

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

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

Structure & Details of US Industry-led Technical Standards Body

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

FDX believes the following important organization details about FDX can inform CFPB's deliberations on the Materials; in particular, how to work with existing industry-led standards bodies:

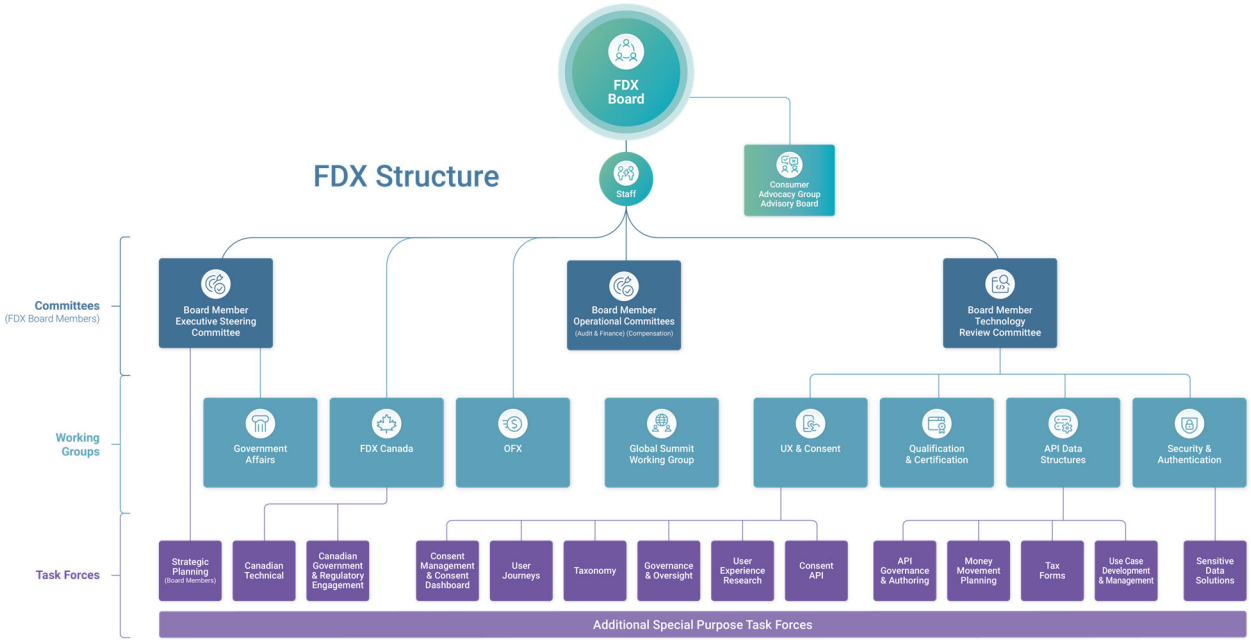
- FDX is currently comprised of ~230 financial data providers (i.e., financial institutions), data recipients (i.e., third-party financial technology companies or fintechs), data access platforms (i.e., data aggregators and ecosystem utilities), consumer groups, financial services industry groups, academics, and other permissioned parties in the user-permissioned financial data ecosystem. More than half of FDX members are fintechs and non-banks.
- FDX technical standards can be tailored to accommodate any regulatory or legal requirements in a given jurisdiction. FDX is neutral on policy and seeks to implement technical standards to accomplish the "means and methods" of user-permissioned data sharing in a way that is responsive to market needs as well as any legal or regulatory compliance requirements. FDX will

ensure its standards meet any principles or requirements that the CFPB may place on user-permissioned data access.

- Since the most recent FDX member survey on adoption and implementation of the FDX API, over 42 million US consumer accounts have been transitioned from screen scraping to a version of the FDX API. FDX estimates that data access and sharing for between 35-55 million US consumer accounts is still provided through credential-based screen scraping. This shift toward the use of the FDX API standard is beneficial to consumers and industry participants for many reasons, including the following:
  - Open finance APIs provide a more secure and reliable way to connect and verify financial data, removing the need for consumers to share their login IDs and passwords by using token-based technology so credentials are never shared.[15]
  - Since most cybercrime is not the result of sophisticated man-in-the-middle attacks but instead result from fraudulent access to credentials, APIs and OAuth connections are more secure by removing credentials from the equation.
  - Having API standards ensures there is interoperability between industry players - bringing parity to data sharing and a common interest to streamline, modernize and secure data driven experiences.
- FDX's organizational structure includes a balanced board of financial institutions (FIs), financial services industry groups and non-financial institutions (Non-FIs)/fintechs as well as an observer-level board seat for consumer advocacy groups.
- Every FDX member organization, regardless of size, type, or dues, has a single and equal vote in Working Groups and Task Forces where most of the FDX work is accomplished (i.e., one member, one vote, leave your market cap at the door). In this, FDX abides by the mantra of "Best idea wins," irrespective of firm size or type. The FDX board voting structure is also balanced by giving different market segments equal voting representation and requiring a super-majority (two-thirds) of board members across industry sectors to agree on major decisions.
- The FDX API specification itself is free for any organization to download and use and membership starts with a no-cost tier for non-profit consumer advocacy groups and an affordable and revenue-based structure for all other entities.
- FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

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

[15] The U.S. Dept. of The Treasury, in its 20118 "A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation, stated "…there was universal agreement among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice. APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping."



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 and 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 services 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 are able to 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. See Appendix B.
7.) Qualification & Certification: developing certification program, definitions, and procedures to certify organizations as compliant with FDX API technical certification requirements.
8.) Communications: Marketing, Public Relations Working Group and Government Affairs Working Group: 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.
9.) Open Financial Exchange: OFX joined FDX in 2019 as an independent working group tasked with maintaining and evolving the OFX standard as necessary to support the existing OFX

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

FDX Deliverables to the Marketplace

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

1.) **FDX API Specification**: Currently at version 5.2, the FDX API is the foundation of FDX data sharing standardization and offers consumers the ability to access over 660 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 and Consent Guidelines**: As adoption and implementation of the FDX API expands, these guidelines are the product of years of FDX and its members work, including significant consumer testing, and are intended to accelerate design decision-making during implementation of data sharing experiences. The User Experience and 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. Forthcoming FDX certification will incorporate adherence to User Experience requirements and the guidelines will be tailored to each FDX defined use case. See Appendix B.

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[16] 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. See Appendix A.

4.) **Use Cases**: Use cases are consumer-permissioned scenarios that help users minimize and limit the scope of data they share by defining the minimum data elements that are needed for a given product or service as reasonably understood by the authorizing consumer. FDX use cases do not limit data access. Rather, FDX enables the financial services ecosystem to identify appropriately minimized and certifiable data sets needed to power an application and then utilize an industry-

[16] FDX Taxonomy of Permissioned Data Sharing v. 1.4 listed as Appendix A

led standard like the FDX API to deploy and increase adoption of these use cases. In addition, FDX use cases offer the user-permissioned financial data ecosystem a pathway to quickly define and implement new or innovative use cases with the entire financial services industry in a way that lowers barriers for new products and services. To date, FDX has approved use cases for the following services:

a. Credit Management and Servicing
b. Personal Financial Management
c. Account Owner Verification Certification
d. Account Linking for Payments Certification (a.k.a Money Movement)

and expects to define and certify additional Uses Cases in the future.

5.) **Global Registry**: FDX is creating a registry of known entities, their capabilities and certification status with respect to each entity's specific FDX API instance. A central registry is a useful ecosystem tool and is needed to help the user-permissioned financial data marketplace discover and clearly identify market participants, the status of their FDX capabilities and other characteristics (e.g., contact information, products, identifiers, FDX membership status and technical information). The registry will serve as a definitive reference on what entities are FDX-certified and provide details about the certification. The consolidation of this information into an easily searchable registry provides efficiency and transparency for the market. Registrants will be able to view each entity's information, offerings and capabilities, and the FDX certification status. Certification accelerates the adoption of standards and serves to align the ecosystem players to each other. Common identification is crucial to support data traceability and forensics needed in support of issue or dispute resolution. FDX intends the Global Registry to act as a non-profit, non-commercial, technology agnostic, multi-tenant, cross-sector, international resource.[17]

6.) **Developing a Certification Program**: Creating a standard alone cannot drive adoption or guarantee adherence. 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. Initial certification programs will develop, test and certify organizations' technical adherence as FDX API certified Data Providers, Data Recipients, and Data Access Platforms. FDX certification relates to the certification of technical standards which compliments, and does not conflict with, the CFPB, OCC, FDIC, Federal Reserve, and other government bodies' role in overseeing FDX accredited companies for their compliance with applicable law and regulation.

Remaining Barriers to Adoption. Despite the many benefits of the FDX API solution, barriers to more ubiquitous adoption remain. These include:

1) Challenges Faced by Small Institutions
2) Reliance on third party service providers for technological implementation
3) Costs of building and maintaining APIs

FDX will discuss each of these barriers in turn and will suggest potential ways in which these barriers can be overcome. To some extent, the CFPB can mitigate these factors by careful drafting of its proposed rule, but the agency must be mindful that it does not create new problems in the process of doing so. FDX is already working hard to overcome these barriers to entry by reaching out to data access providers of all sizes, working with the third party service providers to smaller industry participants to encourage the adoption of the FDX API as on offering to their clients and providing the FDX API as an alternative to

[17] The FDX registry in progress can be viewed at: https://registry.financialdataexchange.org/.

screen scraping (which becomes easier to adopt the more it is accepted and utilized by industry participants).

1) **Challenges Faced by Small Institutions**
   Perceived costs, staffing constraints, and compliance concerns present challenges for small data providers in particular. Switching to APIs involves technology changes, contract negotiations, training, and other costs that may be difficult for a small institution to prioritize. Regulatory clarity will provide new incentives for all market participants to act. Additionally, this barrier to API adoption can be addressed by education and lowered costs over time. FDX and industry trade associations educate data providers about the availability of the resources FDX offers. As the number of users of APIs increases, the cost of adoption will likely decline. Any support for education of the financial services industry as part of the CFPB's broader efforts to implement Section 1033 will also be valuable.
2) **Reliance on third party service providers for technological implementation**
   Even after the data providers become aware of the efficacy of APIs to mitigate their risk, they may be unable to implement them from a technological standpoint. This is because many smaller entities outsource the building and maintaining of their own architecture and rely on third-party service providers to do so. These third party service providers must manage a wide array of considerations, such as instituting a variety of system updates to remain compliant with changing laws and regulations. Due to the need to prioritize resources, these third party service providers may not have been in a position to develop an API framework for all their clients when it is not, strictly speaking, required. The number of third party service providers serving this smaller entity market has grown in recent years, no longer provided only by a handful of large companies. With additional tools (such as the FDX API) and additional third party service providers, this barrier to entry will continue to be lowered over time. Having the FDX API free to the market can only aid in broad market adoption of APIs and moving away from screen scraping.
3) **Costs of building and maintaining APIs**
   Even if a data provider utilizes a third-party service provider, they would need to go through some sort of procurement process and establish a program to specify the technical requirements, conduct testing, and accept the program. If the data provider does not leverage a service provider, they must build an API using their own resources or find and work with another service provider. After the initial development, there is the secondary consideration of whether maintenance is performed by the data provider or outsourced. The CFPB could support smaller data providers by working with their third party service providers and other industry participants on an appropriate timeframe to transition to APIs, publishing educational materials or statements on the merits of APIs, and collaborating with prudential regulators to try to ease compliance concerns.

While the FDX standards are free and available, it still requires institutional will, personnel, and resources to make the transition from screen scraping to APIs. While this is an investment well worth making, business leaders may have different priorities. Until such time that screen scraping becomes treated as a risk item for examiners, the upfront and ongoing costs associated with APIs may have a chilling effect on adoption. Working with service providers and other industry participants on an appropriate timeframe to transition to APIs coupled with an educational push on the merits of APIs may help to overcome this barrier. Having the FDX API free to the market can only aid in broad market adoption of APIs and moving away from screen scraping.

Thus, while barriers to adoption exist in the status quo, the CFPB support adoption by:

1) Setting clear mandate for API adoption;

2) Ensuring third-party providers are able to help data providers meet requirements; and
3) Working with third-party providers and other industry participants on an appropriate timeframe to transition to APIs.

FDX is actively working hard to overcome these barriers to entry by engaging data providers of all sizes, working with the ecosystem to encourage the adoption of the FDX API as on offering to their clients and providing the FDX API as an alternative to screen scraping

Lessons Learned – Examining Other Jurisdictions

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

The UK, EU, Australia, Mexico, and Brazil, among others, are pursuing regulatory approaches to technical standards for user-permissioned financial data sharing and data access. Such a regulatory-driven approach is common and easier to implement in these jurisdictions because these markets tend to have a single financial regulator and a concentrated banking market (i.e., nine major banks in the UK, four in Australia, four in Mexico). The resulting technical standards often apply to a significant portion of the market all at once.

However, without an ecosystem approach that considers the needs of a large and complex market, and its diverse participants (especially important in the US with over 14,000 financial institutions), such technical standards can be ill-fitting to smaller market participants. In addition, regulatory-driven standards in these jurisdictions have required significant technical resources and have incurred substantial start up and opportunity costs. Finally, and most importantly, regulatory standards in these jurisdictions have become more akin to regulatory compliance – meeting regulatory minimums – rather than standards that seek to address the full breadth of market participants, prioritize/solve market problems, or that adapt to market needs. The result has been standards that cover a limited scope of financial data elements with adoption and utilization rates that are below industry-led approaches like FDX, despite the weight of a government mandate and significant public resources.

Specifically, the government mandated approach in the UK is led by the government funded Open Banking Implementation Entity (OBIE). OBIE was created by the UK's Competition and Markets Authority to create software standards and industry guidelines that drive competition and innovation in UK retail banking. This approach was driven by privacy concerns and the need to create more competition. The OBIE technical approach was twofold: to build functional APIs to cover account information and payments in partnership with the nine largest banks and develop security controls with the OpenID Foundation. While operating with a significantly smaller population than the US, Open Banking in the UK reached ~6.5 million consumer accounts and one billion API calls with a staff of more than 150 and annual cost of more than £36m 2021 (approximately USD 43.7 million). In comparison, FDX's voluntary and industry-led approach (with less than 10 full-time employees and a budget of approximately $3 million - supported significantly on voluntary hours and support from its members) in the US reached 42 million consumer accounts with more than 3.5 billion API calls by the same time with

no regulatory mandate, government resources, or the benefit of a multi-year head start.[18] FDX also has developed twice as many use cases, supports hundreds more data elements and many other similar magnifying comparisons. From this example alone, as referenced in the Materials, FDX supports the CFPB's desire to promote the development of industry standards as a positive development for the financial market.

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

FDX suggests the CFPB also consider the experience of other industry-led approaches to financial technology innovation like online banking, mobile banking, and the EMV (EuroPay, Mastercard, Visa) chip replacing the magnetic stripe on cards. All of these significant technological transitions in financial services moved forward without government mandates or artificial timelines. Further, outside the fintech sector – examples like Bluetooth, Fast Identity Online (FIDO), Universal Serial Bus (USB) and the Payment Card Industry Data Security Standard (PCI DSS) show how market-driven solutions have been successful.

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

Working with FDX as Part of the Solution

FDX hopes that it has provided the CFPB a clear view of how FDX works and the progress it has made to develop and drive adoption of the FDX API as a neutral industry-led technical standards for consumer data sharing. FDX wishes to reiterate the progress, maturity, and overall benefits of FDX API to enable end-users to access, share, and use their own financial data in compliance with regulatory and legislative requirements. FDX wishes to submit that an industry-led approach is best suited to develop, implement, promote, and certify technical standards for user-permissioned data sharing in the United States.

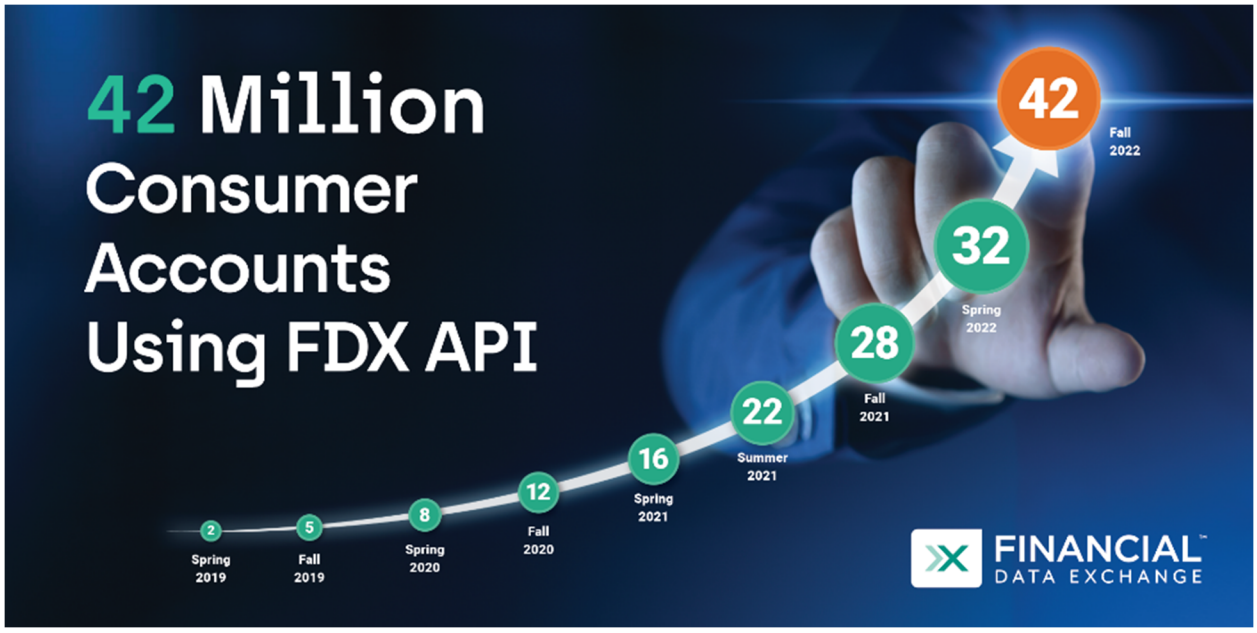
Enabling the industry to continue to drive adoption of the FDX API standard would be the most efficient and inclusive path forward toward providing consumers reliable and secure access to their financial information in support of managing their financial wellness. FDX is dedicated to unifying the financial services industry around a common, interoperable, royalty-free standard for the secure and convenient access of permissioned consumer and business financial data. Membership is open to all stakeholders and the FDX Board maintains a diversity of organizations across the ecosystem. Most importantly, regardless

[18] Derived from information contained in The Open Banking Impact Report, June 2022, the Open Banking Implementation Entity 2023 New Year message, and other sources and articles.

of membership status, FDX provides free access to the API standard along with tools, guides and supporting materials to enable equal access and promote successful implementation. By providing free access to a common, interoperable, royalty-free standard, FDX lowers barriers for smaller financial institutions and start-ups, encouraging competition in the marketplace, and creating a more level playing field for service providers meeting the needs of traditionally underserved communities.

The industry driven FDX API standard provides opportunities for participants in the open banking ecosystem to continue to develop innovative market driven solutions for consumer permissioned sharing of financial information collaboratively and efficiently as both technology and regulation evolve. The standard is consumer centric and based on five core principals: control, access, transparency, traceability and security. These principles drive continuous focus on maintaining consumers ability to control the sharing of their data with trusted parties who provide transparency into how the consumer's data is used, with best-in-class security.

FDX membership and adoption of the standard continues to grow since its inception in 2018. There are ~230 member organizations. In the short time from Spring to Fall 2022, the number of consumer accounts benefiting from using the FDX API standard grew over 30% from 32 million to 42 million (a significant increase in pace over prior periods). FDX expects adoption to continue to grow with the planned launch of the FDX Certification during 2023.



As the CFPB considers its rulemaking, FDX encourages the CFPB to consider that it is in the best interests of the financial services industry to grow and change in order to make compliance easier and less expensive for ALL market participants. The FDX API as a neutral industry-led technical standard for consumer data sharing has proven to be more successful than any government or other solution in place. FDX therefore submits that industry-led approaches are best suited to develop, implement, promote, and certify technical standards for user-permissioned data sharing in the US.

Conclusion:

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

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

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

FDX welcomes continued engagement with the CFPB on these issues.

Appendices

A. FDX Taxonomy of Permissioned Data Sharing v. 1.4
B. FDX User Experience Guidelines v. 2.2
C. Publicly Announced Data Sharing Agreements Mentioning FDX API

Appendix A

FDX Taxonomy of Permissioned Data v. 1.4

Taxonomy v 1.4 Attached Hereto

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) '**consumer**' means a natural person who, in payment service contracts covered by this Directive, is acting for purposes other than his or her trade, business or profession;

(29) '**authentication**' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's 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 B

User Experience Guidelines v. 2.2

User Experience Guidelines v. 2.2 Attached Hereto

FINANCIAL™ DATA EXCHANGE

User Experience Guidelines

Version 2.2
December 2022

Legal Notice

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

Revision History

Document Version	Notes	Date
2.2	Incorporates RFC 0240 to introduce a Money Movement user journey and edits to the Data Clusters section. Reorders Consent Dashboard subsections, removes the DAP Consent Dashboard section, and determined must vs should language.	**December 2022**
2.1	Incorporates RFC 0151 describing consent editing, as well as changes to the data cluster section.	**May 2022**
2.0	Incorporates RFCs 0150, 0159, and 0160 describing consent management, data cluster requirements, and journey notification.	**October 2021**
1.0	Initial Document Release This document was created as a result of FDX RFC 0019 and incorporates the full contents of the RFC for public release.	**December 2020**

Contents

Section 1: Introduction

Document Purpose and Intended Audience

This document provides the user experience (UX) guidelines and best practices for FDX implementers. The intended audience is anyone responsible for the financial data sharing interface/experience of any FDX-participating software or service. This audience includes, but is not limited to, user experience designers, product managers, and software development teams.

In particular, these UX guidelines aim to accelerate design decision-making during implementation of data sharing experiences, as well as specify what information and control must be given to end users.

The principles and guidelines in this document were developed following multiple sessions of consumer research, in accordance with principles and recommendations from FDX, its members, and several organizations such as the Consumer Financial Protection Bureau (CFPB), the Clearing House, and the Financial Services Information Sharing and Analysis Center (FS-ISAC). Existing data sharing experiences that are currently in production were also reviewed and served as input in the research and evaluation process.

These recommendations represent FDX's perspective on how to provide access and control for consumers and businesses. These User Experience (UX) guidelines should be used in tandem with other FDX publications, such as the FDX API and Security guidelines. See References below for a list of reference documents.

Please note that the term "Required" refers to likely future certification requirements and should be considered as best practices until certification requirements are established.

Scope

This document describes the concepts of 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.

More guidelines will be presented in future published versions of this document. Please refer to Appendix A: Topics for Further Review for a full list of topics being considered.

Terminology and Concepts

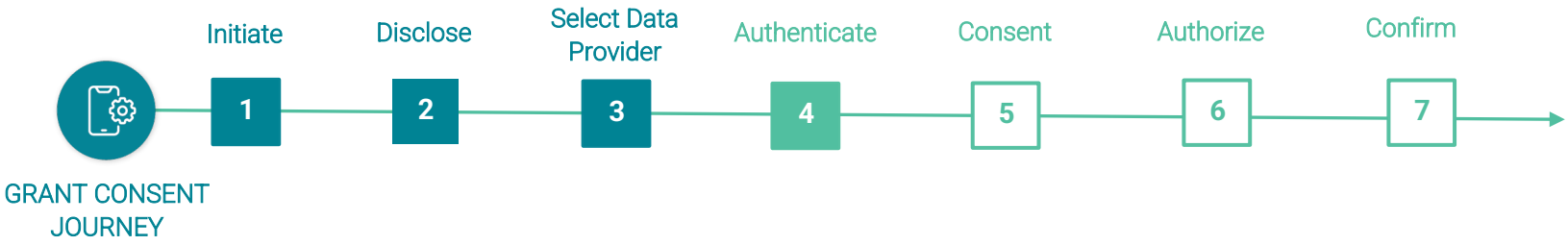
Please refer to the *FDX Taxonomy of Permissioned Data Sharing* document for a clear definition of recurring terms such as data provider, data recipient, data services platform, end user delegate, and end user.

Section 3 of this document describes the user experience guidelines. Two concepts are applied during the presentation of the UX guidelines. The top level of a user experience is presented as a **Journey**. Each journey contains a set of **Processes**.

1. **Journeys** – These capture the end-to-end view of a consent management operation, such as granting consent, refreshing consent, or modifying/revoking the consent.
2. **Process** – Each journey is broken up into a process that maps to a specific user goal, for example, disclosure, authentication, authorization, etc. Processes contain steps and options for the user to complete each goal.

For example, granting consent is a larger Journey that the end user embarks upon. The Journey contains a few Processes, for example authorize, which is a multi-step process. During the authorize Process, an end user will complete steps to select accounts to include in authorization. Thus, granting consent is the Journey and the act of authorizing is a Process within that Journey.

Breadcrumbs depicting the relevant journey and process will appear throughout the document as such.



Regulatory Requirements and Considerations

The following regulatory considerations are key drivers of these guidelines and must be adhered to for any user experience. Relevant items and their source are included in the table below for informational purposes only.

FDX is a standards body and adopts these guidelines for general use among industry stakeholders. Many of the terms, however, are subject to additional guidance under prevailing laws, industry norms, and/or governmental regulations. While referencing certain laws that may be applicable, stakeholders should seek legal advice of counsel relating to their particular practices and applicable laws in the jurisdictions where they are deemed to do business. Each participant must determine which laws, rules and regulations apply to each aspect of the experience. See FDX's complete Legal Disclaimer located at http://www.financialdataexchange.org for other applicable disclaimers.

Table 1 Regulatory Requirements and Considerations (including but not limited to):

Certain Regulations	Items
UDAAP (Unfair Deceptive and Abusive Practices)	Need to be clear with the messaging as to what is taking place when a user provides consent so that expectations are set properly. Need to ensure that a user's requested action, such as revoking access, is honored completely to avoid the perception of deceptive statements or unfair treatment of the member by allowing data flow to continue. If there are circumstances where data flow needs to continue (e.g. to manage fraud), that it is disclosed clearly to the consumer the circumstances under which the action would not apply.
GLBA (Gramm-Leach-Bliley Act)	Cannot share a user's non-public personal Information without their consent except for a set of limited exceptions. Need to allow users to opt out of sharing of user's non-public personal information with non-affiliates, except for a set of limited exceptions. See Title V of Gramm-Leach-Bliley Act (GLBA); implemented by Reg. P.
ADA (American Disabilities Act)	Need to make sure that the UX/UI are compliant with ADA, e.g. usage of screen readers, etc.

COPPA (Child Online Privacy Protection Act)	Cannot collect or share personal information of children under 13; should be enforced at the time of consent.
Electronic Fund Transfers (Regulation E)	Regulation E protects consumers when they use electronic fund transfers (EFTs). Institutions must disclose the consumer's liability for unauthorized EFTs, the types of EFTs the consumer may make, and any limit on the frequency or dollar amount; fees charged by the institution; and error-resolution procedures. Institutions must also provide a summary of various consumer rights under the regulation.
CFPB Principles For Consumer-Authorized Financial Data Sharing and Aggregation*	These principles established a set of guidelines for permissioned data sharing related to data access, data scope, data control, informed consent, data security, transparency on data access rights, and accountability for access and use. It essentially calls out rules for consent, revocation access, and transparency of data access. * CFPB principles are not regulations, but should be considered when shaping the user experience

References

Other FDX publications that are referenced in this document include:

- FDX API Documentation
- FDX API - Data Structures
- FDX Security Control Considerations for Consumer Financial Account Aggregation Services
- FDX Financial-Grade API Security Specification
- FDX Taxonomy of Permissioned Data Sharing

Section 2: Data Sharing

This section describes the principles that guide data sharing, the concepts of data sharing and flow, the consent components involved, and the concept of consent by business purpose.

Principles Guiding Data Sharing Experiences

The user experience guidelines described herein have been derived from a number of sources:

- FDX's core principles: Control, Access, Transparency, Traceability and Security;
- FS-ISAC's initial work on DDA user experiences; and
- research into permissions and consent performed by The Clearing House.

FDX's core principles of data sharing are defined as follows:

Control

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

Access

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

Transparency

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

Traceability

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

Security

Entities need to ensure the safety and privacy of data during access and transport and when that data is at rest.

Based on these core principles, the user experience guidelines contribute to building trust in financial data sharing. Consistency of experiences that results from adoption of these guidelines means that end users will not need to learn new models or interactions each time they opt to share financial data. Further the guidelines are informed by user research, resulting in clear and efficient user experiences that ensure security and privacy.

Data Sharing and Flow

Financial data sharing describes the process by which a consumer or business entity uses an application or service to access their own financial data, which is available at one of their financial service providers. This flow of data enables people and businesses to manage and interact with their financial data using their chosen applications, experiences and services.

Types of Financial Data

Financial data can generally be considered in three broad categories:

1. **Primary financial data** is data associated with actual financial accounts, including balances, holdings, and transactions directly reflecting monetary and financial actions. There are many types of primary financial data; the most commonly accessed include banking and investment account data, but may also include commerce data, tax data, employment data, credit score data, asset information, and business accounting data.
2. **Customer identity data** is information about the end user that can be used to uniquely identify such end user, such as name, address, or telephone number.
3. **Derived financial data** consists of observations, analysis, or models developed with primary data as an input, such as a cash flow analysis. Derived data may be the result of numerous financial and non-financial inputs.

For the purposes of this document and guidelines, we will focus on the first two categories - primary financial data and customer identity data that is often included or part of primary financial data. They correspond to the majority of financial data access business purposes. Derived or secondary financial data is often proprietary information that is retained at the data source.

In the recommendations below, we discuss **data types** and **data elements**. Data types are categories of data that are accessed or shared, for example, account balances, transactions or account statements. Data elements are the specific data fields within each data type, for example, transaction ID in a deposit account data type.

Parties Involved in Financial Data Sharing

Please refer to the FDX Taxonomy of Permissioned Data Sharing document for additional definitions.

Consumers: are end users acting in their personal capacity.

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

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

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

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

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

Flow of Financial Data

Financial data flows from a data provider (source) to the data recipient (requester). Data access platforms/End user delegates may be involved in one or more aspects of facilitating this flow. The financial data flow process is as follows:

1. Data sharing is often initiated with a prompt by the data recipient to the end user, in order to access their accounts.
2. The end user identifies the data provider where their accounts are held.
3. The data provider inspects the request and allows the end user to grant consent for data sharing.

With this permission recorded, the data provider and data recipient exchange access details to enable the flow of financial data. In some cases, a data access platform may facilitate the access between the data recipient and the data provider. In this instance, the access details are exchanged between the data provider and the data recipient via the data access platform.

Some examples of the flow of financial data between parties are as follows:

- **Financial Institution (data provider) → App (data recipient)**

  Account transaction data flows to a budgeting app where it is used to track spending by category

- **Financial Institution (data provider) → Service Provider (data recipient)**

  Account balance data flows to a loan-provider to determine the end user's borrowing power

- **Financial Institution (data provider) → Aggregator (data access platform) → App (data recipient)**

  Investment holdings from across multiple brokerages flow through an aggregator, which normalizes the data, to an app where it is used to give a 360° view of assets

- **Employer (data provider) → App (data recipient)**

  Employment information such as payroll data and W-2s flowing to a payroll, tax or loan application

- **App (data provider) → Financial Institution (data recipient)**

  Credit score information or personal/business financial information going to a financial institution to help deliver tailored financial services to that consumer or business

- **Service Provider (data provider) → Financial Institution (data recipient)**

Product recommendations based on portfolio data from across multiple financial institutions flows to a bank which can then offer financial products to their customer

Consent Components

An end user granting consent to a data provider to share data with a data recipient requires a clear understanding of what is being shared and with whom, how it is being used and how long this agreement will last. This consent should allow the end user to do so without sharing their credentials for the data provider. With the use of a token-based consent, in lieu of credentials, and controls around what they authorize to share, the end user can better manage access to their data. These components of consent include data clusters, duration and business purposes.

The **data recipient** should clearly describe the consent components to the end user. The data recipient may optionally use data services provided by the data access platform to service the consent components and to manage the various parts of the consent lifecycle. Refer to the FDX Taxonomy of Permissioned Data Sharing document for more information on token-based consent/tokenized access.

Data Clusters

What is a data cluster?

A data cluster is a term used to group a functional collection of data elements. As a fundamental part of the scope of consent, it's used to communicate to the end user what data will be shared when consent is granted and to ensure that only that data is shared. An example of a data cluster would be ACCOUNT_DETAILED, providing the data elements needed to obtain balances for an account. Standardizing Data Clusters provides a consistent definition for all parties involved.

Data Clusters provide the mechanism for the Data Recipient to identify what kind of data it needs for the service(s) it provides. Likewise, Data Clusters allow the Data Provider to not only convey what data will be shared but to control access to the data to ensure that only authorized data is accessible.

Data Clusters can be combined as "building blocks" to identify the data being authorized. For example, a budgeting business purpose may want to access both ACCOUNT_DETAILED and TRANSACTIONS, a data cluster which covers all historical and current transactions for an account. Likewise, different business purposes may be supported using the same data clusters. For example, budgeting or mortgage applications might both have a need to access the balances for the accounts that where authorized covered by the Account Information Basic data cluster. Once the Account Information Basic data cluster is authorized, the Data Recipient

can use that same data to support both business purposes. A Data Recipient should request the set of all Data Clusters that will access all of the data they need to provide all of the services they perform.

See Table 2 Data Cluster Terminology for the full list of data elements associated to each data cluster.

Data Cluster Uses

While data clusters are used to communicate what data is being shared, not all data elements covered by a data cluster are of particular importance to an end user. For example, the ACCOUNT_DETAILED data cluster includes a field that indicates whether a balance increase is a fixed, percentage or dollar value. This field may be important to the Data Recipient to provide the correct experience but is not relevant to the end user. However, there are some key data elements in each data cluster that are sufficiently important that they should be specifically exposed so that the end user understands what they are agreeing to share. These guidelines intend to provide a common name for each data cluster plus the list of key elements that should be openly disclosed to the end user, during the Grant Consent journey as well as, later, when managing that consent. The guidelines specifically do not intend to specify the tone and specific language that each entity uses, intentionally leaving that up to the individual entities. However, each entity must include the specific key elements in the description, tool tip or explanatory content provided for the data cluster.

Data Cluster Terminology

Data clusters should be represented in a consistent way for the End User, across all involved parties and throughout all flows, much like an industry taxonomy. This provides the following benefits:

- Harmonizes representation of data to be shared across data recipients, data access platforms and data providers
- Increases end user confidence in sharing data when consents appear the same across parties
- Facilitates interoperability across parties to avoid one-off bilateral agreements
- Allows data recipients to capture data sharing scope programmatically
- Allows data providers to limit data access based on the authorized data categories

Data Cluster Components

The table below provides the list of approved Data Clusters supported by FDX.

- **Data Cluster** - the enum included in the consent scope, either directly or registered for a Data Recipient.
- **Required Label** - the short label for the associated Data Category. This name must be displayed to the end user in the Grant Consent journey. The Data Recipient and in the disclosure step and by the Data Provider in the consent step. Likewise, this

name should be presented to the end user during Consent Management to ensure that the end user is aware of what data they have authorized.

- **Required Key Elements** - a list of key data elements which must be included, either directly or in a more detailed description, such as a tool tip. The entity may provide additional commentary, as needed, using any tone or style they choose, as long as these terms are included for consistency.

The following terms are prescribed for use in all End User-facing interactions, applications, and experiences.

Note: These Data Clusters are intended to be used as documented herein.

Table 2 Data Cluster Terminology

Data Cluster	Read/Write	Required Label	Required Key Elements
CUSTOMER_CONTACT	Read Only	Account contact details	• Your name, address, email and phone • Name(s), address, email and phone of any account holders
CUSTOMER_PERSONAL	Read Only	Sensitive personal information	• Your name, address, email and phone • Name(s), address, email and phone of any account holders • Your date of birth • Social Security Number (SSN) • Government ID
ACCOUNT_BASIC	Read Only	Account identifying information	• Account display name • Masked account number • Account type and description
ACCOUNT_DETAILED	Read Only	Account summary information	• Account display name • Masked account number • Account type and description • Account balances • Credit limits

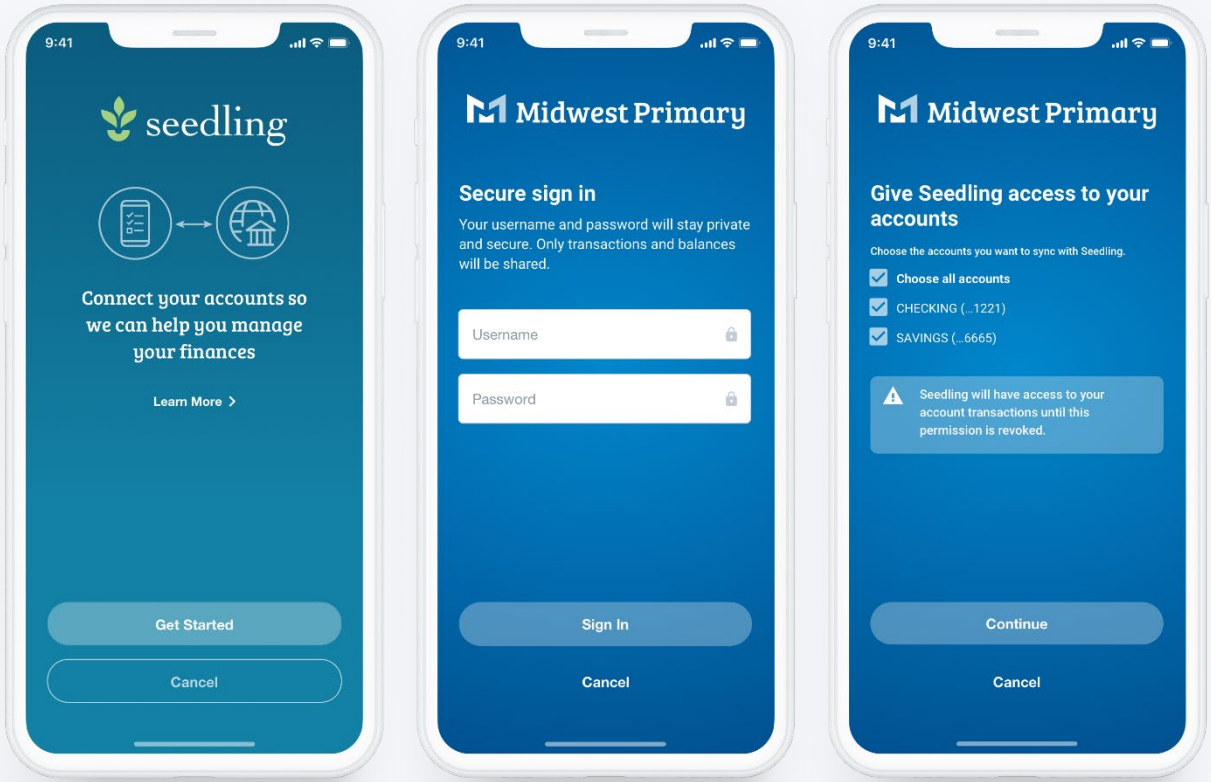
			• Due dates and interest rates
ACCOUNT_PAYMENTS	Read Only	Account information payments	• Full account and routing number • SWIFT or IBAN numbers
INVESTMENTS	Read Only	Account investment details	• Investment contributions • Investment loans • Pension data • Vesting and account holding details
TRANSACTIONS	Read Only	Transaction data	• Pending and posted account transactions • Transaction types, amounts • Dates and descriptions
STATEMENTS	Read Only	Account statements	• Account PDF statements containing personal information • Account and transaction details

Duration of Consent

Within the FDX model, the duration of the consent provides the context defining when and how long the data recipient will have access to the end user's data and whether the end user must take action to revoke access, if needed. It can be described in one of three ways: persistent, time-based, or one-time (single) use. A single consent must use only one of these durations.

Persistent

Persistent consent is granted for ongoing data sharing. This allows the data recipient to access end user's data, within the constraints of the permitted business purpose, whenever it deems necessary to execute the service it provides for the end user. Access does not have to be tied to an explicit end user action or application event, such as a daily updates for the purpose of budgeting. With persistent consent, an application can regularly investigate an end user's financial standing in order to form data models or recognize behavior patterns to inform a recommendation engine. Persistent consent should remain active until the end user specifically revokes that consent, either through the data provider or the data recipient. As in the other cases, the end user should always be informed about the duration of the consent they are providing.

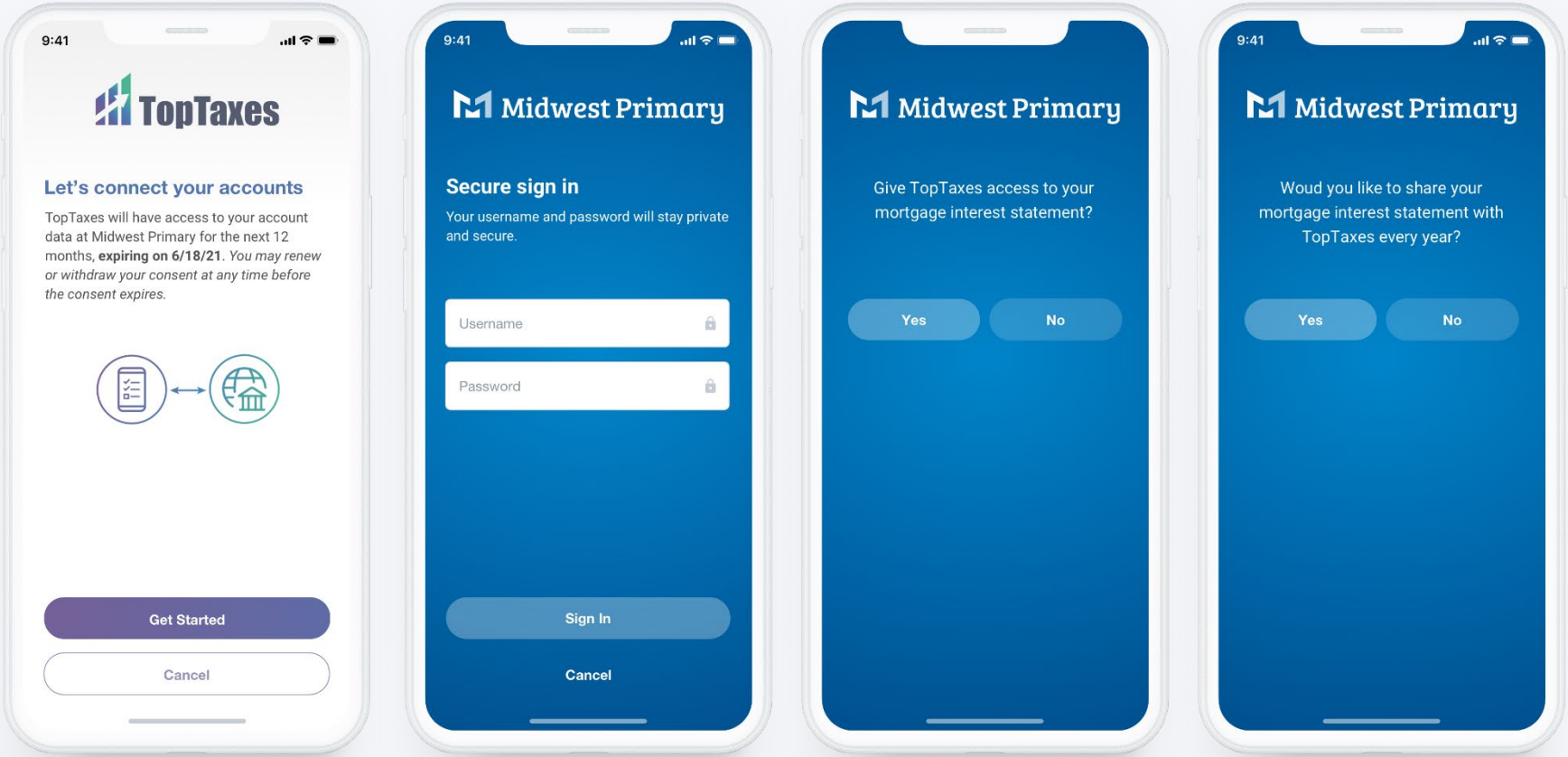


Sample Persistent Consent language

[Data Recipient] will have access to your account data at [Data Provider] until you withdraw your consent to share this account data. You may withdraw your consent at any time.

Time-based

Time-based consent is granted when the service provided by the data recipient has a discrete window need to complete a specific task such as applying for a loan. The consent is granted for the specific window (e.g., 90 days) and should be automatically revoked at the end of specified time period. Access after that time will require the end user to re-consent. The specified time should be communicated to the end user to provide clear understanding of how long the access will be active and why.



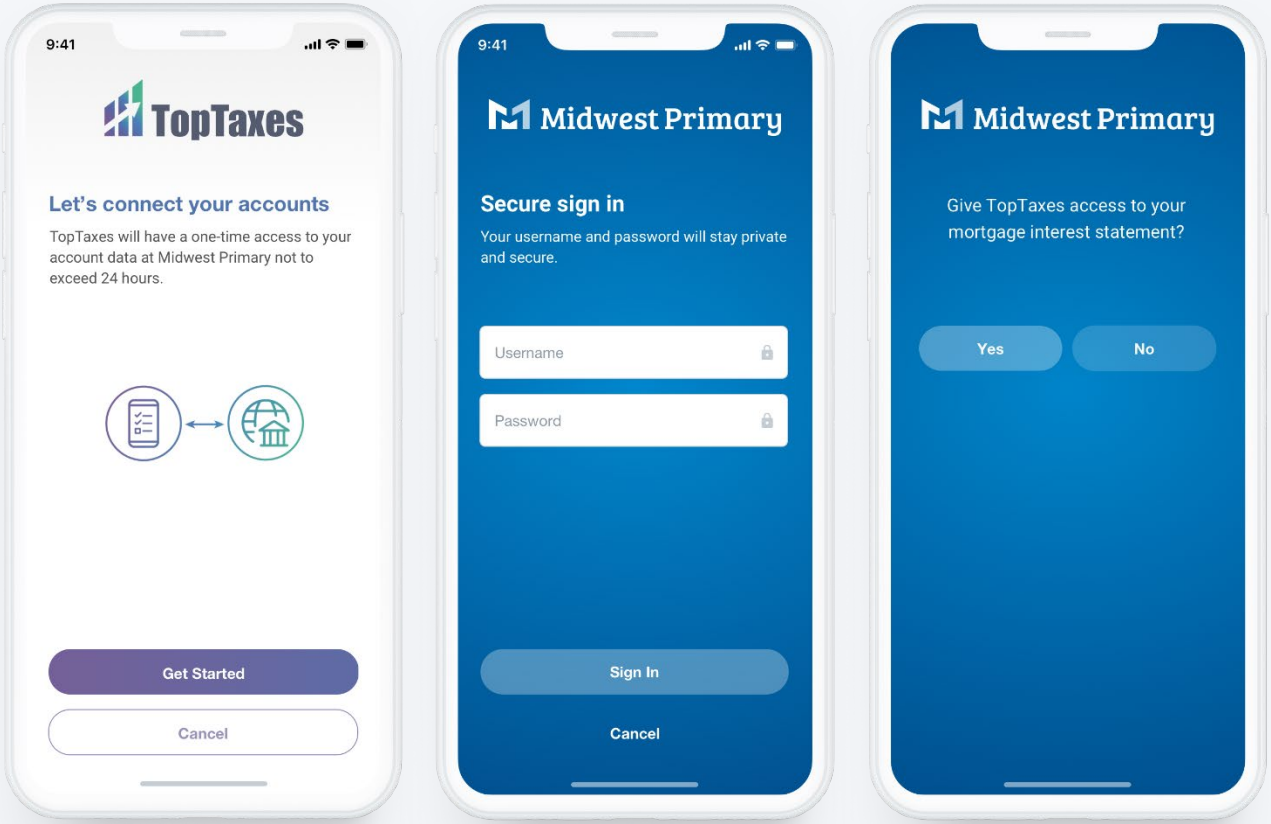
Sample Time-based Consent Language

[Data Recipient] will have access to your account data at [Data Provider] for the next 12 months, expiring on [end of consent period]. You may renew or withdraw your consent at any time before the consent expires.

One-Time Use

One-time consent is granted for a single, discrete, and short-lived interaction. One-time use consent is tied to an explicit end-user action or application event that requires only one retrieval of the required data, such as identity or account verification. The expectation is that once the data has been retrieved, the consent will be automatically revoked, preventing it from being used again at a later time.

The end user's data may only be accessed in the context of this interaction and, typically, the data will not be stored beyond the time required for this specific interaction to be completed. There are exceptions when, for legal or regulatory purposes (for example transaction records or tax returns), the data that was accessed may be stored for a longer period of time. In that case, it must be very clearly disclosed to the end user that the data recipient will keep the data, for how long and why. Further, the stored data must not be used for a purpose outside the scope of the original consent without a new consent from the end user and additional data may not be accessed to contextualize the original data.



Sample One-time Consent Language

[Data Recipient] will have a one-time access to your account data at [Data Provider] not to exceed 24 hours.

Consent by Business Purpose

Data recipients may provide a specific service that the end user may want to leverage. With FDX, this service, or business purpose, will be defined as a specific set of data clusters which provide the necessary data elements for that service as well as the prescribed duration for that consent. As specific business purposes are established, data recipients must define their consent based on these business purposes. The data recipient must clearly describe the primary business purpose with the data clusters and duration required.

In some cases, data recipients may want to provide services for more than one business purpose. In this case, the data recipient should indicate which business purpose, or cases, are required, and which ones may be optional. The consent provided by the end user will cover, at a minimum, access to the data clusters needed to provide the services for the required business purposes.

Life Cycle of Consent

FDX requires that exchange or sharing of financial or other end user (customer) data must be authorized by the end user. Ultimately, the end user has control over who is able to access that data. The end user whose data flows between data providers and data recipients or data access platforms must give informed and unique consent for the stated business purpose.

Data sharing must be **explicitly** permissioned by the end user. Changes to what data is included in the consent require explicit re-consent by the end user.

While the consent itself represents this permission for a period of time, the user experience of data sharing takes place in three discrete phases:

- Grant Consent
- Manage Consent
- Revoke Consent

Grant Consent

Granting consent is the process of **establishing the terms of data access** between a data provider (e.g. financial institution) and a data recipient (e.g. financial application). In some instances, a data access platform may be involved as a way for the data recipient to more easily access a larger number of data providers. A given consent defines the access that an end user has authorized.

The process to grant consent is initiated from within the data recipient experience.

The data recipient is responsible for defining the types of data, or data clusters, needed to support the business purpose(s) presented to the end user. If the end user wants to enlist these services, they must consent to the data required to do so. The data recipient must clearly explain what types of data they need and why they need this data to best inform the end user during consent. In addition, this consent always has a prerequisite period of time, or duration. During the consent process, the end user directs the data provider to share none, one, some or all of their accounts with the data recipient.

During the consent process, the selection of which accounts to access data from should be performed at the data provider during authorization. This avoids any account information having to be unnecessarily disclosed outside of the data provider. The end user must **explicitly** authorize the use of their data. Authorization to share data requires that the end user be presented with the parameters of use and have the option to decline. Data providers MUST display the data clusters as they were presented to the user by the data recipient at the disclose stage. Data providers MUST NOT permit end users to configure data usage.

Consent for financial or other data access is granted by one end user, to data recipient(s), for a specific set of data clusters (defined by the business purpose(s) for which the data is requested), for a specific list of accounts held by a data provider, and for a specified period of time.

Manage Consent

Managing consent is the process of maintaining or **modifying the access** between the data provider and the data recipient, and when applicable, through a data access platform.

Management is typically handled through the data provider where the consent was given, but, in some cases, may be initiated by the data recipient or through a data access platform experience.

More information and a detailed journey for how to allow an end user to manage their consent will be provided in future versions of the FDX User Experience Guidelines.

Revoke Consent

Revoking consent is the process of **removing the access** between a data provider and a data recipient.

Access can be revoked from within the data provider, data recipient, or data access platform experience when applicable. If revoked by a data provider or recipient, the access will also be removed from the data access platform when applicable.

More information and a detailed journey for how to allow an end user to revoke their consent will be provided in future versions of the FDX User Experience Guidelines.

Section 3: User Experience Guidelines

Journey | Consent

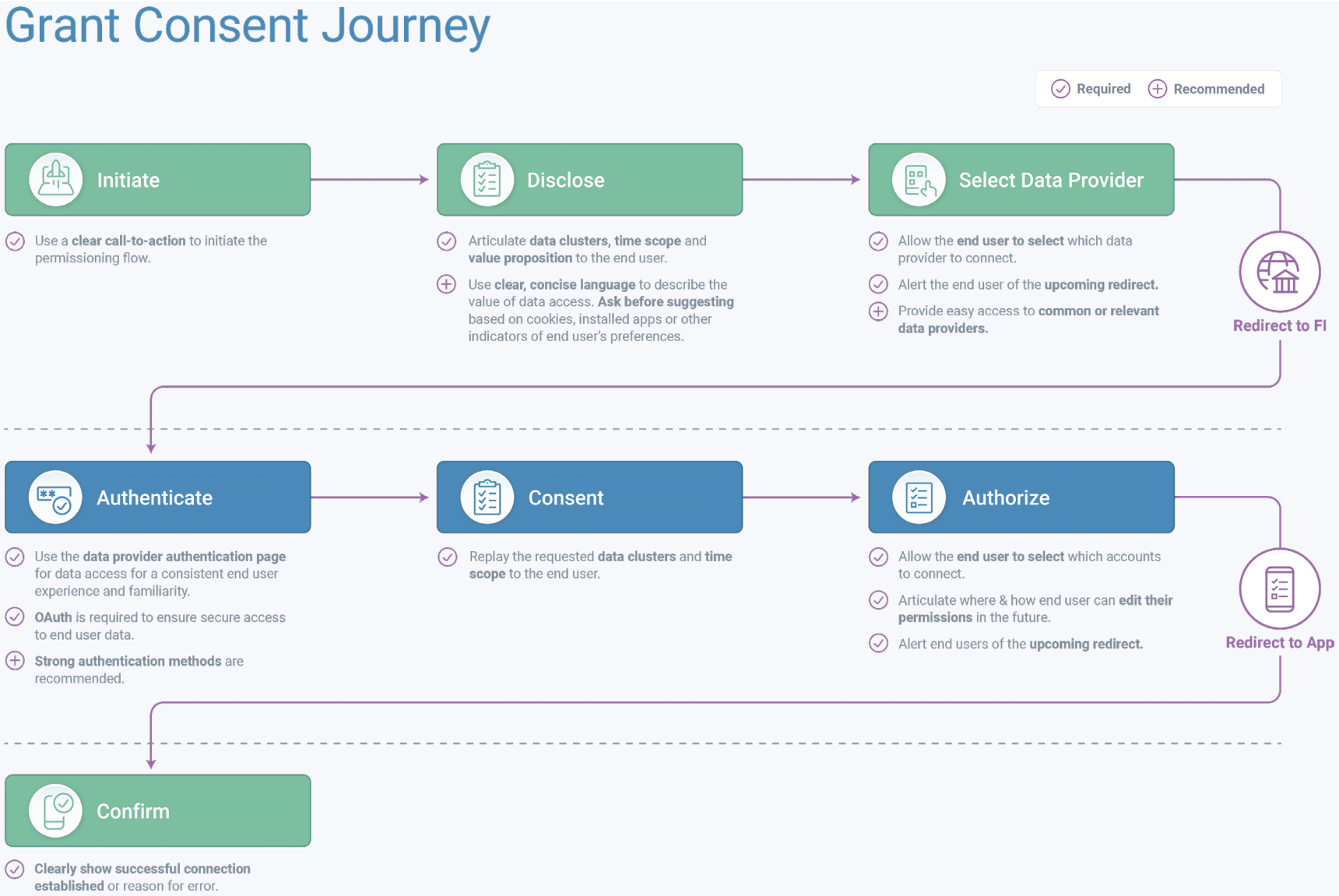
The prescribed journey shown below reflects the recommended information and functionality provided by the data recipient and the data provider. They are intended to show who is responsible for each but not necessarily indicative of the number of physical pages required by either the data provider or the data recipient. Screen images are meant to serve as illustrative examples of implementations.

Please note that within all journeys, the term “Required” refers to likely future certification requirements and should be considered as best practices until certification requirements are established. This is intended to provide a base understanding of the user experience and thus journeys will change and adapt based on business purpose.

Refer to Table 2 Data Cluster Terminology on page 18 for specific data cluster terms that should be displayed in End User applications.

Customer Grant Consent Journey

The Grant Consent Journey consists of seven process steps.



1 Initiate

Purpose — Motivate the end user to provide access to their financial data

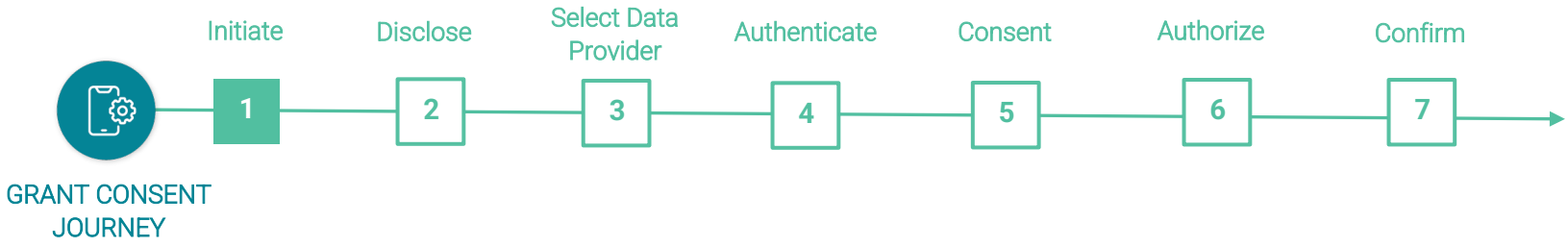
This step provides details about how the end user can share their data from a data provider to the recipient to provide the services requested. It is important that the end user is clear about the benefits of sharing their accounts and who is involved.

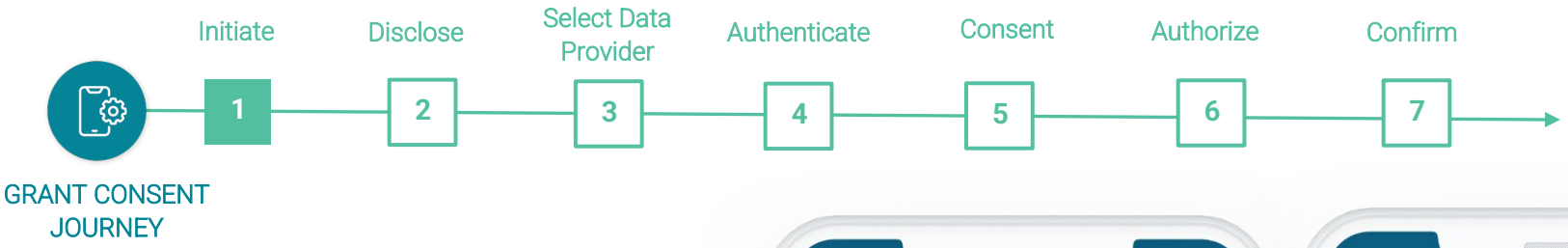
Required

- A clear explanation of the purpose/benefits for sharing accounts to the application or service
  - Provide a path to view a description of what steps are involved on a secondary screen, such as “Learn More”
  - Include a description of what happens to data if the consent grant process is terminated or incomplete. Conversely, state that the end user’s data will only be shared upon completion of the entire process, after confirmation
- If an intermediary data access platform, or any entity with access or that processes the data for their own purposes, is involved in setting up access to the data provider, make that apparent to the end user, for example, “Data access provided by” or “Data access facilitated by” (The exact language is to be agreed upon by the parties involved and must specify the existence of the data access platform.)
  - Maintain this indicator on all subsequent screens for consent and data provider selection

Recommended

- Description of Steps
  - Increase comprehension by using a numbered list format to describe a sequence
  - Be concise and call attention to the important part of the customer benefit
- Provide a path (inline or in an optional screen) to view details about the data access platform
- Ensure that the end user understands how their data will be kept secure through this process
- Consider a prominent call to action or guide first-time users through an explanation of the steps to share their data



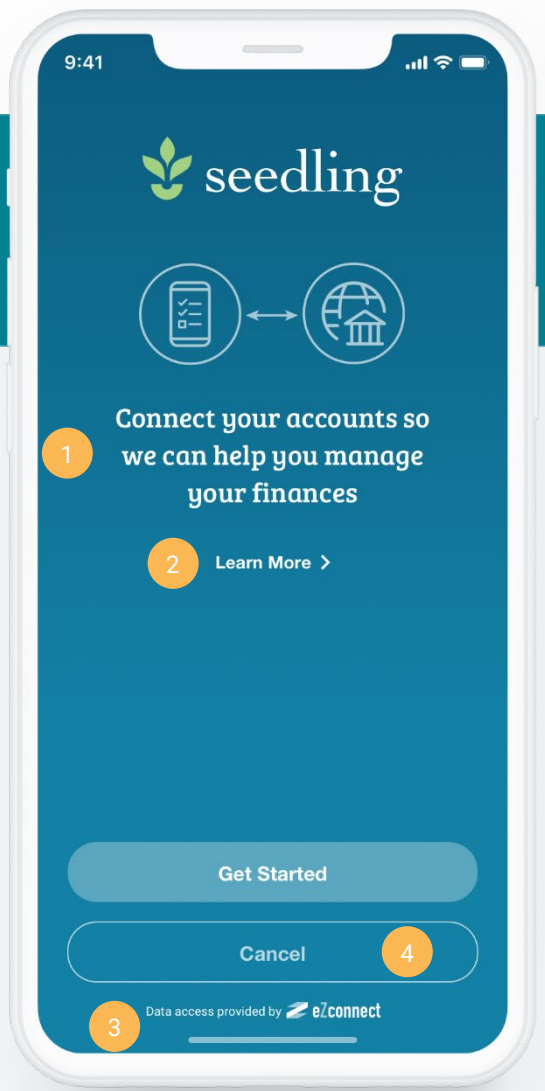


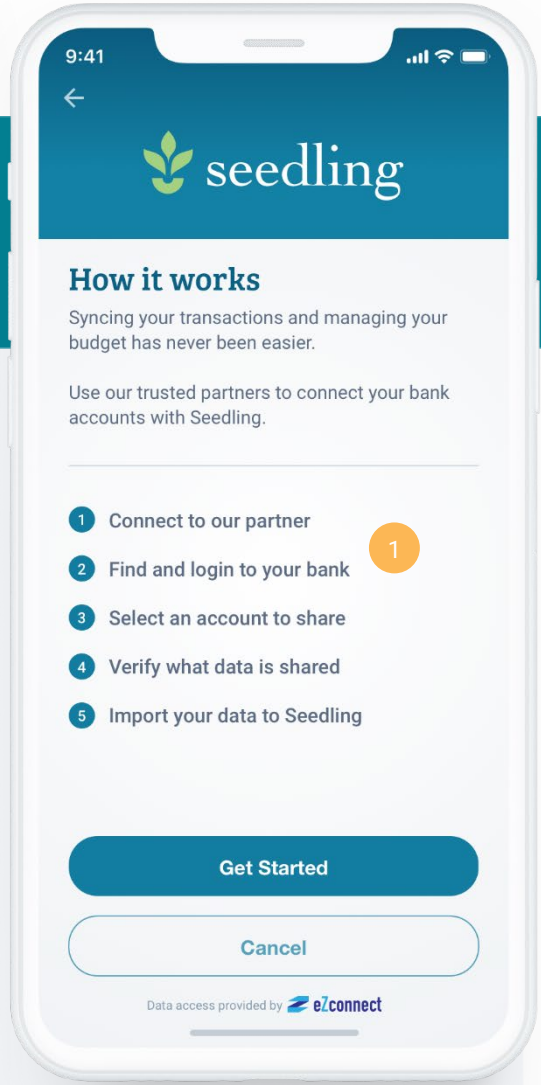
Initiate | Sample User Content

Initiate

Clearly indicate to the user that a process to access one of their providers is being initiated.

1. Tell the end user what they are going to do
2. Provide a path to learn more
3. When applicable, identify the data access platform and provide a path to learn more
4. Provide an option to cancel the flow





2 Disclose

Purpose — Communicate the details of the consent to be requested and why

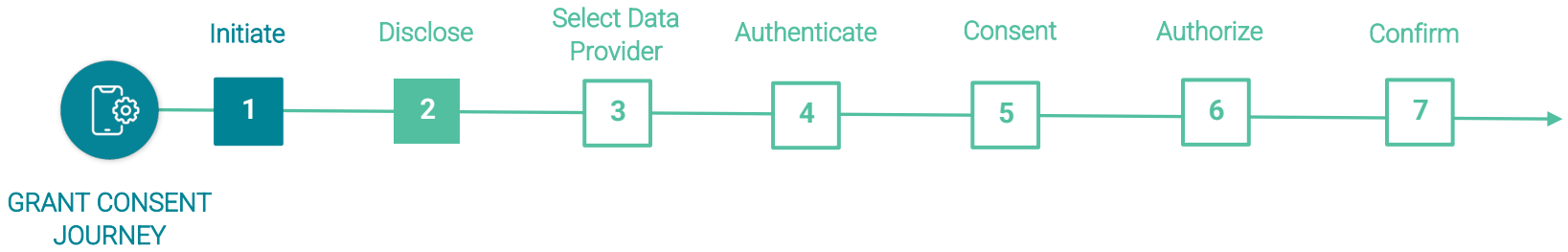
This step provides important information to the end user about what financial data the data recipient needs from the data provider (data clusters, etc.) and why they need it (business purposes) and how long they may need to continue to request this data.

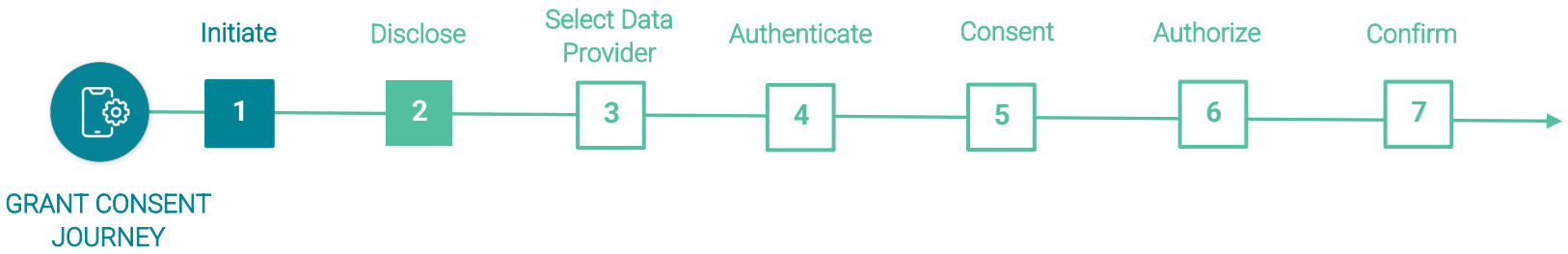
Required

- A clear summary of the data to be accessed using data clusters with familiar terminology for the end user (e.g., account balances, transaction details, account statements)
  - Put the most sensitive or important data clusters at the top of the list for clear visibility to the end user. An additional flag should be added for PII information.
  - Provide a path to view an expanded description of each data cluster and how it will be used by the data recipient
- A summary of what reason (business purpose) the data is requested, such as for delivering a budgeting service
- The data recipient should only require data that is needed for the business purpose in which the end user is engaged
  - Provide a description of the data included within the data cluster
- A succinct and clear statement of **how long** the data will be accessed by the data recipient
  - Provide a path to view more about the duration or how it was derived (See Life Cycle of Consent)
- The means for a user to leave this consent grant journey if they do not agree with the terms of the consent that the data recipient displays.

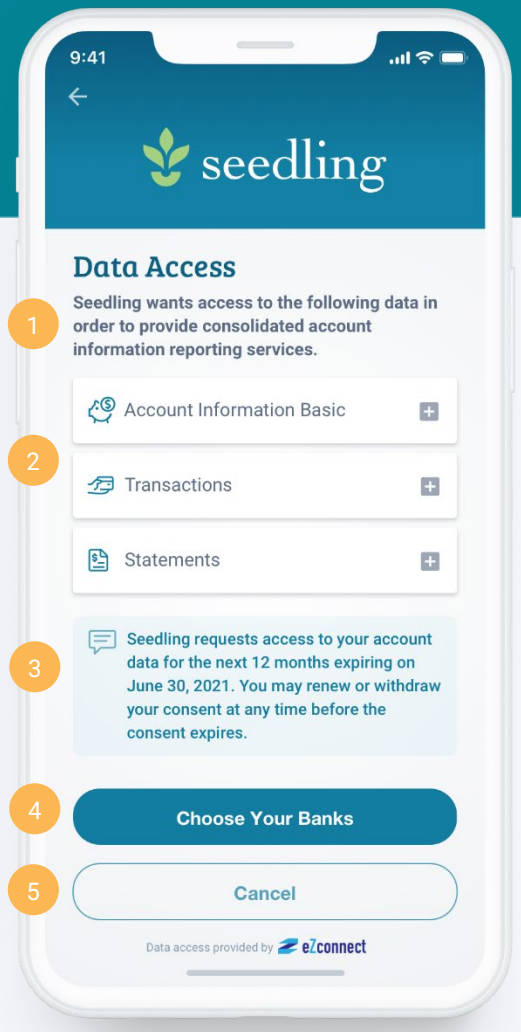
Recommended

- Provide click-down functionality to specific data elements for each data type listed
- Increase comprehension by using succinct and clear language, and use a list format
  - Put most sensitive and/or required data at the top of the list
- Employ familiar and common user interface (UI) patterns for expanding information
  - For example, ⓘ to open a tool tip or an accordion to display more details inline





Disclose | Sample User Content



Disclose

Clearly indicate to the user the data types and duration of the consent.

1. Explain the business purpose
2. Identify the data clusters that the data recipient needs to perform the service
3. State how long this consent will be active
4. Tell the end user what happens next
5. Provide an option to cancel the flow

3 Select Data Provider

Purpose —Enable the customer to find and select a relevant data provider

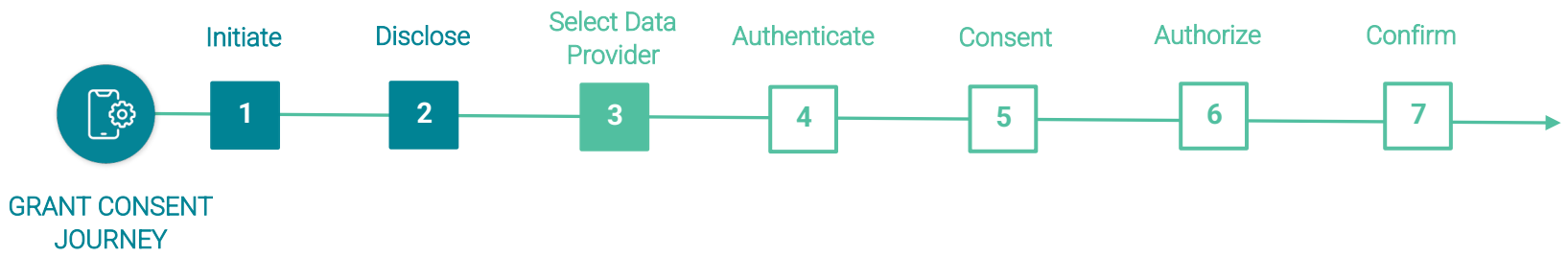
The data recipient, or data access platform acting on behalf of the data recipient, allows the end user to identity and select the data provider(s) for the consent.

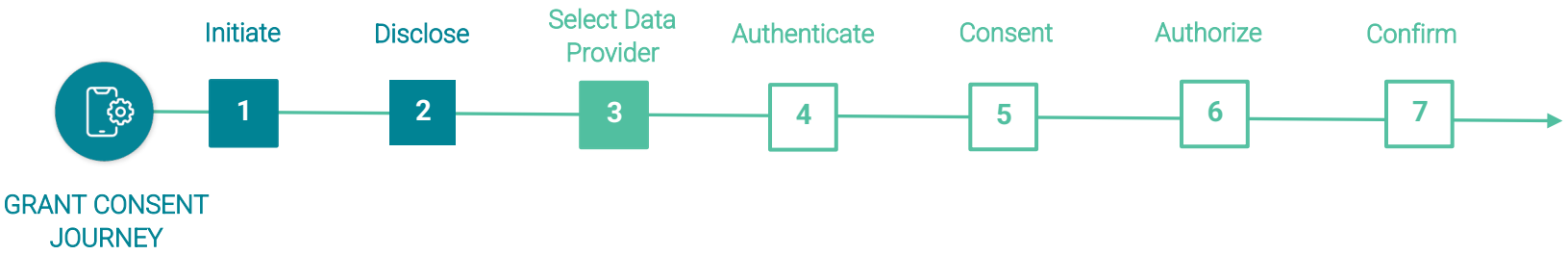
Required

- Succinct and clear presentation of every entity involved
  - Use recognized brand names and iconography with permission from the brand to use their brand art
- Employ familiar and common UI patterns for searching and selecting, including filtering if necessary
  - Provide search capability
- If an intermediary data access platform is involved, make that apparent to the end user
- Indicate to the user that they will be redirected to the data provider
- Provide a cancel or exit option

Recommended

- Explore ways to present a large number of data providers to the user in a manner that helps them find what they are looking for, such as filtering
  - Support elastic search capabilities to simplify searching
- When redirecting the end user to the data provider, use a temporary page/screen to inform the end user that they are being redirected



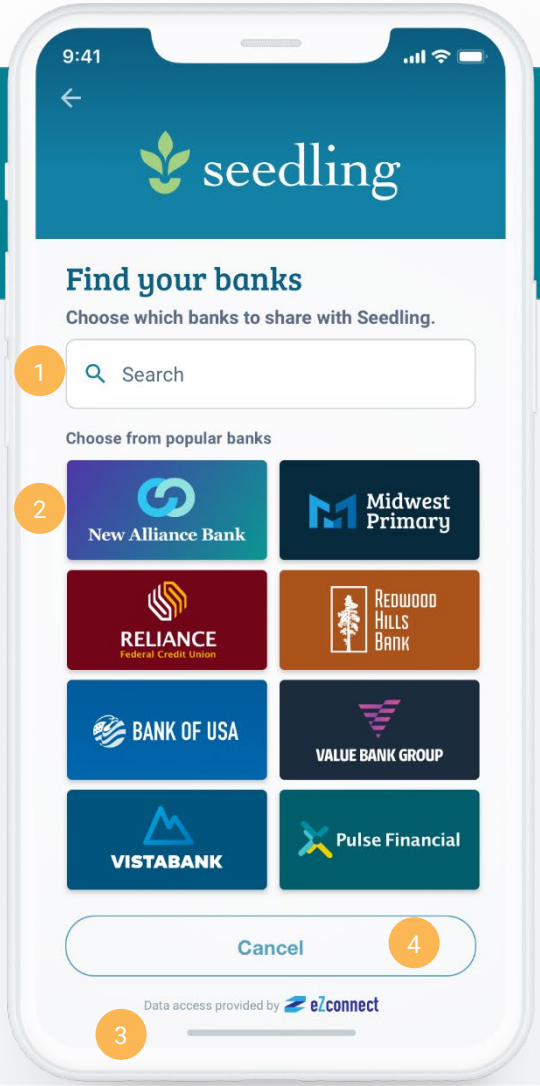


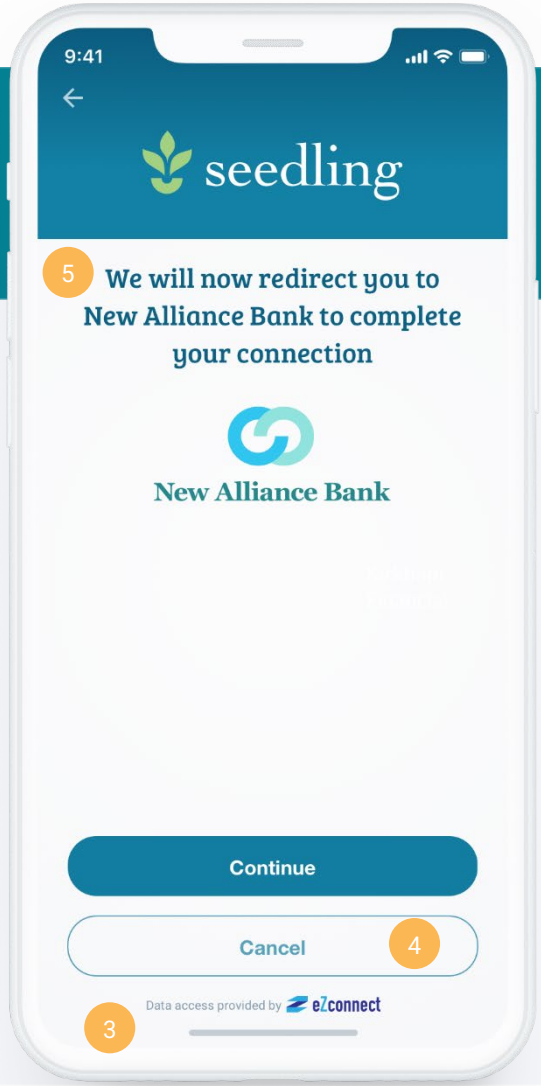
Select Data Provider | Sample User Content

Select Data Provider

Provide an easy to navigate selection screen for all available data providers.

1. Provide a way for the end user to search for their data provider
2. Provide quick links to common data providers
3. When applicable, identify the data access platform and provide a path to learn more
4. Provide an option to cancel the flow
5. Clearly inform the end user that they are going to be redirected to the data provider, ideally using a separate page





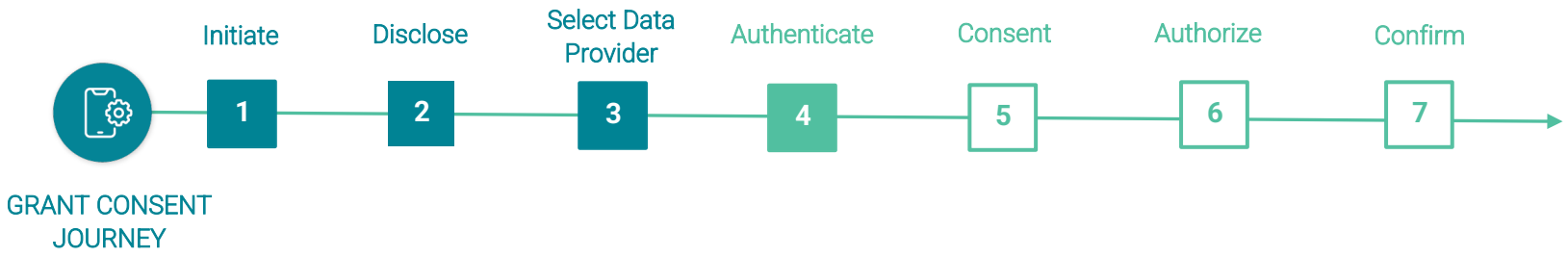
4 Authenticate

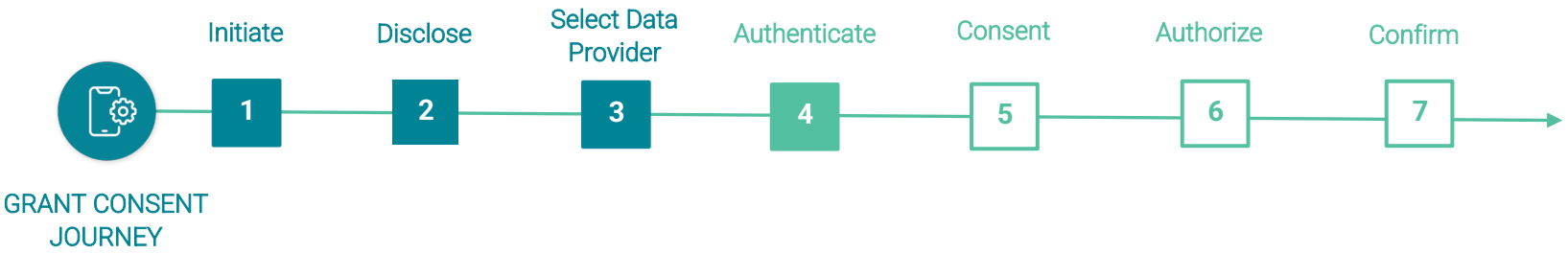
Purpose — Enable the customer to identify themselves to the data provider

This step should be implemented directly by the selected data provider. There is an implicit expectation that the end user is authenticating directly with their data provider and not via another path.

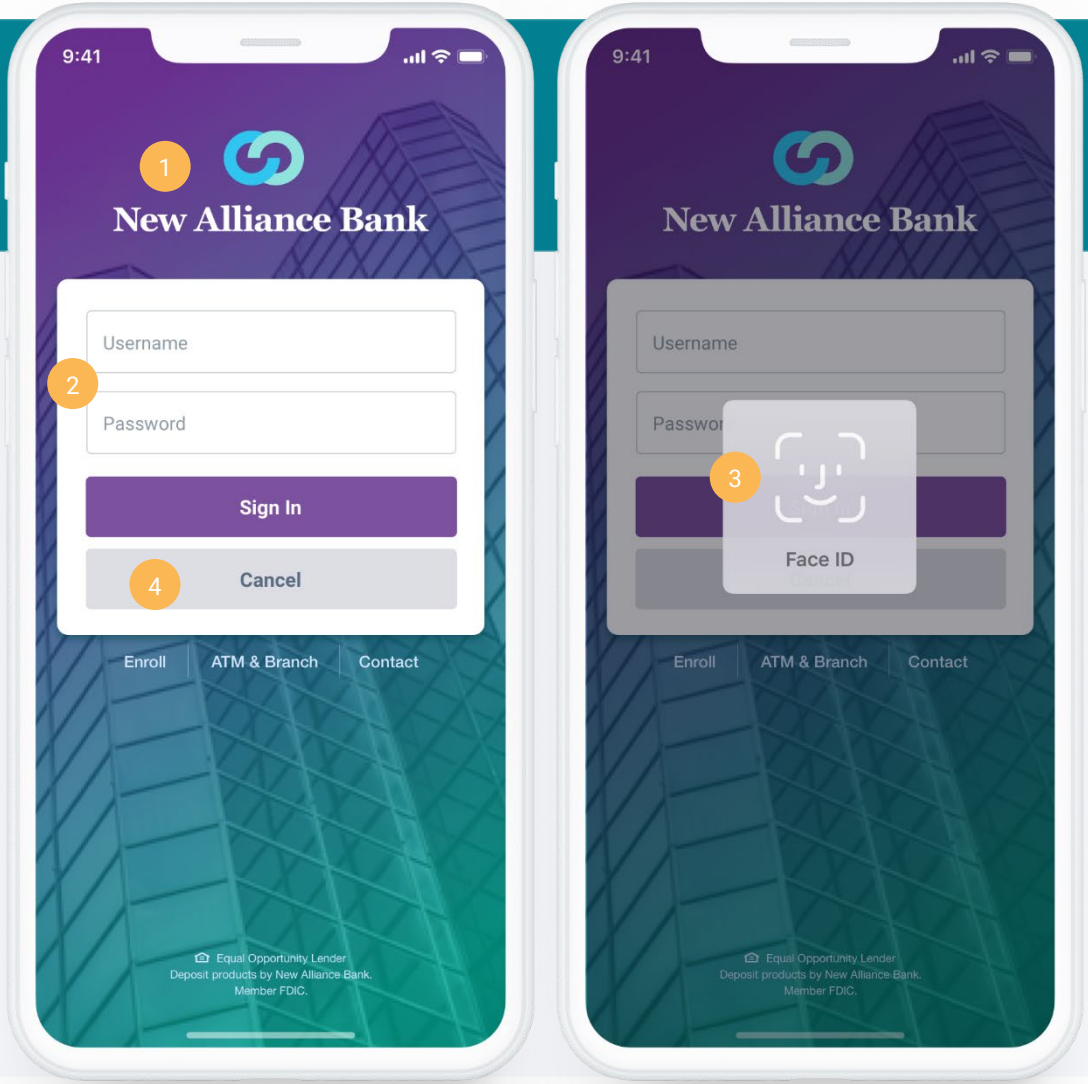
Required

- Provide a way for the end user to securely authenticate via the data provider user interface (e.g. online banking service)
  - Enable familiar and common UI patterns, as well as biometric authentication if the data provider online banking service supports this.
- Delegate authentication to the data provider using the tokenized access process defined by the Financial Data Exchange (utilizing the OIDC extension onto OAuth2.0)
- If authentication is aborted by the end user or fails, provide a path back to the data recipient with an error code with description





Authenticate | Sample User Content



Authenticate

Provide a familiar and easy way for the user to authenticate with the data provider's user interface.

1. Show familiar data provider login page with background and logo
2. Authenticate directly with data provider
3. Allow biometrics when available
4. A path to exit the flow without logging in

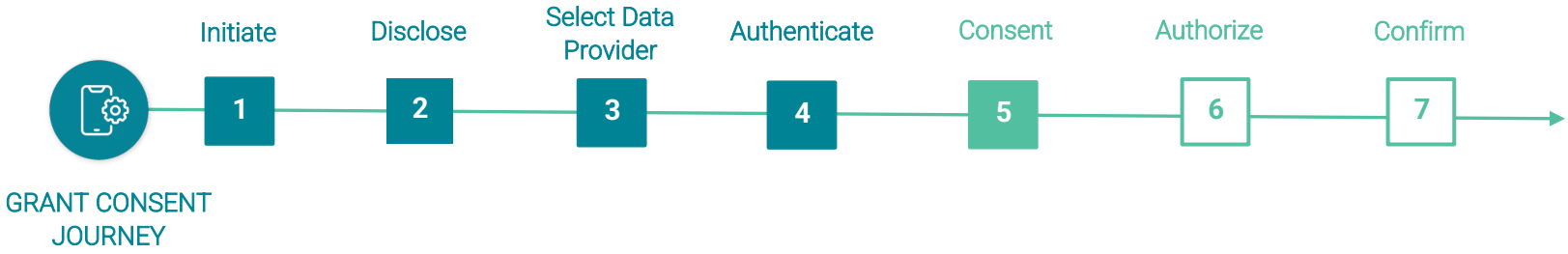
5 Consent

Purpose — Communicate what financial data elements will be shared with the data recipient and for how long

This step allows the data provider to inform the user what data the data recipient is going to request from the provider.

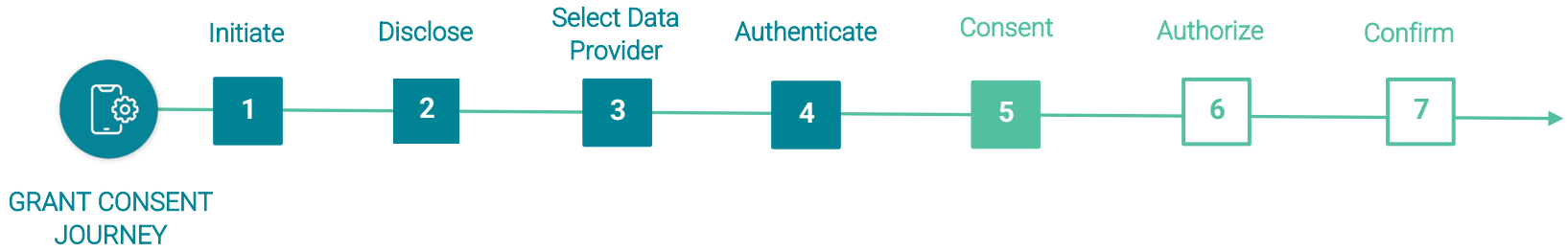
Required

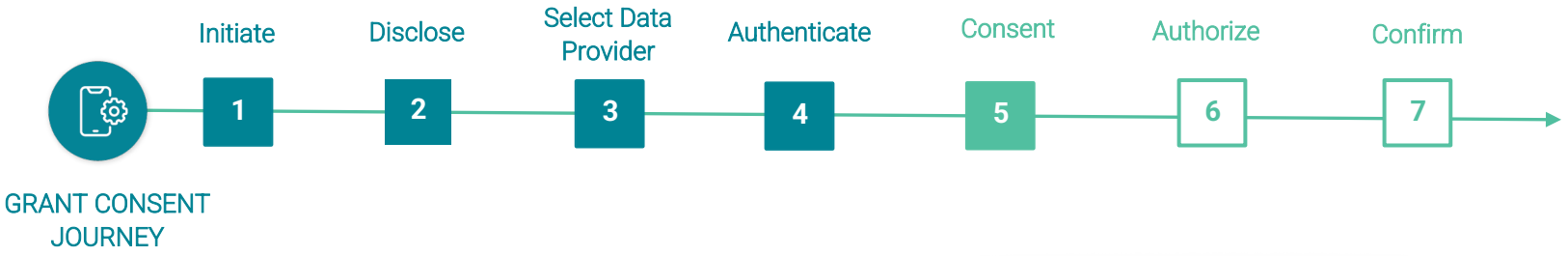
- Clearly identify the data recipient with which data is going to be shared, including data recipient name, as well as any data access platform, if applicable, so that the end user is fully aware with whom they are sharing their data
- A clear summary of what data clusters will be accessed, or shared, written in familiar terminology for the end user (e.g., account balances, transaction details, account statements)
    - Put most sensitive or important data at the top of the list for clear visibility to the end user
    - This must be consistent with context provided by the data recipient during the disclosure
- Include how long this data will be shared with the data recipient, as in the Disclose step
- Provide a path to exit the flow, such as a cancel button, if the end user decides not to share their data
- A call-to-action (CTA) should convey the result of continuing.
    - If account authorization occurs in a separate step, simply using “Continue” or “Next” is adequate
    - However, if this call-to-action is combined with authorization, use terminology such as “Authorize” or “Confirm”



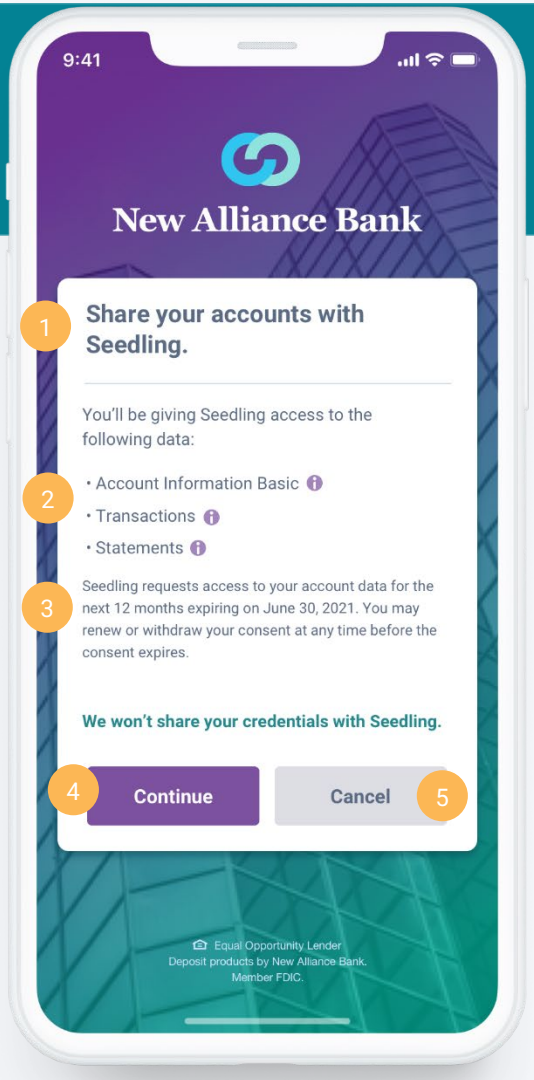
Recommended

- Provide click-down to specific data elements on each data type listed, in a similar manner as on the data recipient disclosure step
    - Provide a description of the minimum data that is being requested by the Data Recipient
- Clearly indicate that the consent to access and share the specified data is happening on these data provider screens, while maintaining visibility of the data recipient to orient the user
- Inform the end user of sensitive data that will **not** be shared with the data recipient
    - Remind users that their username and password will **not** be shared with the data recipient or data access platforms involved
- Indicate what will happen next
- Include the data recipient logo and data access platform logo, if applicable,
- Employ familiar and common UI patterns for expanding information
    - For example, ⓘ to open a tool tip or a **v** to display more details inline
- Consider combining Scope with Authorize in order to provide information in as succinct and clear manner as possible





Consent | Sample User Content



Consent

Clearly explain the exact items the user is consenting and what will happen next.

1. Clearly identify the recipient
2. Provide a clear summary of the data clusters that will be accessed, ideally with the ability to view more details
3. State how long this consent will be active
4. A clear call to action (CTA)
5. A path to exit the flow without consent

6 Authorize

Purpose — Enable selection of accounts and authorize data sharing

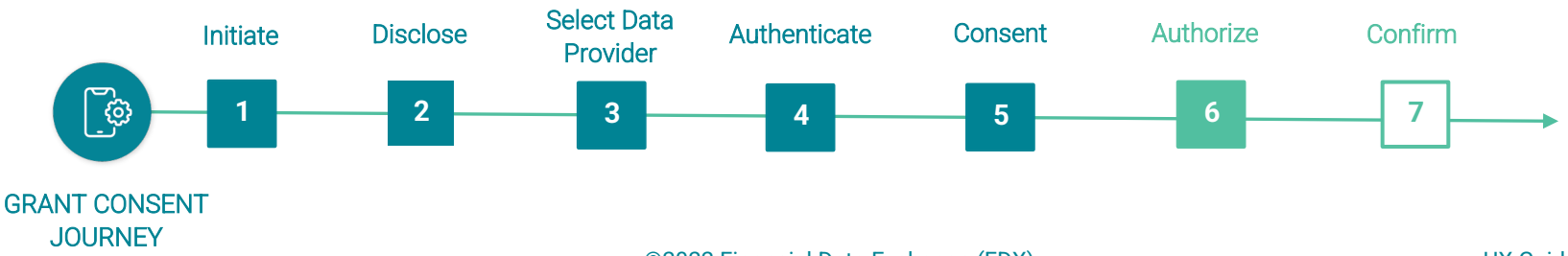
This step allows the end user to specify to the data provider exactly which accounts they authorize under the consent to share with the data recipient. This is handled by the data provider so that any accounts not authorized by the end user will be withheld from exposure to the data recipient.

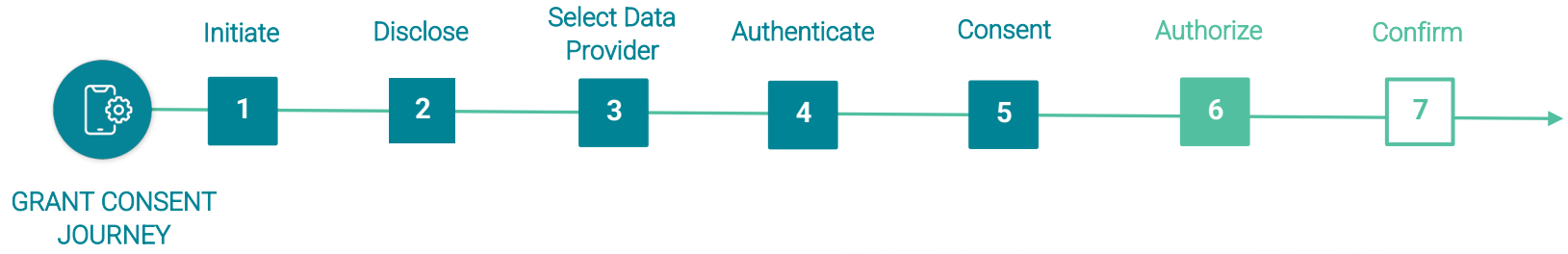
Required

- Clearly display the data recipient who will be requesting data from the chosen accounts
- Display all of the user's accounts at the data provider that are available through the authentication credentials
- The end user must have control to select which accounts to share; however, the data provider has discretion to determine whether to default to preselected or unselected in the initial presentation
- A call-to-action must clearly communicate that the action will authorize data sharing
    - Use terminology such as "Authorize" or "Confirm"
- A message to the user that this access can be modified at any point the future, including where
- Inform the end user that, upon completion, they will be logged out of the data provider and returned to the data recipient

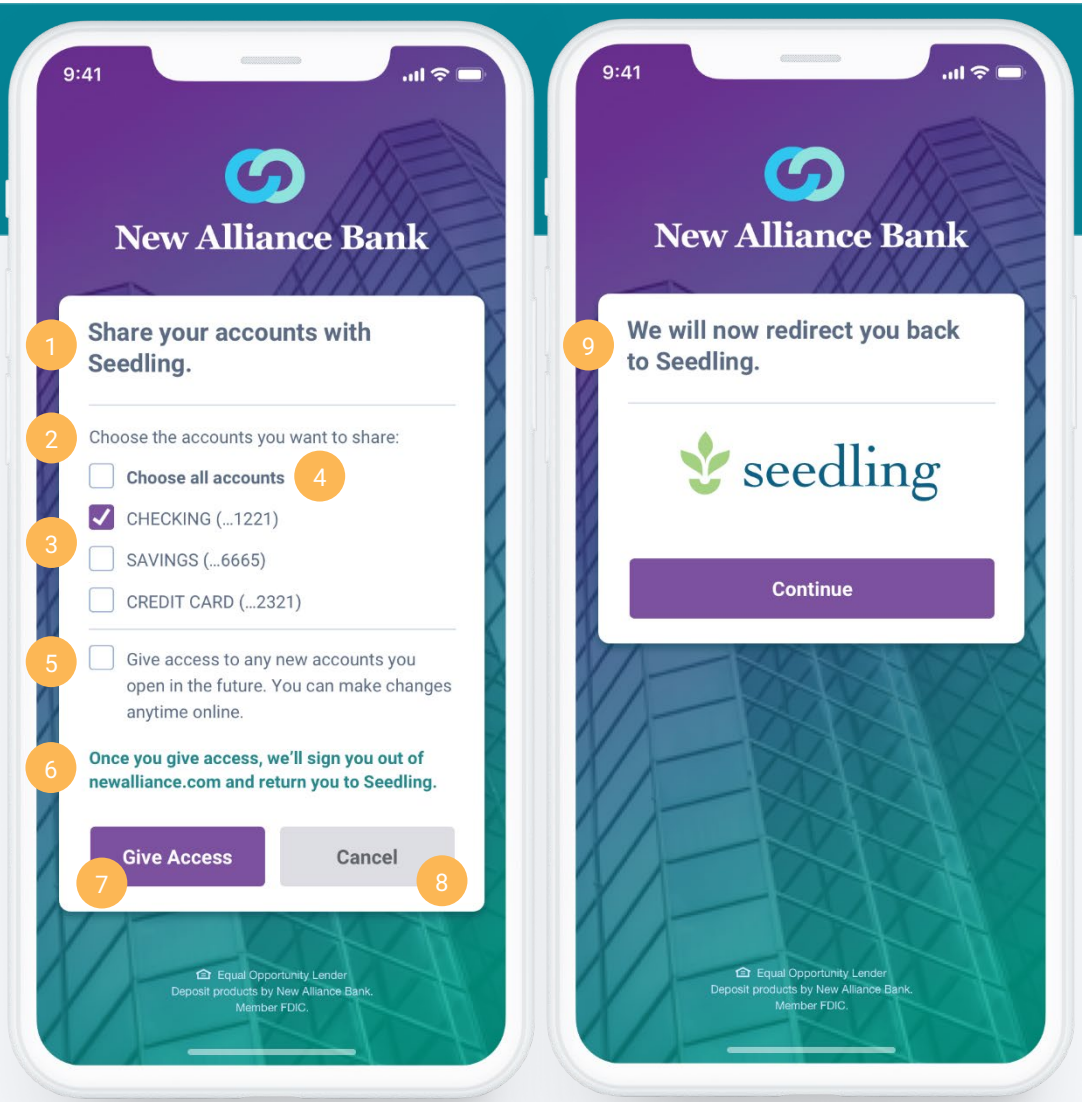
Recommended

- Use check boxes to allow the user to select which accounts to share
    - Select all / deselect all controllers may be used when the list of accounts is long
- Include an option to automatically share new accounts with the authorized consent
- Clearly indicate the time duration that this consent will be active (persistent, time-based, or one-time use) and any actions the end user may take to change this
- Indicate what will happen next
- The end user has the ability to share what is available and applicable for the business purpose
- When redirecting the end user to the data provider, use a temporary page/screen to inform the end user that they are being redirected





Authorize | Sample User Content



Authorize

Display all of the accounts that the data recipient could access and give the user control over which accounts to authorize.

1. Clearly show the data recipient who will be accessing these accounts
2. Show the list of eligible accounts to share
3. Provide an easy way to select which accounts will or will not be shared with the data recipient
4. Provide a quick way to select all accounts to be shared
5. Optionally, provide a way to automatically authorize future accounts to be shared with this data recipient
6. Inform the end user that, upon completion, they will be logged out of the data provider and returned to the data recipient
7. Provide a clear call to action
8. A path to exit the flow without consent
9. Clearly inform the end user that they are going to be redirected to the data recipient, ideally using a separate page

7 Confirm

Purpose — Indicate that data sharing is now authorized and confirm to the end user that they have returned to the data recipient

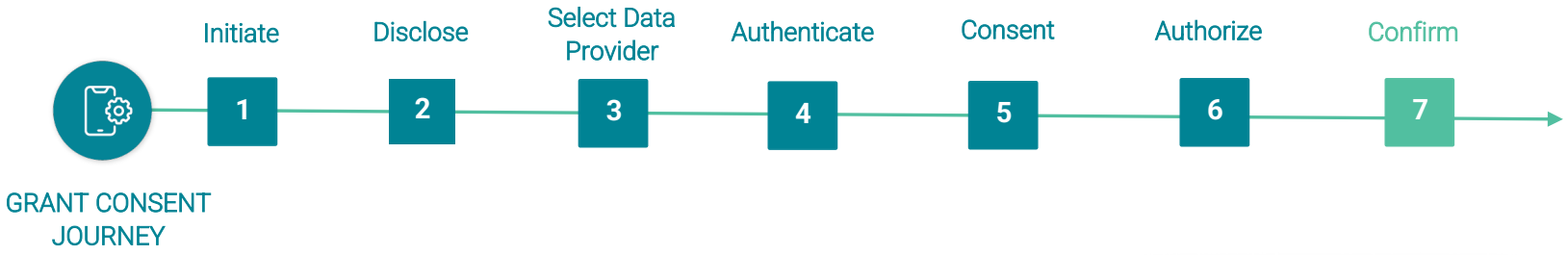
This step acknowledges to the end user that they have been redirected to the data recipient and that the access has been successfully established, or provides information why it has not.

Required

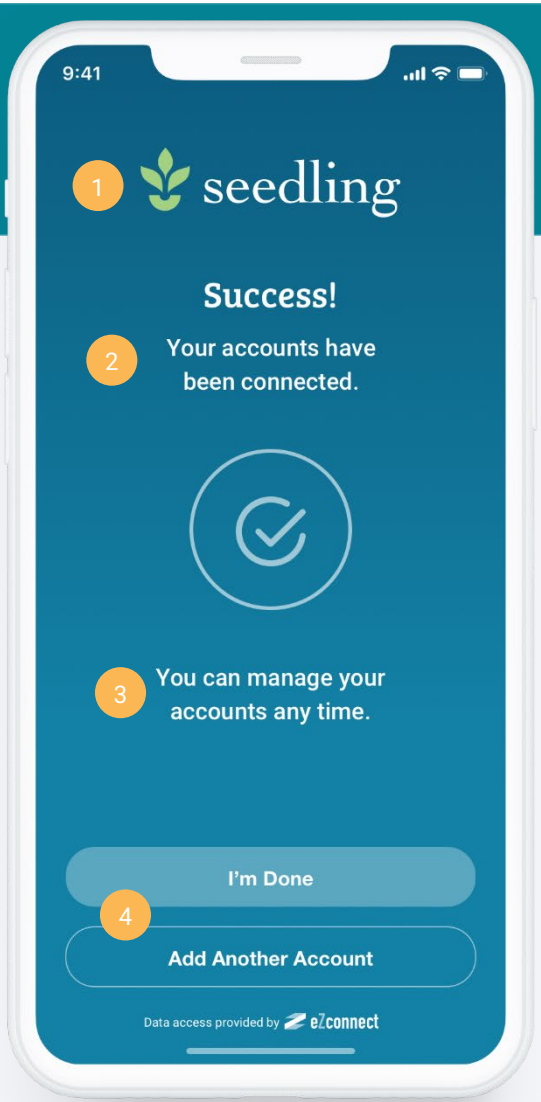
- A clear indication that the consent has been granted and that data sharing has commenced
- Confirm to the end user that they have been redirected to the data recipient if they successfully authorized the consent at the data provider
- If the process was aborted by the end user or fails, the data provider must provide an error code with a description to the data recipient so that the data recipient can describe to the end user what went wrong
- Communicate that end users can manage this consent
- Provide a path to add another data sharing consent

Recommended

- Data provider should provide an alternate notification to the end user (such as email) that the consent has been granted, to whom and scope of consent so that the end user has record of this action



Confirmation | Sample User Content



Confirmation

Give a clear indication that the data sharing consent has been established and that the journey is complete. Provide a way for the user to return to the data recipient application.

1. Clearly indicate that they have returned to the data recipient
2. Indicate success or reason for failure, if applicable
3. Provide an indication that this can be updated by the end user
4. Provide direction for next steps

Journey | Money Movement Consent

The Money Movement use case allows the Data Recipient to be able to access certain money movement capabilities provided by the Data Provider. In this use case, the Data Recipient is providing a service that requires the ability to execute a payment or transfer of funds such as payments to a Data Provider product (e.g., credit card or mortgage, etc.), adding payees, paying external bills, person-to-person payments, or transferring funds between deposit accounts. Such capabilities may be considered potentially risky and, as such, the end user must be made aware of what they are authorizing.

It's important to note that granting consent to use the Data Provider payments and transfers capabilities is not the same as executing the actual transaction. The end user must first consent to allow the Data Recipient to access the payment and transfers functionality and related data. At a later time the end user may decide to execute a payment or transfer via the Data Recipient.

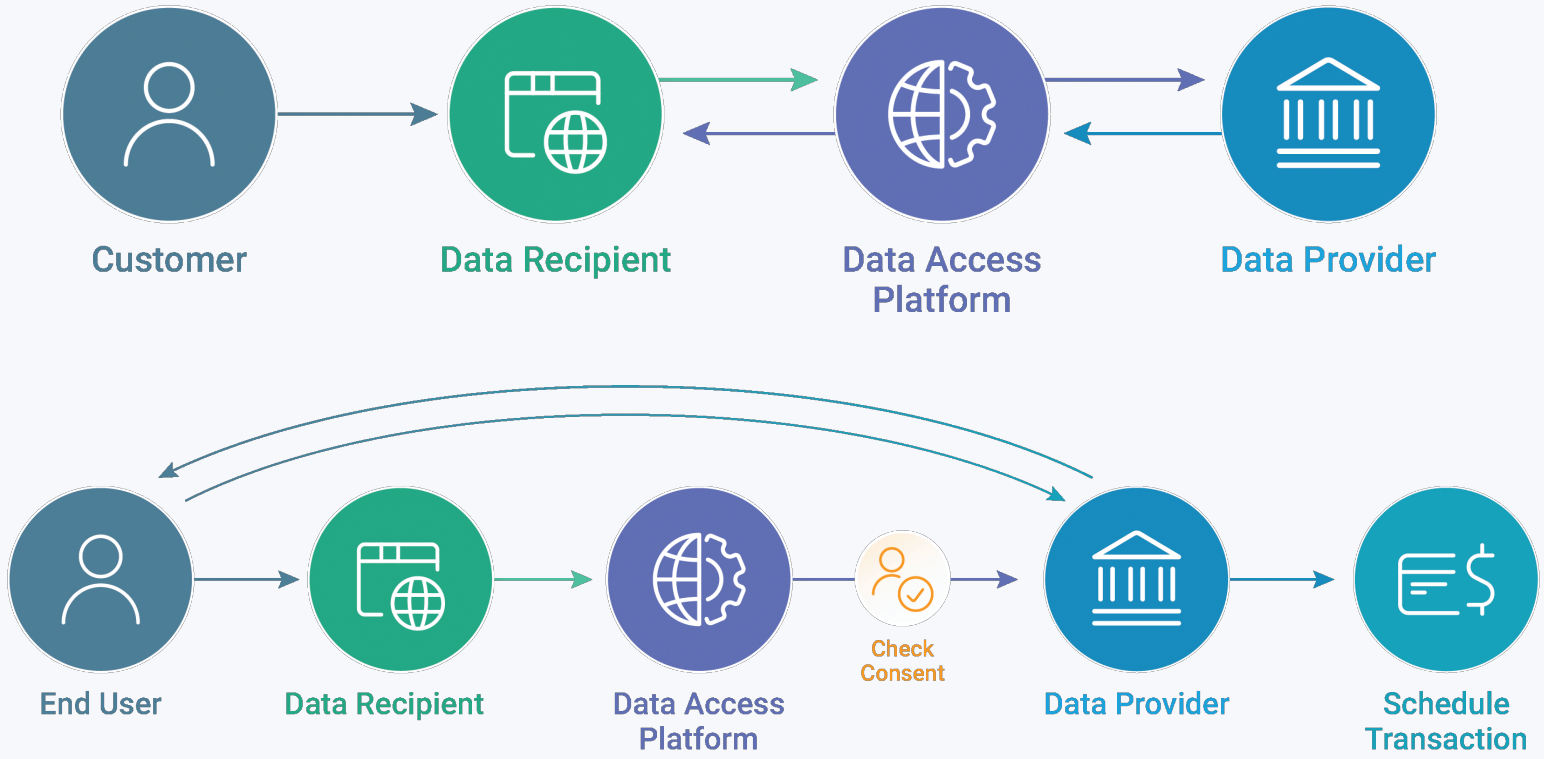
Once the consent has been granted, the end user is able to schedule payments or transfers and view related payment activity at the Data Recipient via FDX APIs. In some case, a Data Provider may require a step up authentication when scheduling a payment or transfer from the Data Recipient. The data cluster granted during consent allows the Data Recipient to use the APIs but the execution method is beyond the scope of this document.

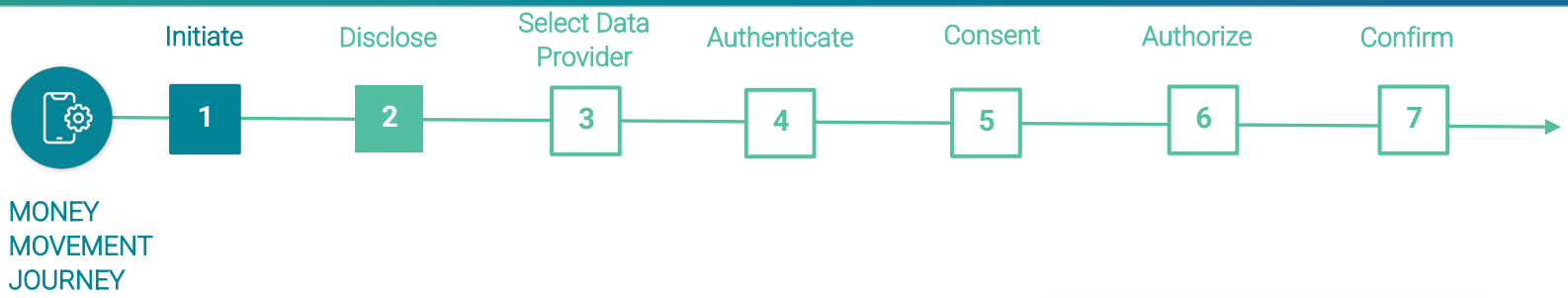
This section solely describes the Disclose and Consent steps of a money movement journey as they differ slightly from the standard grant consent journey above.

Money Movement Consent Journey

Similar to the Grant Consent Journey, the Money Movement Consent Journey consists of seven process steps.

A money movement consent may consist of the following entities and data flows:

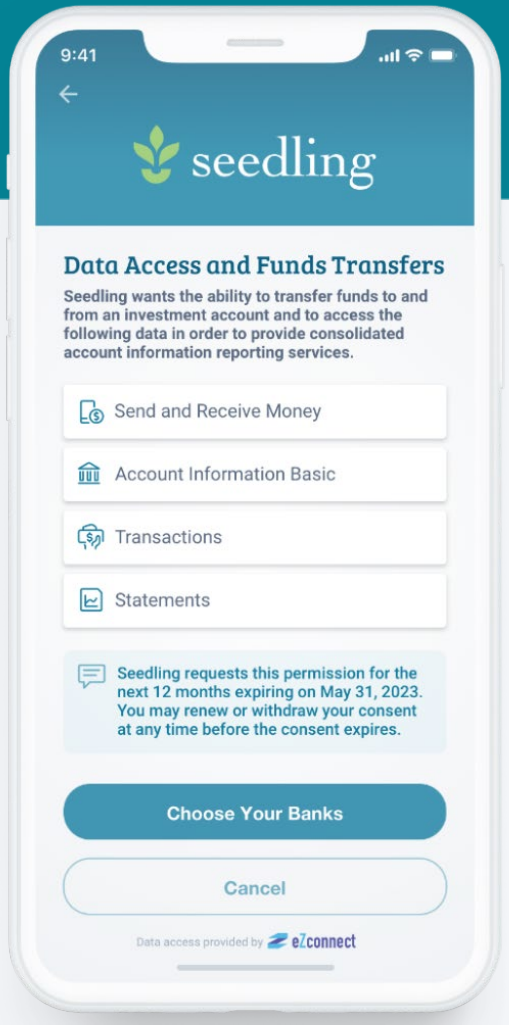




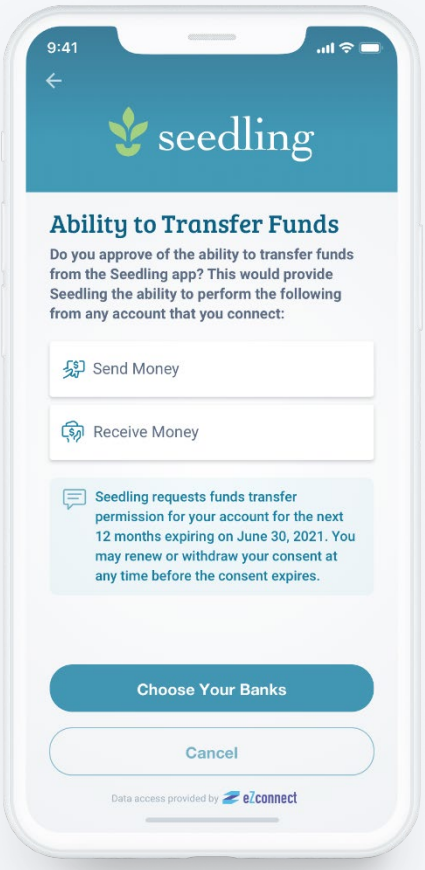
Disclose | Sample User Content

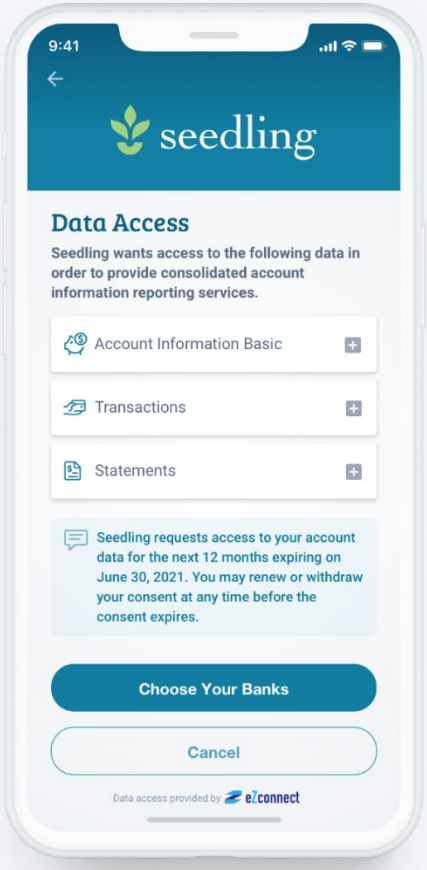
Following the same guidelines as the standard data sharing Consent Grant journey, the Data Recipient must explicitly communicate in the Disclose step that, in addition to the other data, they need to access the **money movement capabilities**, as shown here.

An optional Disclose implementation example is shown below.



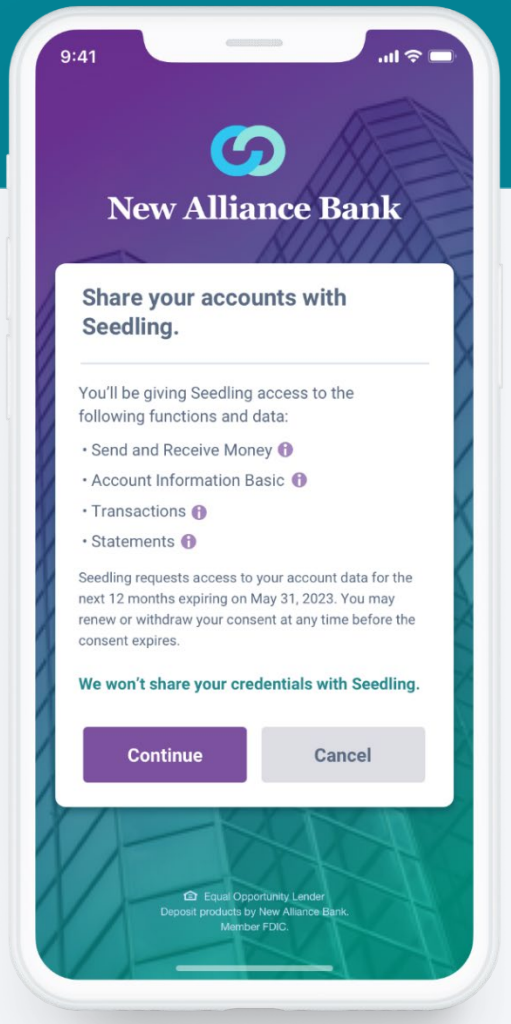
A separate Disclose screen for money movement is an **optional** implementation, such that it appears before or after the data cluster screen for data sharing. This ensures that the user will not miss the vital money movement disclosure and provides a clear separation of concepts between data sharing and money movement. The decision to use one or two screens is at the discretion of the implementor.





Consent | Sample User Content

Likewise, the Data Provider must also inform the end user that this consent includes access to specific **money movement capabilities** during the Consent step. A specific message must be shown that clearly indicates they are **enabling the transfer of funds** (or other payment capabilities) through the Data Recipient, thus providing the transparency and control that the end user deserves.



Section 4: Post Consent

This section describes user notification and consent management requirements.

Notification

Purpose – Enable End Users to have confirmation of authorizing data sharing with a Data Recipient and a consistent experience across open banking applications

Providing a durable notification back to the End User via a previously established out-of-band mechanism, such as email, provides additional assurance to the End User of completion of the authorization for data sharing and gives an opportunity for End Users to identify unauthorized or unintended access requests. The notification also delivers a consistent verification experience across the industry and with other consumer services.

Required

- It is the responsibility of the Data Provider to send a notification to the End User via the communication channel selected by the End User. The involved Data Access Platform or Data Recipient may also provide notification.
- If the Data Provider does not allow a choice of communication channel, or if a choice has not been selected by the End User, the default is to send an email notification.
- The content of the notification to the End User must:
    - Identify the name of the Data Recipient that has been authorized to access the data
    - Provide the date when the End User provided consent to the Data Provider to authorize data access for the Data Recipient. For security, the date should be included in the main body of the notification
    - State that the end user's login credentials will not be shared with the named Data Recipient
    - State the duration of the data access that has been authorized based on the duration of consent that has been specified (e.g. persistent, time-based, or one time)
    - Provide information on where the End User can review their data access authorizations, for example, directions on how to manage the consent, such as a consent dashboard.
- Data Recipients and Data Access Platforms should provide the following information in a Terms of Use/Data Sharing Policy that is accessible to the End User
    - An explanation of the data security practices implemented so that the End User is assured that their consent information and other sensitive data collected is kept safe and protected from fraudulent access
    - An explanation of data sharing and privacy so that the End User knows if the Data Recipient/Data Access Platform will or may sell/share their data
- Notify the End User when they have successfully revoked Consent

Recommended

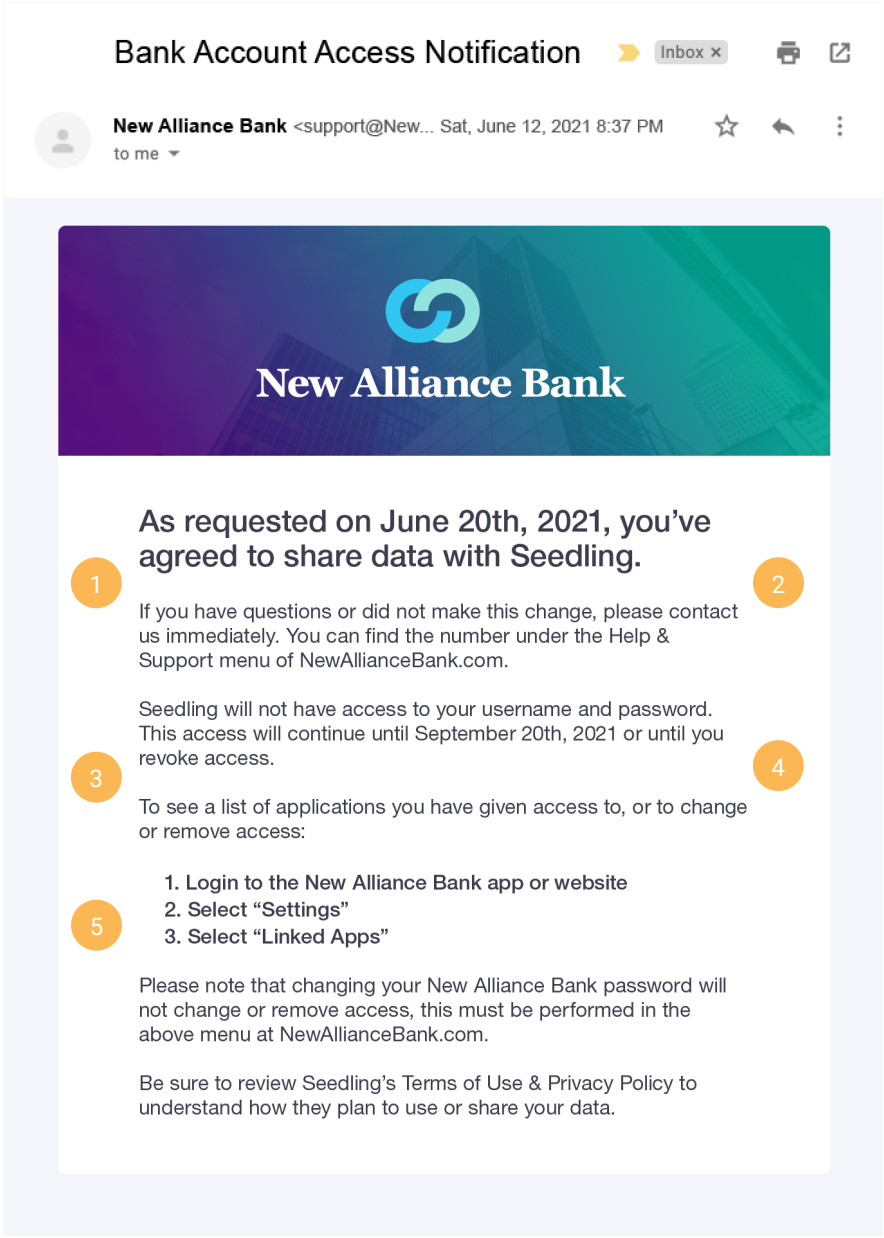
- Data Provider may allow an option for the End User to choose the notification delivery method including:
  - Email
  - Text message
  - Push notification to their Data Provider application
- The content of the notification to the End User:
  - May choose to indicate that changing their password will not revoke access
  - Does not need to include details of the lists of accounts selected or the data clusters being shared.

Notification | Sample User Content

Notification

Provide a notification to the End User via email, text, or push notification that states the End User has authorized data sharing.

1. Identify the name of the Data Recipient that has been authorized to access the data
2. Provide the date when the End User provided consent to the Data Provider to authorize data access for the Data Recipient. For security, the date should be included in the main body of the email.
3. State that their online banking login credentials will not be captured or stored by the named Data Recipient
4. State the duration of the data access that has been authorized based on the duration of consent that has been specified (e.g. persistent, time-based, or one time)
5. Provide directions on where the End User can review their data access authorizations, for example, directions to find the dashboard within their online banking service (for security reasons do not include a hotlink to the dashboard).



Consent Management and Dashboards

Purpose – Once consent has been granted to share data from a Data Provider to a Data Recipient, the End User should have the ability to manage that consent.

Overview

Data Providers and Data Recipients must provide a software interface for End Users to view, edit, and revoke Consent.

> **Note**: Data Access Platforms acting as a Data Recipient are included in this requirement. Data Access Platforms not acting as a Data Recipient may provide similar capabilities as they see fit. Any Data Access Platform that provides an interface should use the Data Recipient examples as a guide.

This interface is referred to herein as a Consent Dashboard. This section describes the requirements that should be met for the Consent Dashboard of each entity.

A vital component to user experience is the ability to manage consent via a consent dashboard. The required functionality that must be provided to users is described herein. Also of vital importance to implementers is to ensure that all parties are notified of **any change** to a consent via the FDX Consent API.

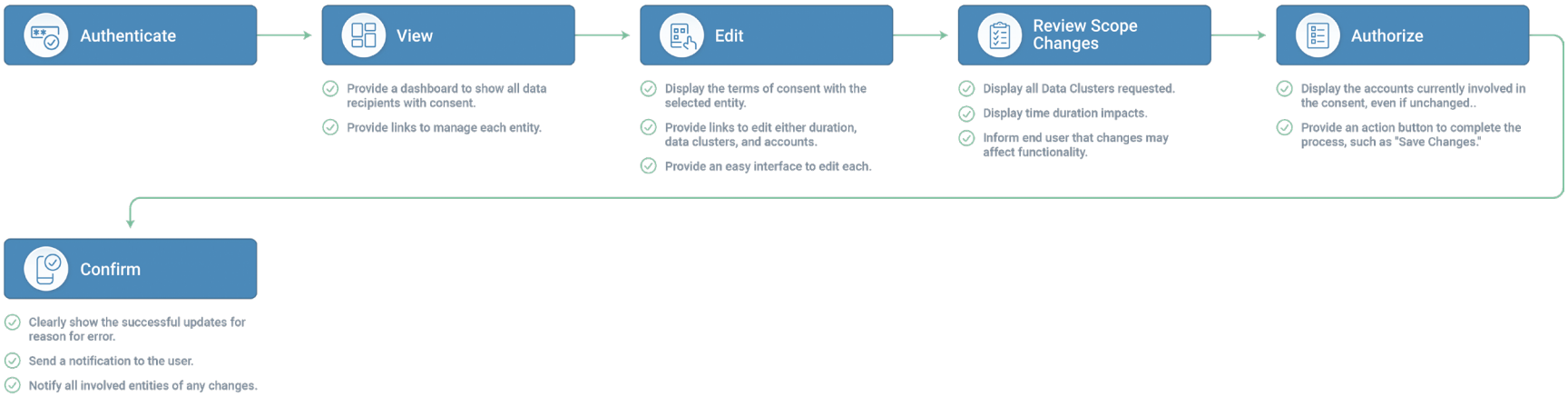
Entity Notification

Independent of end user notification, parties must notify each other of certain events. Regardless of where the Consent modification originates, the entity capturing the Consent change request should implement a mechanism to notify all other parties of the change. It is also desirable that the entity verify that all notified entities have acknowledged the notification. The notified parties should act upon the notification and take any necessary actions to ensure that the end-user receives a consistent user experience, and that there is transparency and traceability of any change actions.

Consent Editing Journey

Any changes to a consent should result in the end user reviewing the scope changes, authorizing all involved accounts, and confirming the changes.

Edit Consent Journey (from Data Provider)



If changes originate from a Data Recipient, the end user may need to repeat steps of the original Consent Journey, for example if a new Data Provider must be selected. Ensure that the end user is redirected to the appropriate place in the consent journey after making a change to a Consent.

Note: All parties must be notified of any changes to consent via the Consent API.

Data Provider

View Consent from a Data Provider

View Consent

End Users should be able to view the following from a Data Provider Consent Dashboard:

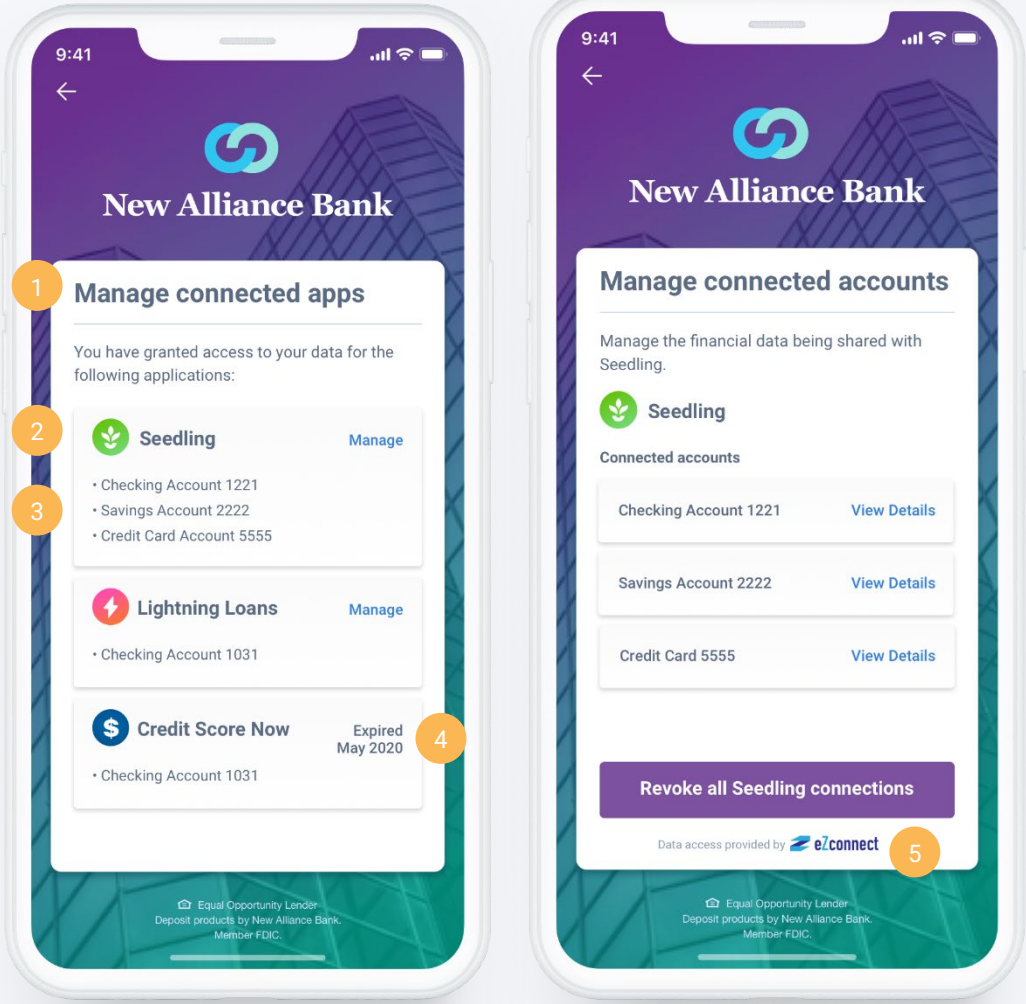
- The entities with which the data is being shared.
    - It should be indicated if one or more Data Access Platforms have access to the End User's data, along with the names of any Data Access Platforms involved in the Consent. Provide access to additional information about the Data Access Platform and its role, including links if possible.
- The duration of Consent specifying the exact date that the Consent will expire, along with the date that the current Consent was granted. If the Consent was renewed, then the date of renewal should be displayed as the date the Consent was granted.
- The accounts authorized under the Consent.
- The data items (clusters) that are being shared for the accounts authorized under the Consent. These should be specified in language that is clear to the End User and a lay person, such as "transactions" or "statements".
- The Consent Dashboard should be accessible at all times.
- Prior Consents or a link to prior Consents that have expired or have been revoked within a timeframe consistent with the Data Provider data usage policy should be displayed, along with the date of expiration/revocation.

Consent Dashboard – Data Provider | Sample User Content

View Consent

End Users should be able to view the following from a Data Provider Consent Dashboard:

1. The Consent Dashboard should be accessible at all times.
2. The entities with which the data is being shared.
3. The accounts authorized under the consent.
4. Prior Consents or a link to prior Consents that have expired or have been revoked should be displayed, along with the date of expiration/revocation.
5. Specify any Data Access Platforms that have access to the End User's data and the names of any Data Access Platforms involved in the Consent. Provide access to additional information about the Data Access Platform and its role, including links if possible.

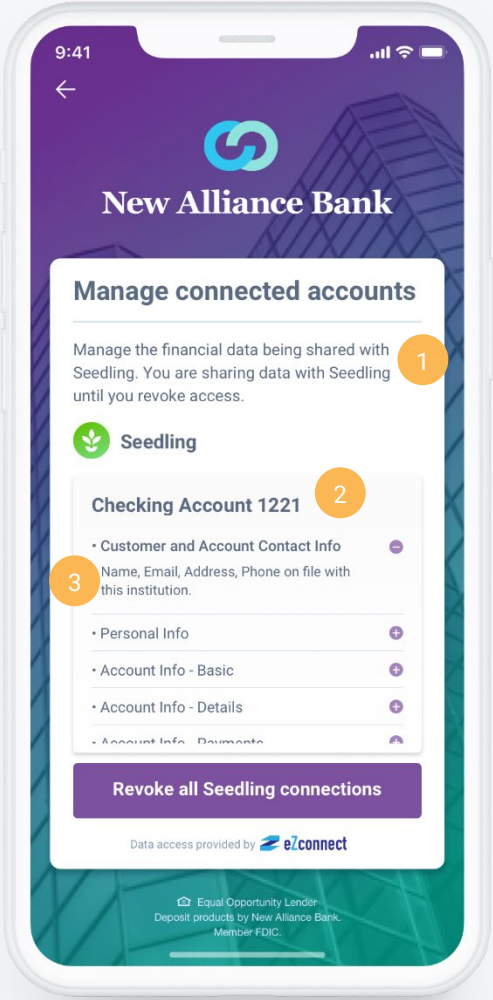


Consent Dashboard – Data Provider | Sample User Content

View Consent

End Users should be able to view the following from a Data Provider Consent Dashboard:

1. The duration of Consent specifying the exact date that the Consent will expire, along with the date that the current Consent was granted. If the Consent was renewed, then the date of renewal should be displayed as the date the Consent was granted.
2. The accounts authorized under the consent.
3. (Optional) Specify items in the Data Cluster



Edit from a Data Provider

The following functionality should be provided to end users for editing the scope of a consent. Users will have to complete certain steps in the Consent Journey after making changes in order to fulfill the scope change. Within a Data Provider flow, the Consent Dashboard should be considered an editable version of a Consent screen.

All edits to a Consent require a final **acknowledgement** from the end user. The end user should be clearly notified of the changes being made to the Consent with an option to **approve** or **cancel**. The Consent API should be used to notify all involved parties of any changes to a Consent, whether user-initiated or system-initiated.

End User Initiated Changes

Increases of Scope

- Add an account
- Extend/renew the consent
- Change a time scope/duration-based consent to a persistent consent (if applicable)
- Enhance the look back period (e.g. 3 months to 1 year)

Decreases of Scope

- Remove an account (sole owner)
- Remove an account (joint owner)
- Provide standing instructions on addition or removal of an account, for example an automatically add new accounts check box on an account selection screen
- Reduce the time scope/duration of consent, for example from Persistent to time-based
- Reduce the look back period, for example from 1 year to 3 months

System Initiated Changes

Increases of Scope

- An authorized user opens a new account
- A new account type is available
- The Financial Institution changes name (via new branding, merger, or acquisition)
- The End User undergoes a legal name change

Decreases of Scope

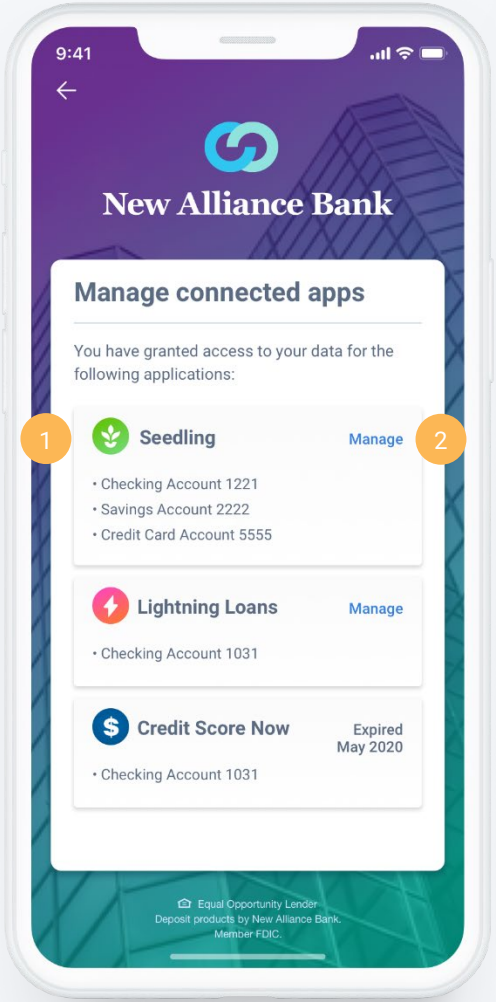
- An account owner removes access for another end user who previously had access, such that the other end user no longer has access to the account. This could occur in a a joint, authorized or delegated end user situation.
- The account is closed by the financial institution
- An end user closes the account
- The authorized user (delegate) has a change in permissions on an existing account, for example if the delegated user no longer has an explicit permission to the account but still has read/view access to transactions
- A reduction of API capabilities that affect the consent (example - statements no longer provided)

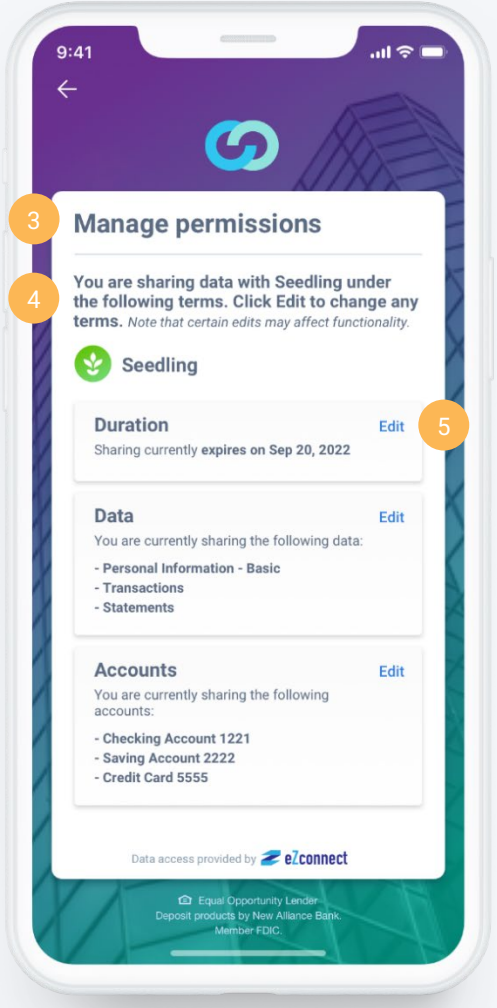
Consent Dashboard – Data Provider | Sample User Content

Edit Consent

End Users should be able to view and perform the following edits from a Data Provider Consent Dashboard:

1. The entities with which the data is being shared.
2. A link to manage the access for any specific entity.
3. An interface to view and edit the terms of the Consent.
4. An explanation that certain edits may affect functionality.
5. A way to make changes to each editable portion of the Consent, such as duration, data clusters, and accounts.





Revoke from a Data Provider

Revoke

End Users should have the following revoke functionality from a Data Provider Consent Dashboard:

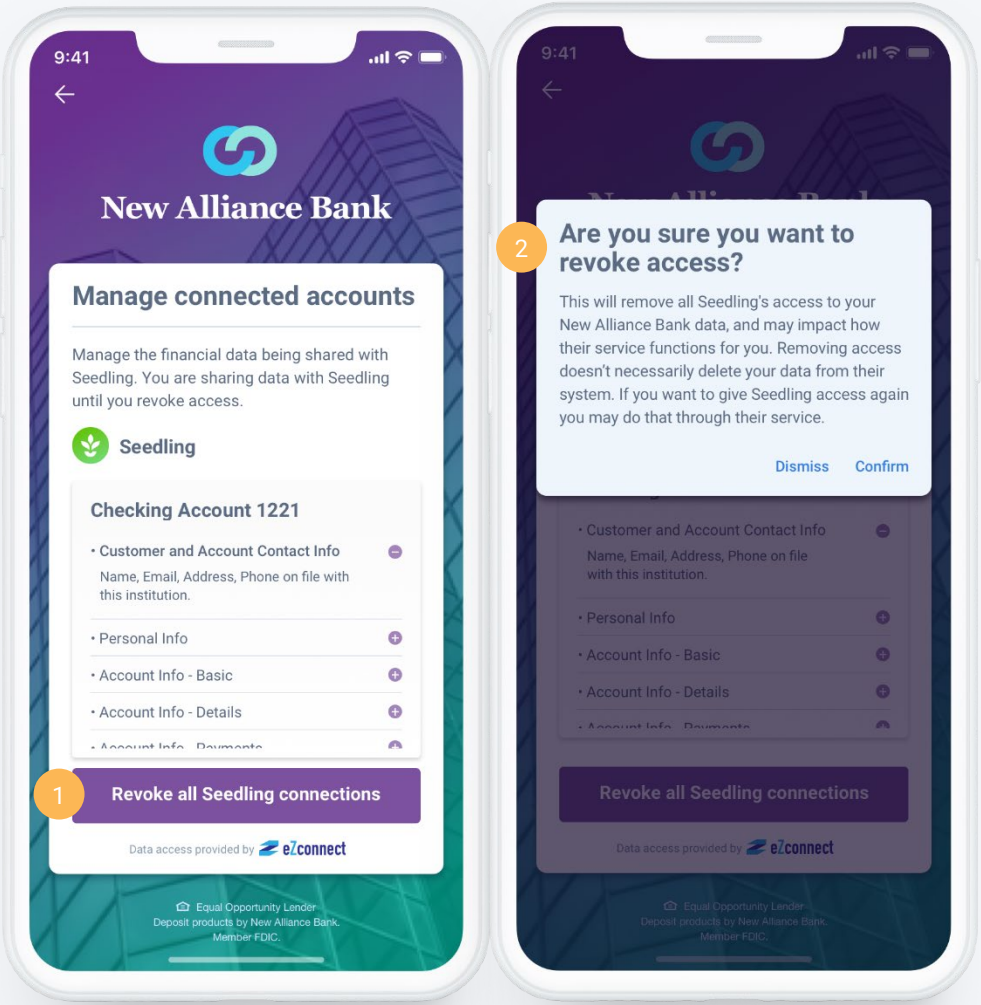
- Immediately revoke all access to their data from any specific entity
- Revoke all access from a specific Data Recipient and each Data Access Platform involved in the Consent
- Before revoking Consent to their data, notification should be provided to the End User that clearly explains the impact revocation will have on the services, such that the End User receives a full understanding of the impact to the services.
- (Optional) The ability to immediately revoke all access to their data from all entities at once

Consent Dashboard – Data Provider | Sample User Content

Revoke Consent

End Users should be able to perform the following from a Data Provider Consent Dashboard:

1. Immediately revoke all access to their data from the specific entity
2. Include a confirmation step before revoking the Consent. Before revoking Consent to their data, notification should be provided to the End User that clearly explains the impact revocation will have on the services, such that the End User receives a full understanding of the impact to the services.



Data Recipients

View Consent from a Data Recipient

View Consent

End Users should be able to view the following from a Data Recipient Consent Dashboard:

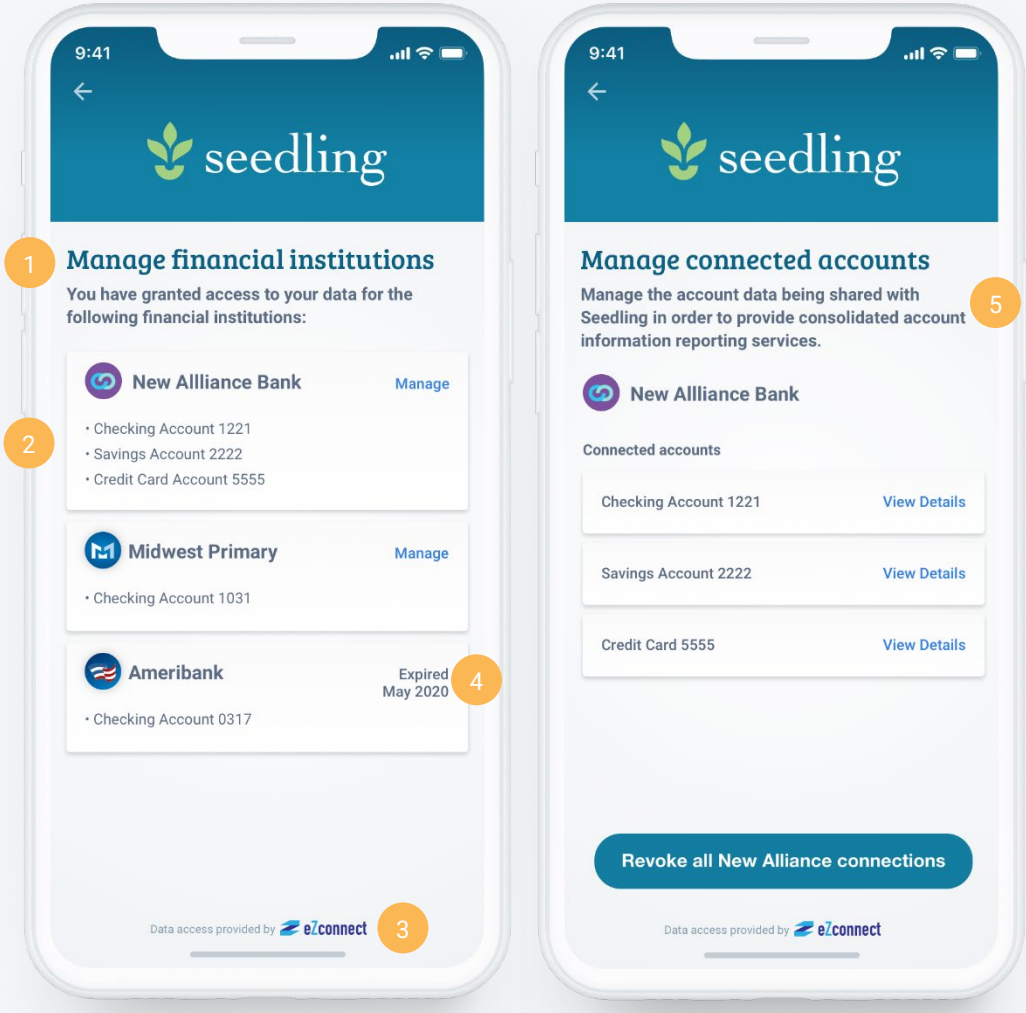
- The Data Provider and what accounts have authorized under the Consent.
- If a Data Access Platform is involved:
    - It should be indicated if a Data Access Platform has access to the End User's data and the names of all Data Access Platforms involved in the Consent or sharing of data. Provide access to additional information about the Data Access Platform and its role, including links if possible
- The business purpose of the Consent, which was provided at the time of consent, such as budgeting or a mortgage application.
- The duration of Consent specifying the exact date that the Consent will expire (if time-based), along with the date that the current Consent was granted. If the Consent was renewed, then the date of renewal should be displayed as the date the Consent was granted.
    - (Optional) Provide a notification if it will become necessary to renew Consent at some point in the future, and implications if the End User does not
- The most recent date/time that the Data Recipient accessed data via this Consent
- The data items (clusters) that are being shared for the accounts authorized under the Consent. These should be specified in language that is clear to the End User and a lay person, such as "transactions" or "statements".
- Prior Consents that have expired or have been revoked within a timeframe consistent with the Data Recipient data usage policy, along with the date of expiration/revocation.
- The Consent Dashboard should be accessible at all times.
- If a consumer has authorized all accounts or new accounts to automatically be added when they initially grant consent, then those accounts will appear listed under the account section.
- If a Data Access Platform is part of the Consent, the end user should be able to navigate to the Data Access Platform to revoke any relevant Data Recipient access to their data

Consent Dashboard – Data Recipient | Sample User Content

View Consent

End Users should be able to view the following from a Data Recipient Consent Dashboard:

1. The Consent Dashboard should be accessible at all times.
2. The Data Provider and what accounts have authorized under the Consent.
3. Any Data Access Platforms that have access to the End User's data and the names of any Data Access Platforms involved in the Consent. Provide access to additional information about the Data Access Platform and its role, including links if possible.
4. Prior Consents or a link to prior Consents that have expired or have been revoked should be displayed, along with the date of expiration/revocation.
5. The business purpose(s) of the Consent that describes why the information is being shared, which was described at the time of consent, such as Budgeting or a Mortgage Application

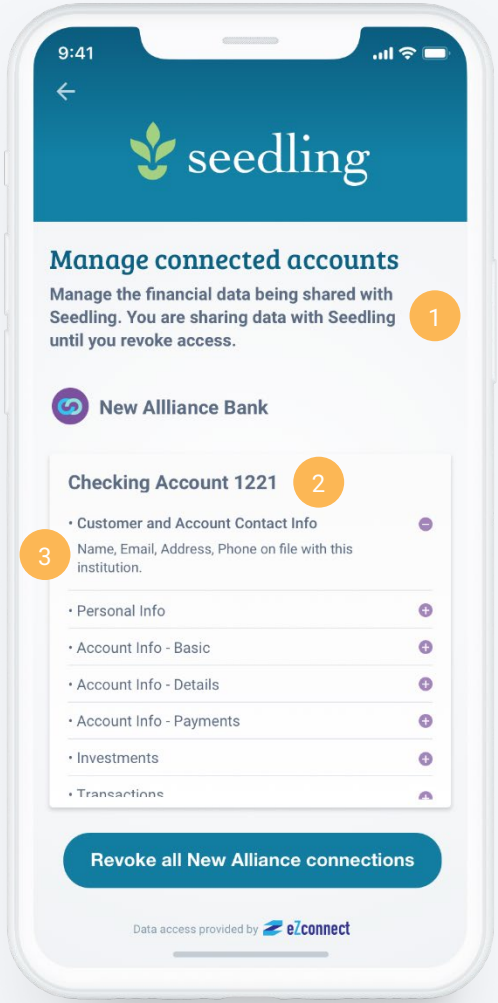


Consent Dashboard – Data Recipient | Sample User Content

View Consent

End Users should be able to view and perform the following from a Data Recipient Consent Dashboard:

1. The duration of Consent specifying the exact date that the Consent will expire, along with the date that the current Consent was granted. If the Consent was renewed, then the date of renewal should be displayed as the date the Consent was granted.
2. The accounts authorized under the consent
3. (Optional) Specify items in the Data Cluster



Edit from a Data Recipient

The following functionality should be provided to end users for editing the scope of a consent. Users will have to complete certain steps in the Consent Journey after making changes in order to fulfill the scope change.

All edits to a Consent require a final **acknowledgement** from the end user. The end user should be clearly notified of the changes being made to the Consent with an option to **approve** or **cancel**. The Consent API should be used to notify all involved parties of any changes to a Consent, whether user-initiated or system-initiated.

End User Initiated Changes

Increases of Scope

- Add an account
- Add a non-account resource e.g., customer information or payments/ an action that can occur on a resource, provisioning of Bill Pay Services, tax statement download
- Add data scopes/clusters (non sensitive) e.g. Transactions, Balances, Rewards
- Add data scopes/clusters (sensitive) e.g., Account Owner Data (PII), Account Number
- Extend/ renew the consent
- Change a time scopes/ duration based consent to a persistent consent
- Enhance the look back period (e.g. 3 months to 1 year)

Decreases of Scope

- Remove an account (sole owner)
- Remove an account (joint owner)
- Remove a non-account resource e.g., customer information or payments/ an action that can occur on a resource, provisioning of Bill Pay Services, tax statement download
- Remove data scopes/clusters ***(The system of record is held at Data Recipient)***
- Reduce the time scopes/ duration of consent (e.g. Persistent to time-based) ***(The system of record is held at Data Recipient)***
- Reduce the look back period (e.g. 1 year to 3 months)

System Initiated Changes

Increases of Scope

- Data provider change causes error that requires end user to re-consent
- Enhanced API capabilities affect data elements that have already been consented.
- Statements are not authorized via API, but later becomes accessible (enhanced API)

Decreases of Scope

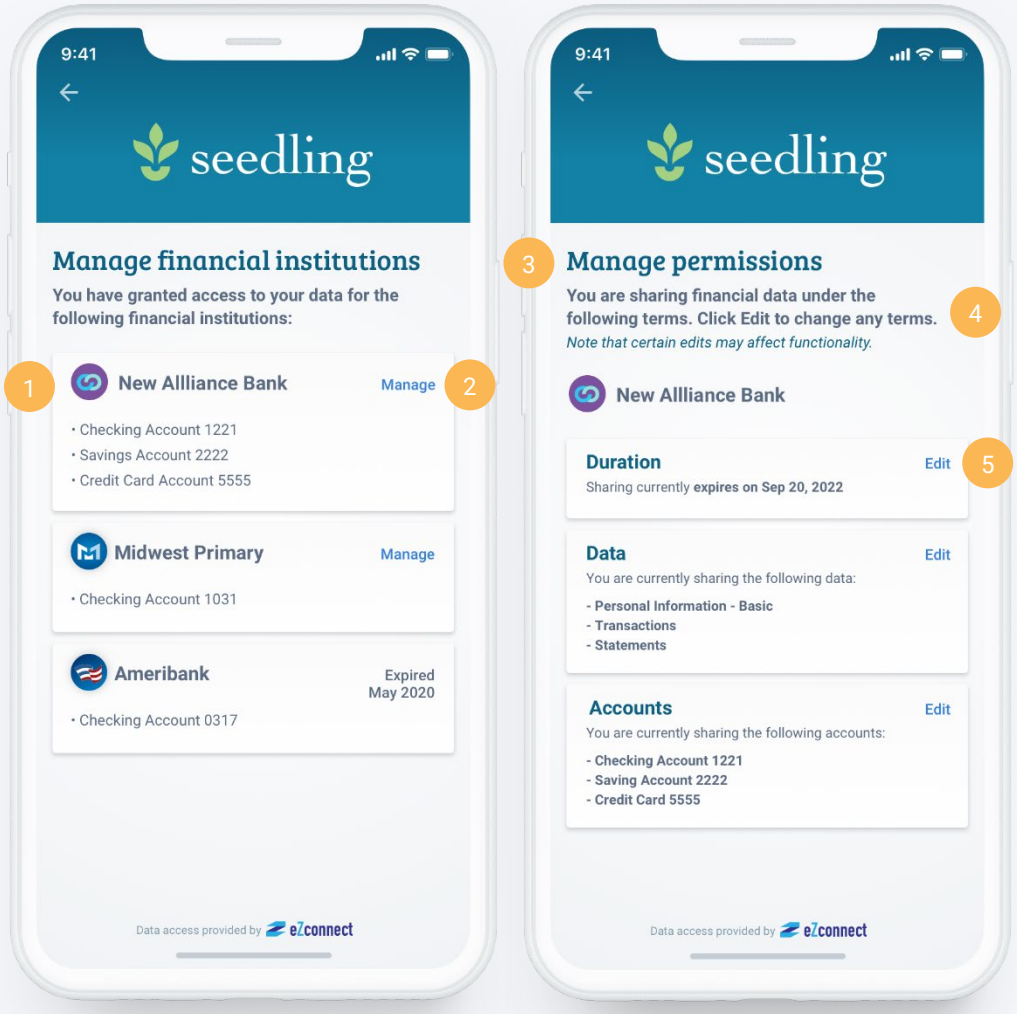
- Data provider change causes error that requires end user to re-consent. *MFA auth / password change / IT Policy / Expired Token

Consent Dashboard – Data Recipient | Sample User Content

Edit Consent

End Users should be able to view and perform the following from a Data Recipient Consent Dashboard:

1. The entities with which the data is being shared.
2. A link to manage the access for any specific entity.
3. An interface to view and edit the terms of the Consent.
4. An explanation that certain edits may affect functionality.
5. A way to make changes to each editable portion of the Consent, such as duration, data clusters, and accounts.



Revoke from a Data Recipient

Revoke

The process of revocation should be easy and straightforward for the End User, without barriers to opt out of future consent (no questions asked).

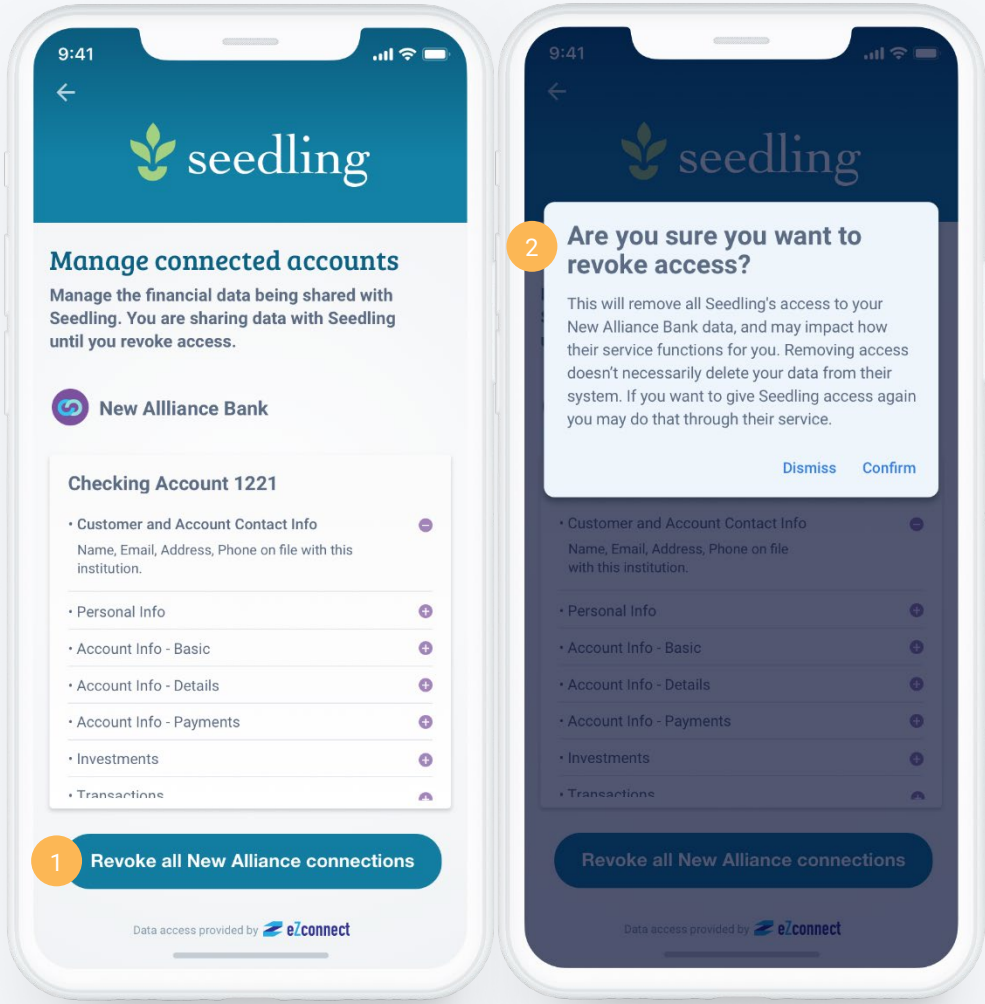
End Users should have the following revoke functionality from a Data Recipient Consent Dashboard:

- Immediately revoke all future access to their data from the Data Recipient.
- Any revocation of Consent should be passed to any and all Data Access Platforms and Data Providers involved in the Consent.
- Before revoking Consent to their data, notification should be provided to the End User that clearly explains the impact revocation will have on the services, such that the End User receives a full understanding of the impact to the services.

Revoke Consent

End Users should be able to view and perform the following from a Data Recipient Consent Dashboard:

1. Immediately revoke all access to their data, as well as from any other involved Data Recipients or Data Access Platforms. Any revocation of Consent should be passed to any and all Data Providers and parties involved in the Consent.
2. Include a confirmation step before revoking the Consent. Before revoking Consent to their data, notification should be provided to the End User that clearly explains the impact revocation will have on the services, such that the End User receives a full understanding of the impact to the services.



Appendix A: Topics for Further Review

The following topics have been identified as needing additional discussion. They will be addressed in later versions of this document after they have been vetted.

This list is not exhaustive. Additional items may be added as they are identified. The order of when they will be addressed is to be determined by the FDX User Experience Working Group. Please contact the UX Working Group if there are topics not listed here that should be addressed.

- Additional clarifications on the Consent flow
  - How long is the prescribed consent flow? Are there concerns about the customer experience through this flow?
  - Can accounts be preselected or should they be explicitly selected by the end user?
  - Considerations for automatically sharing accounts in the future
- Guidelines for end users to change/manage consent from the consent dashboards
- Data Clusters
  - Defining more data clusters
  - What granularity is needed in presenting data clusters to end users?
  - Special considerations for sensitive data, such as PII, DOB, SSN, etc.
  - Mapping data clusters to business purposes
  - Should specific content/phrases be prescribed for consistency?
  - How to handle changes to data clusters? When does a new element require re-consent?
  - Association of data clusters to APIs
- Duration of consent (all) - how to properly ensure communication to the end user by both the data provider and the data recipient
- Handoff/Redirecting – Discuss requiring indications to users when they are being redirected to Data Provider and back to Recipient.
- Journey Error Codes/Error state Journey – How are errors handled by the data provider, should redirects be provided, as well as cancel options.
- Required versus optional data clusters
- Consent for delegated users (subusers)
- Other notifications and/or receipts

- Specifying that access is secure and certified if legal, such as ”FDX Trusted” or “FDX Certified” mark
- How to properly address terms and conditions through the Consent flow
    - Whether or not, and how to include, links to privacy policies and data usage policies
    - Discuss application to de-identified/identified data
    - How long data is held/used after duration of consent ends or consent is revoked
- Re-consent
    - When is it required?
    - How should it be handled?
- Traceability and controls

Appendix C

Examples of Publicly Announced Data Sharing Agreements Featuring the FDX API

- CIBC to enhance secure and seamless access to financial tools and apps for clients through agreement with MX – **Aug 8, 2022**
- RBC and Plaid announce agreement to bolster client security and increase connection to financial services apps – **Jun 14, 2022**
- RBC and Envestnet Data and Analytics announce agreement to provide clients with greater control over their financial data – **Jun 14, 2022**
- FINICITY AND FISERV: SECURING THE OPEN BANKING ECOSYSTEM – **April 19, 2022**
- Fiserv and MX Enable Secure Consumer Financial Data Access to Accelerate Future of Open Finance – **Mar 21, 2022**
- Envestnet | Yodlee Collaborates with Intuit QuickBooks to Provide Financial Data Connections to Millions of Small Businesses – **Oct 13, 2021**
- PNC-launches-Akoya-solution-to-increase-the-security-of-connections-for-consumers-to-safely-transact-with-financial-apps – **Sept 30, 2021**
- 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**
- FINICITY AND GREEN DOT ANNOUNCE SECURE DATA ACCESS AGREEMENT TO DELIVER MORE ACCESSIBLE, SEAMLESS AND SECURE MONEY MANAGEMENT TO CUSTOMERS – **July 21, 2021**
- Wells Fargo joins the Akoya Data Access Network to advance API-based financial data aggregation – **June 22, 2021**
- Putting you in control of your personal data with a new API – **May 21, 2021**
- Plaid and U.S. Bank collaborate to deliver a secure open finance experience – **May 13, 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**
- Citi builds fintech marketplace – **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**
- **FINICITY AND FIDELITY INVESTMENTS JOIN FORCES ON CUSTOMER DATA SECURITY – September 27, 2018**
- **USAA Providing Safer, More Efficient Approach to Data-Sharing – July 2018**
- **Finicity Signs Data Agreement with JPMorgan Chase – July 10, 2017**
- **Bank of America preps data sharing service – May 26, 2017**
- **Finicity and Wells Fargo Ink Data Exchange Deal – April 4, 2017**

Appendix D

Known Development Portals

Wells Fargo: https://developer.wellsfargo.com/

Citi: https://developer.citi.com

US Bank: https://developer.usbank.com/

Capital One: https://developer.capitalone.com/products/customer-transactions

Amex: https://developer.americanexpress.com/open-banking
openbanking@devmail.americanexpress.com

Truist: https://developer.bbt.com/admin/app/home

PNC: https://developer.pnc.com/

Schwab: developer.schwab.com

Discover: Dev Center

Intuit: https://developer.intuit.com/app/developer/homepage

BofA: (invite only) http://dataservicesapi.bankofamerica.com/ds/ **BofA:**
aggregator.support@bankofamerica.com

Chase: (invite only) https://developer.chase.com/

Jack Henry (Banno): https://jackhenry.dev/

FIS: Code Connect: API Marketplace | FIS

FiServ: https://developer.fiserv.com/product/AllDataAggregation

Bank of Montreal (BMO) API Developer Portal bienvenue | API Developer Portal

Royal Bank of Canada (RBC): https://developer.rbc.com/

Akoya: https://recipient.ddp.akoya.com/login

FDX: https://developer.financialdataexchange.org/

FDX Registry: https://registry.financialdataexchange.org/