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

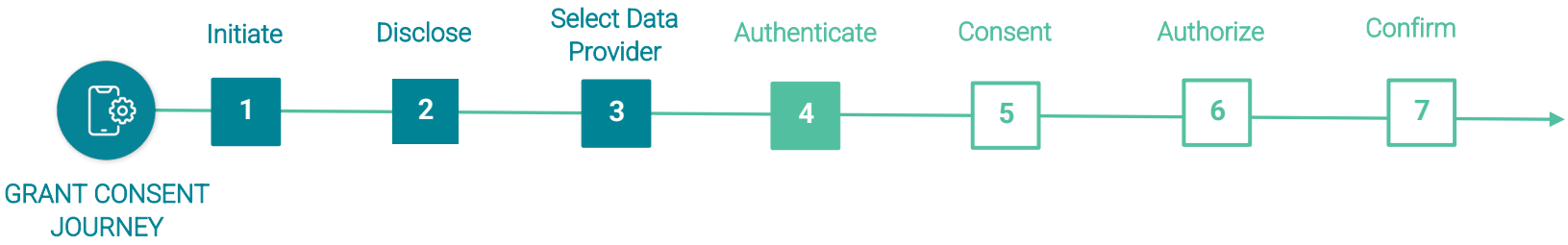
Please refer to the *FDX Taxonomy of Permissioned Data Sharing* document for a clear definition of recurring terms such as data provider, data recipient, data services platform, end user delegate, and end user.

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

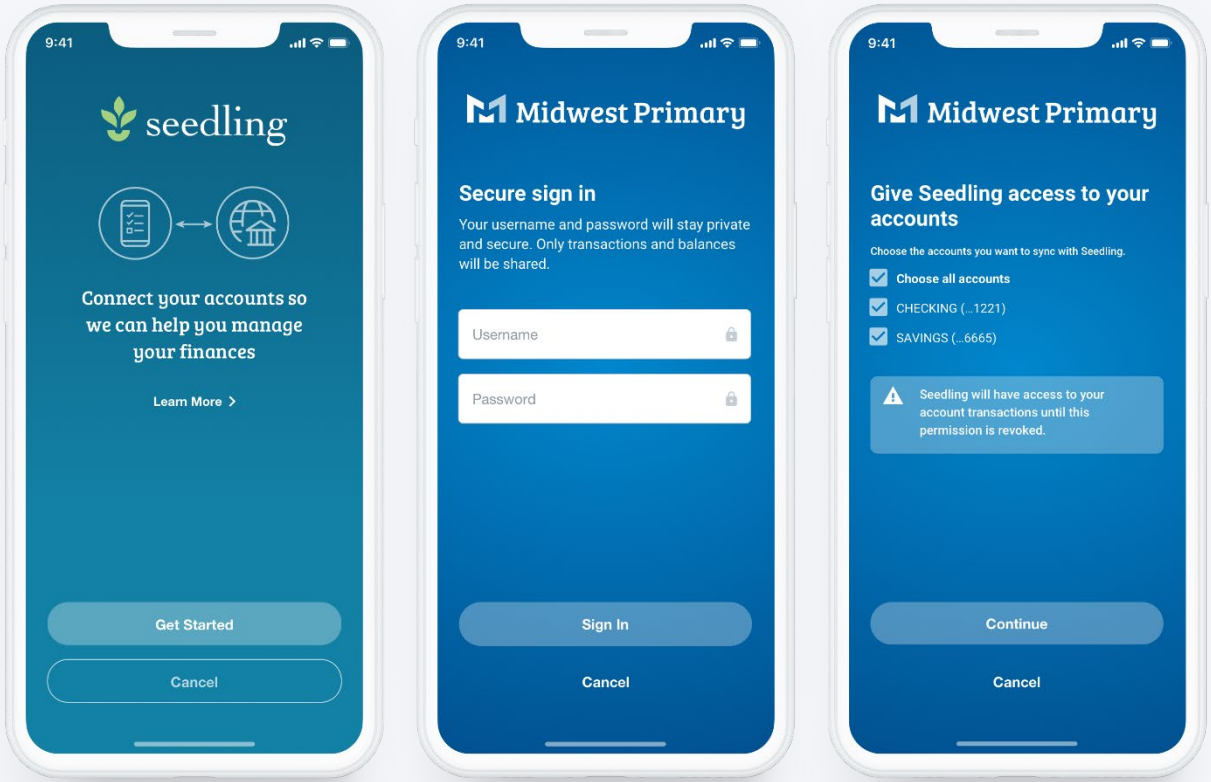
			• Due dates and interest rates
ACCOUNT_PAYMENTS	Read Only	Account information payments	• Full account and routing number • SWIFT or IBAN numbers
INVESTMENTS	Read Only	Account investment details	• Investment contributions • Investment loans • Pension data • Vesting and account holding details
TRANSACTIONS	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.

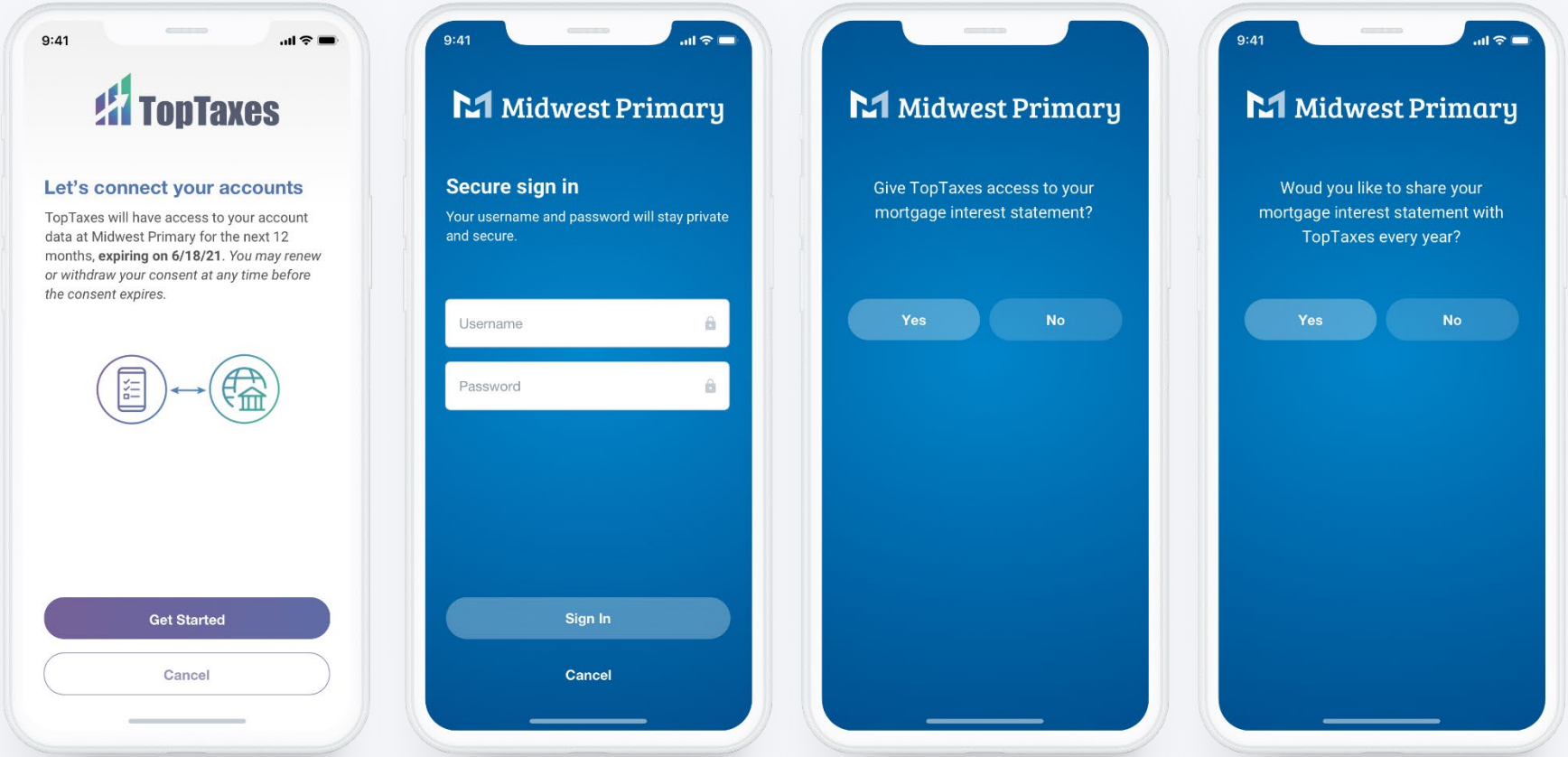


Sample Persistent Consent language

[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.



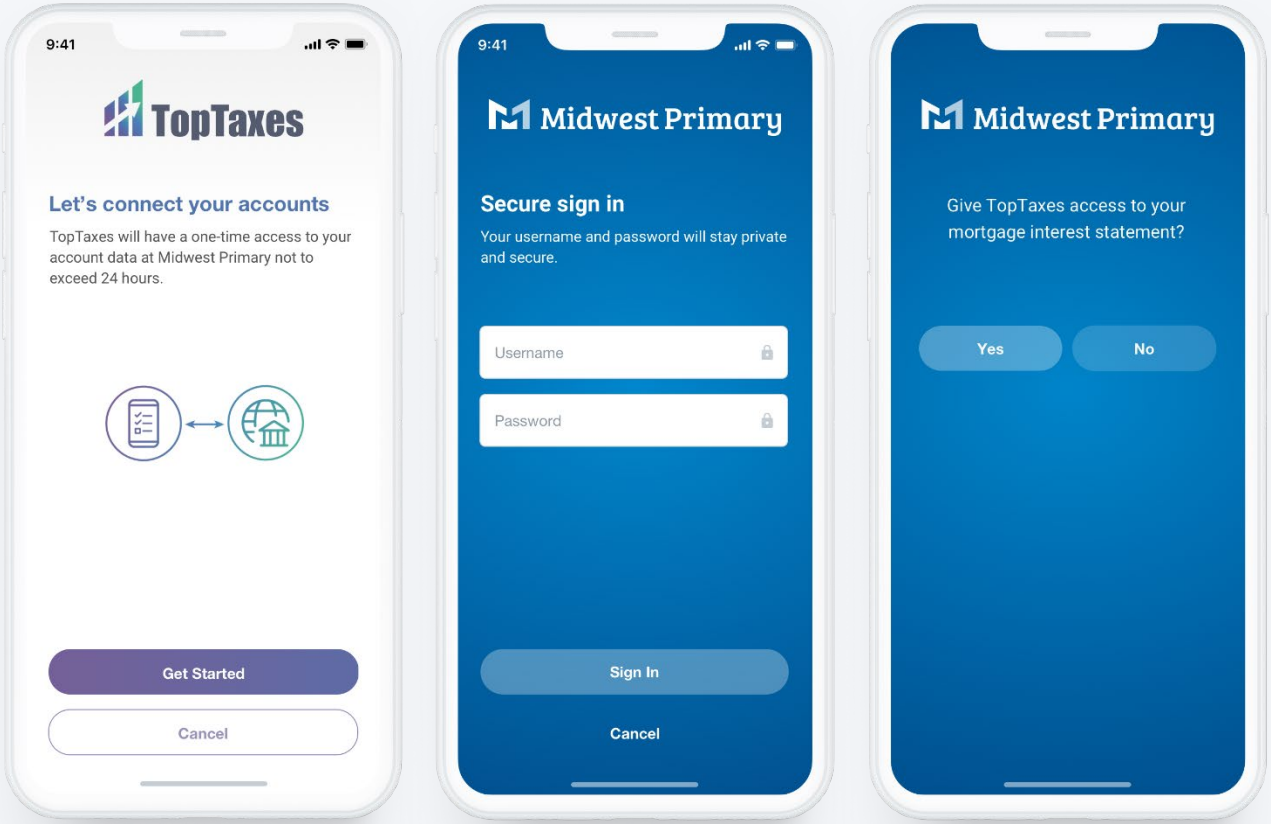
Sample Time-based Consent Language

[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

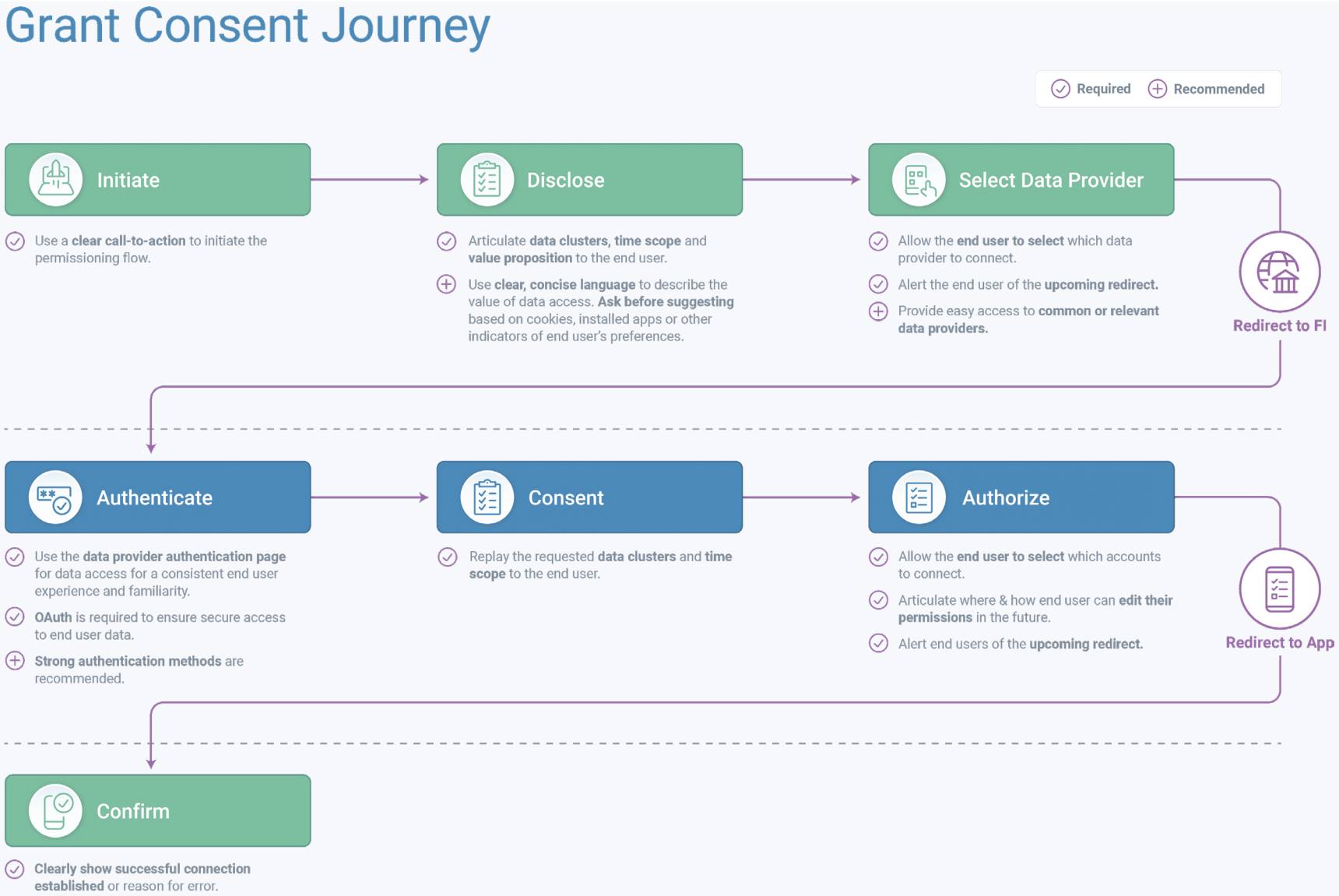
The prescribed journey shown below reflects the recommended information and functionality provided by the data recipient and the data provider. They are intended to show who is responsible for each but not necessarily indicative of the number of physical pages required by either the data provider or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

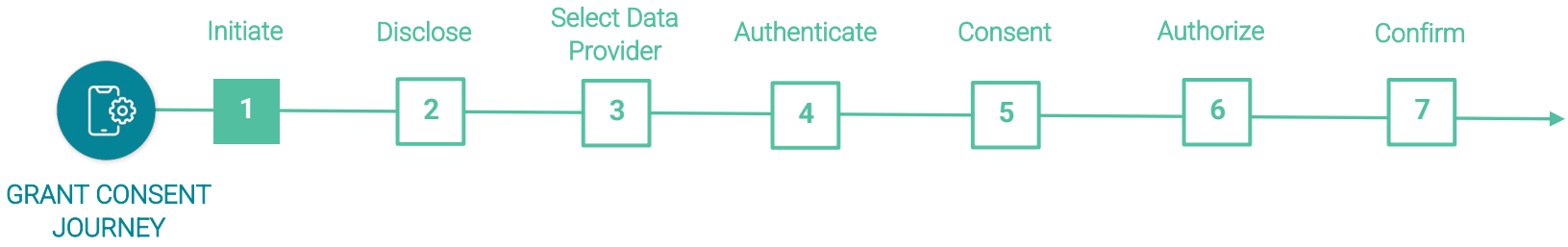
This step provides details about how the end user can share their data from a data provider to the recipient to provide the services requested. It is important that the end user is clear about the benefits of sharing their accounts and who is involved.

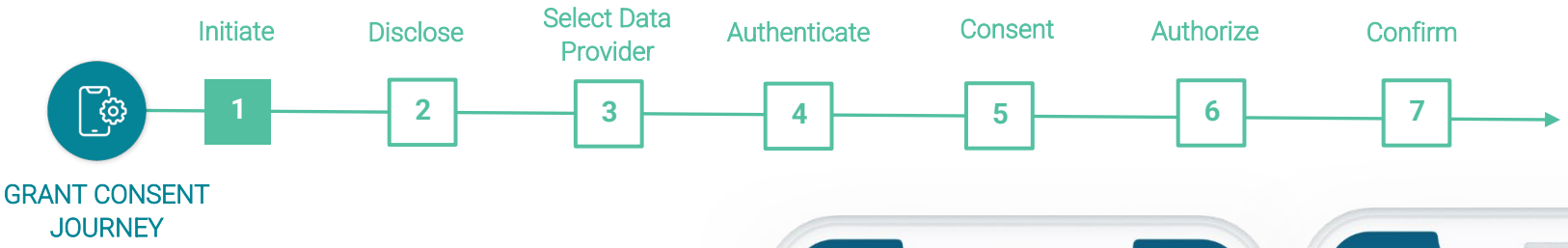
Required

- 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



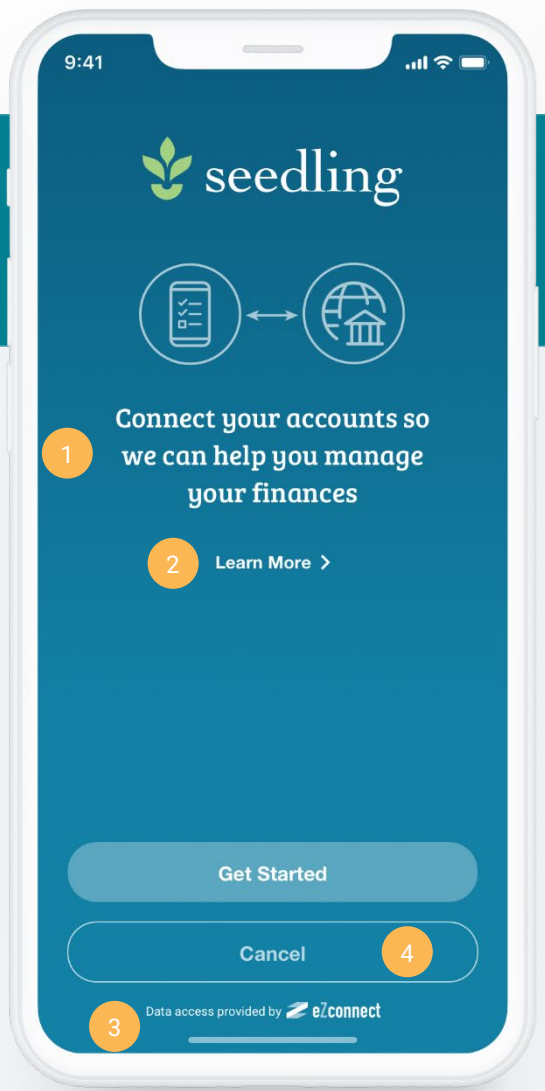


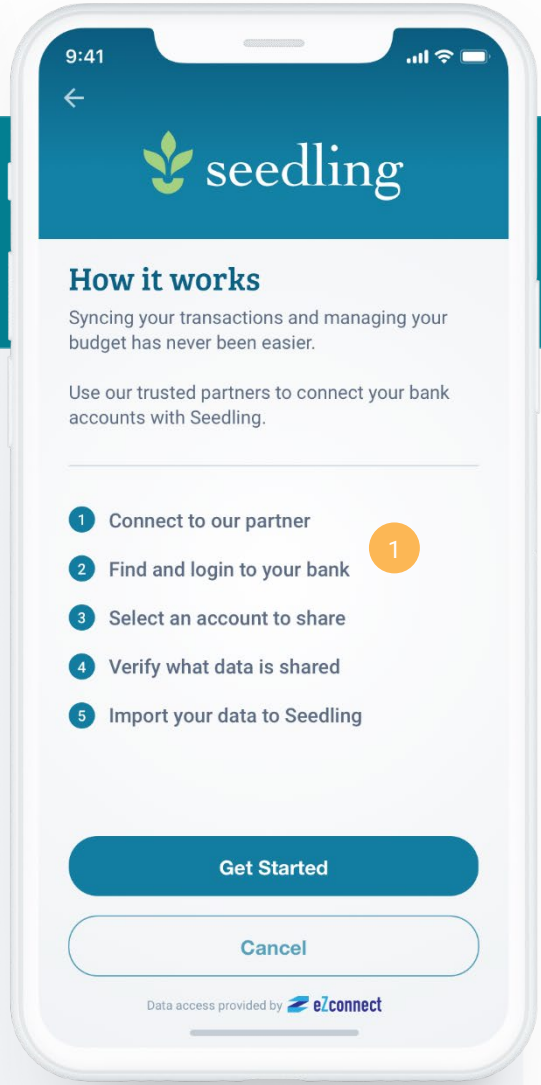
Initiate | Sample User Content

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

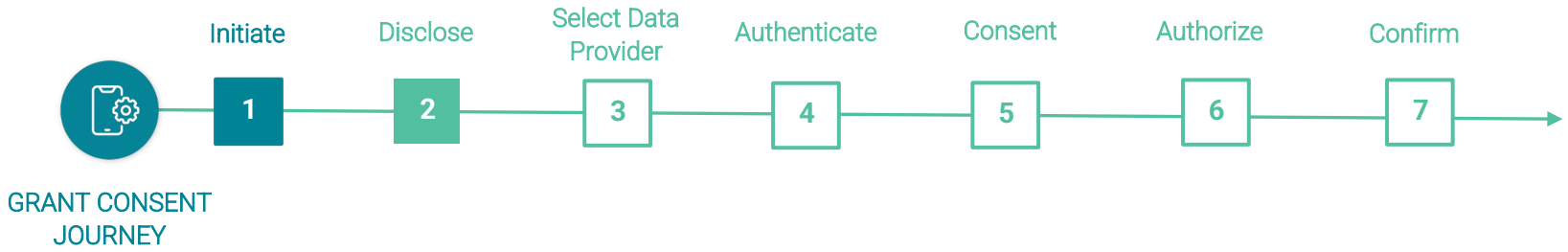
This step provides important information to the end user about what financial data the data recipient needs from the data provider (data clusters, etc.) and why they need it (business purposes) and how long they may need to continue to request this data.

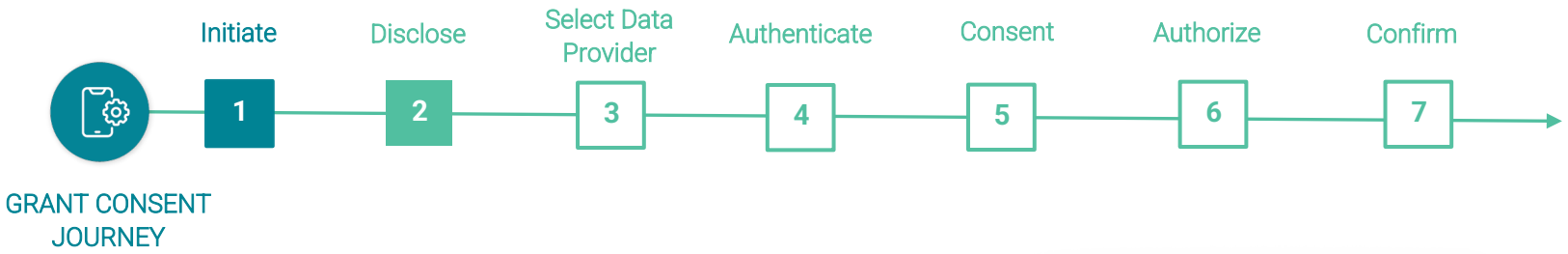
Required

- 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.

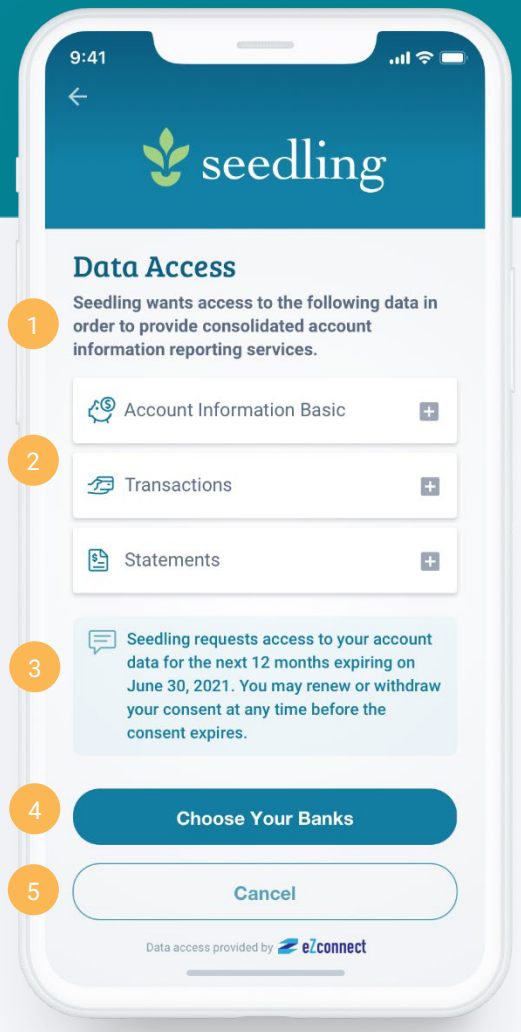
Recommended

- 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

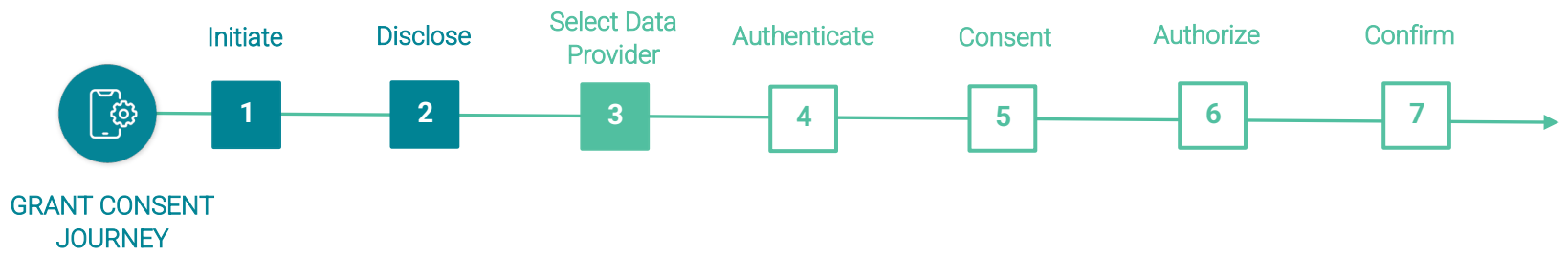
The data recipient, or data access platform acting on behalf of the data recipient, allows the end user to identity and select the data provider(s) for the consent.

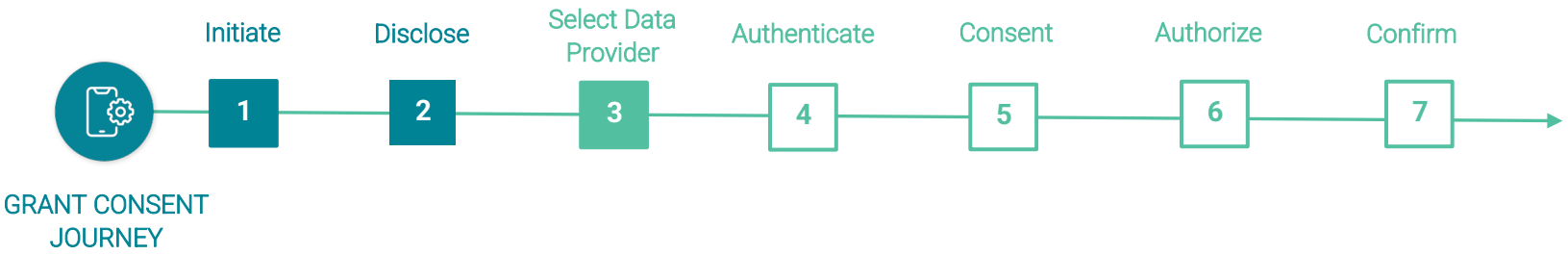
Required

- 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

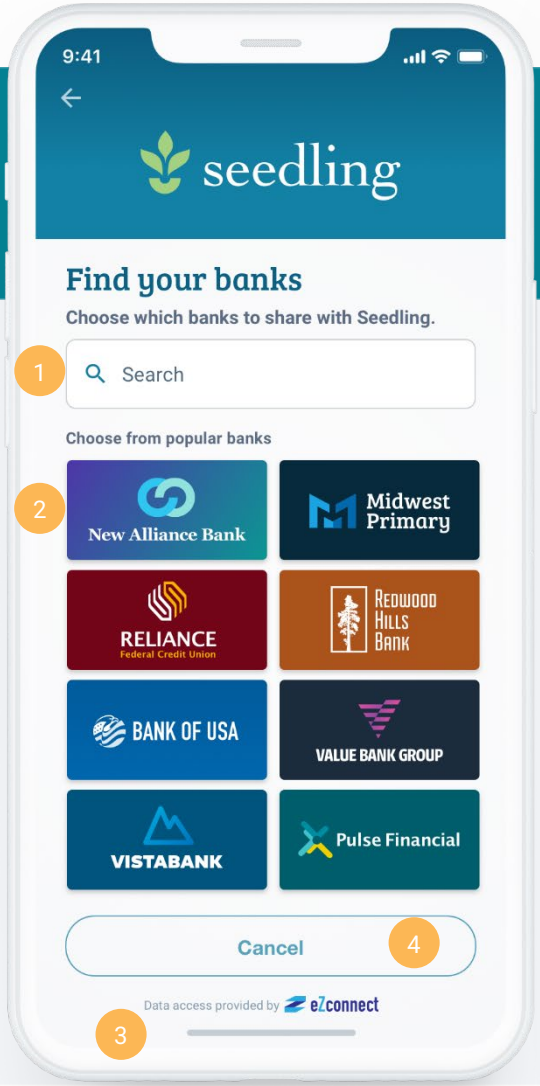
Recommended

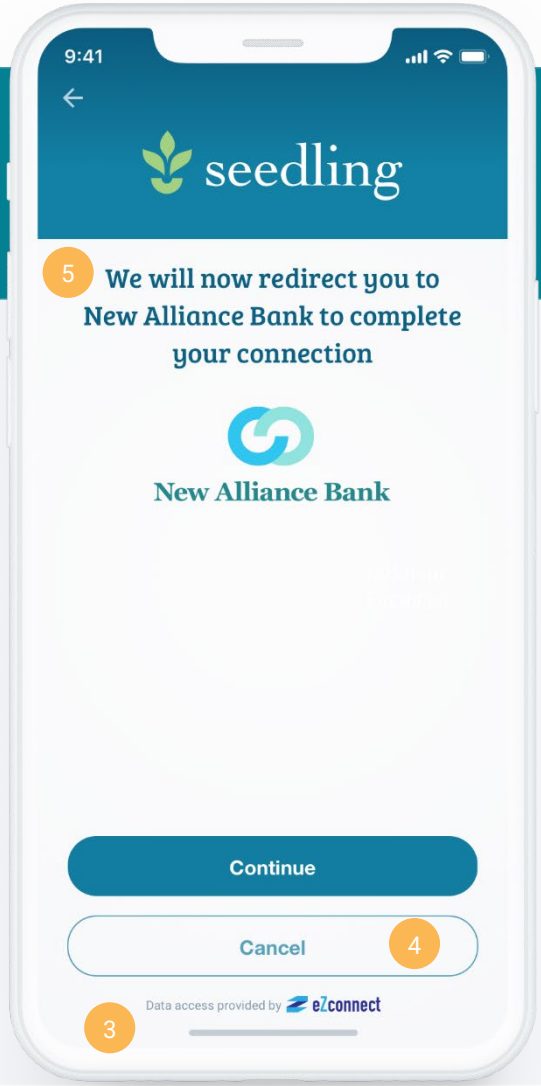
- Explore ways to present a large number of data providers to the user in a manner that helps them find what they are looking for, such as filtering
  - Support elastic search capabilities to simplify searching
- When redirecting the end user to the data provider, use a temporary page/screen to inform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

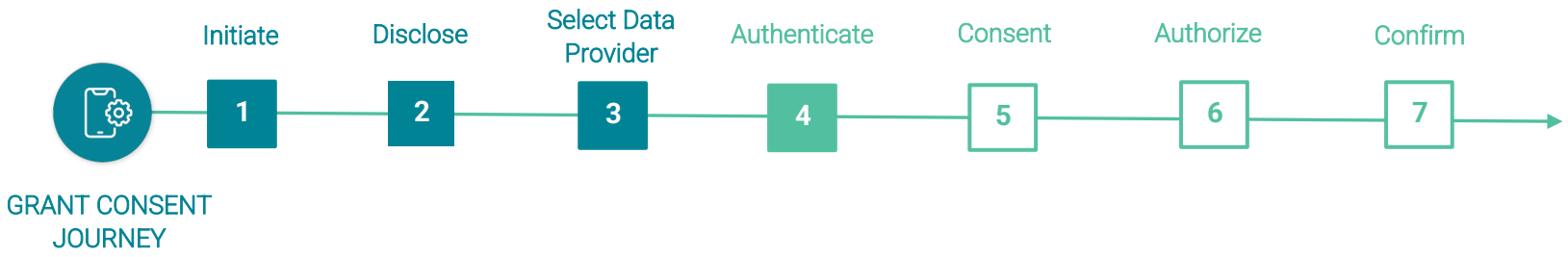
4 Authenticate

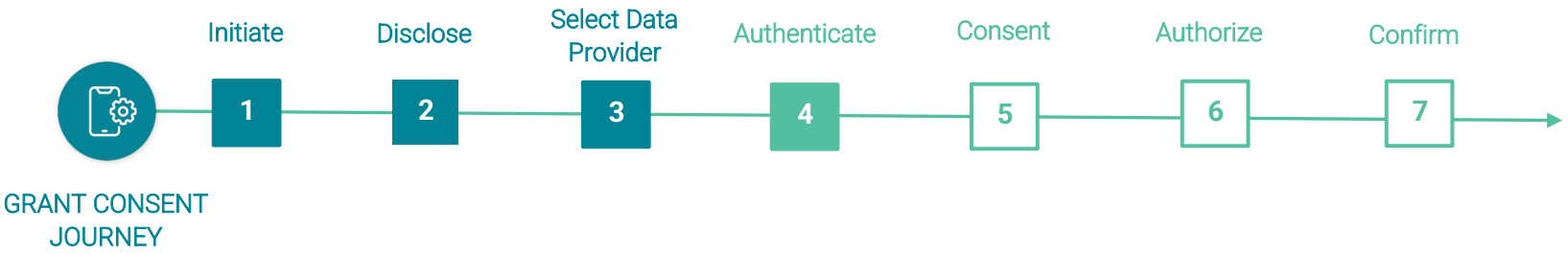
Purpose — Enable the customer to identify themselves to the data provider

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.

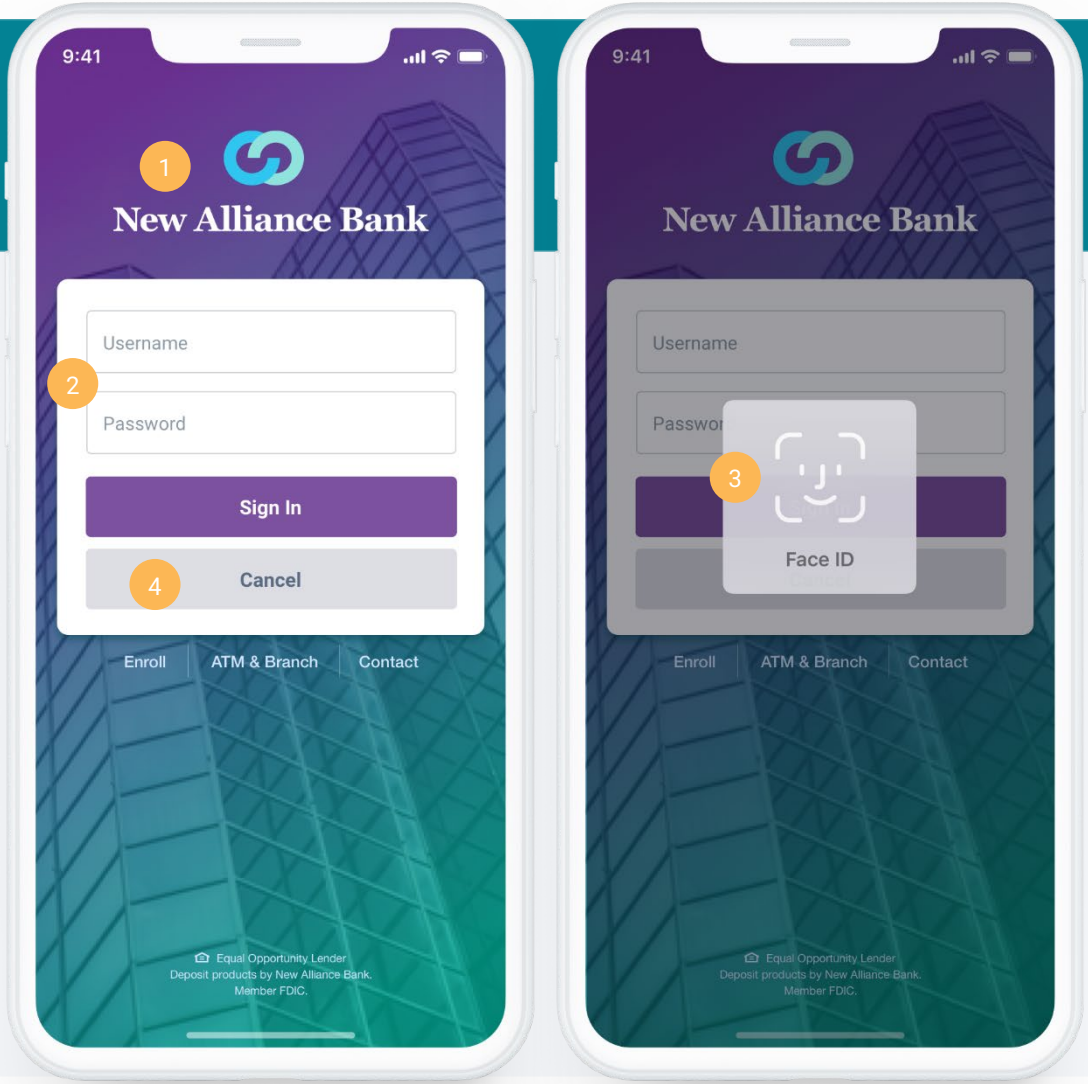
Required

- 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

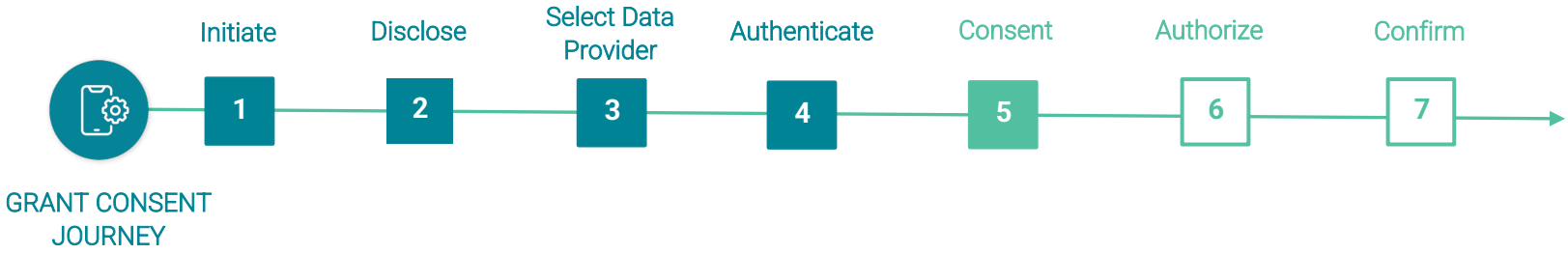
5 Consent

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.

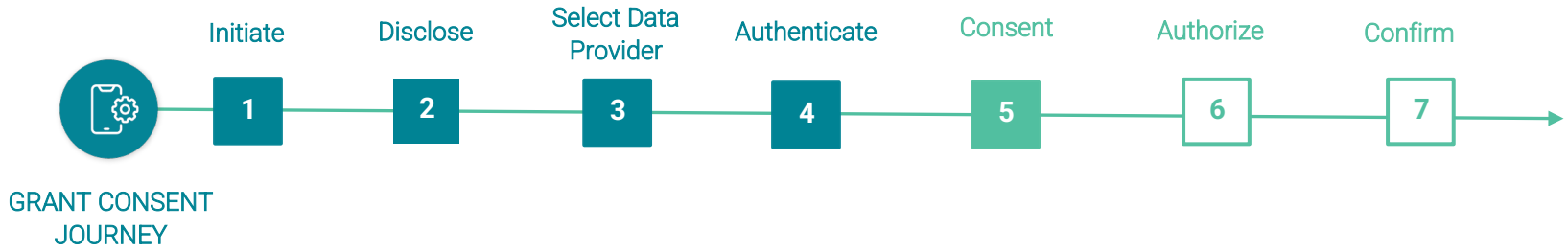
Required

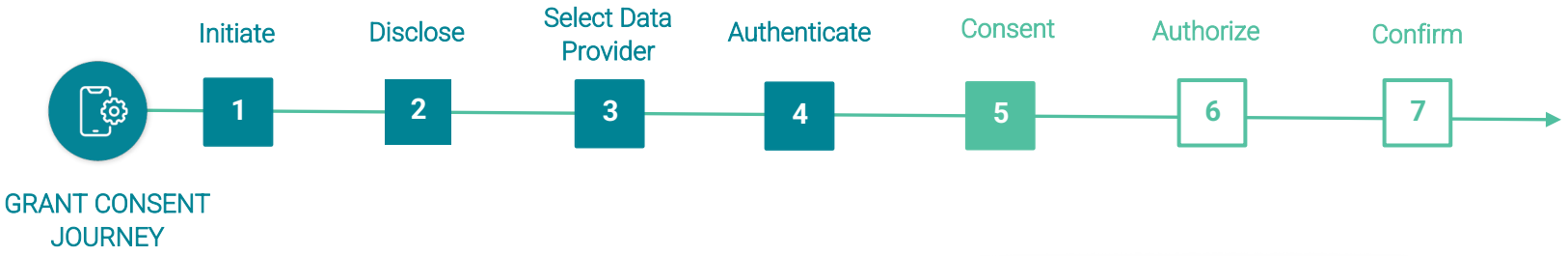
- Clearly identify the data recipient with which data is going to be shared, including data recipient name, as well as any data access platform, if applicable, so that the end user is fully aware with whom they are sharing their data
- A clear summary of what data clusters will be accessed, or shared, 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”



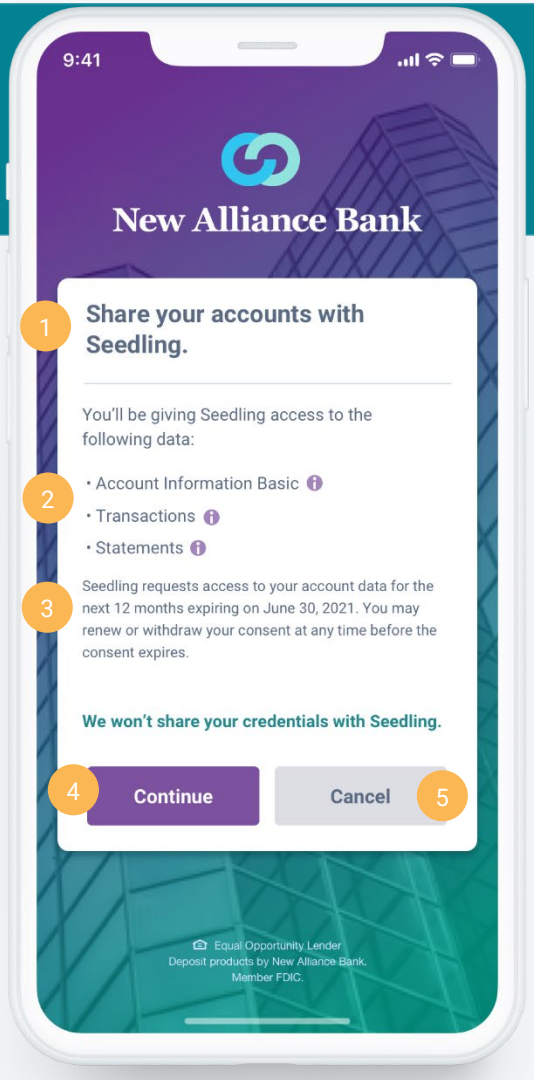
Recommended

- 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

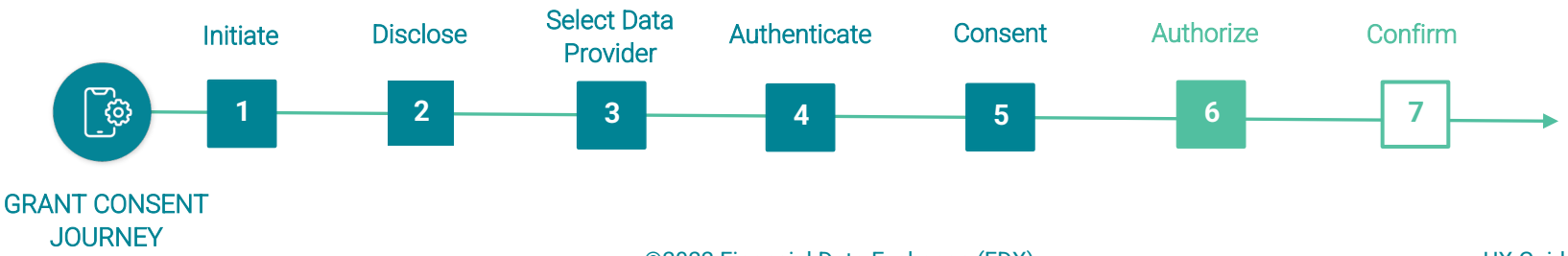
This step allows the end user to specify to the data provider exactly which accounts they authorize under the consent to share with the data recipient. This is handled by the data provider so that any accounts not authorized by the end user will be withheld from exposure to the data recipient.

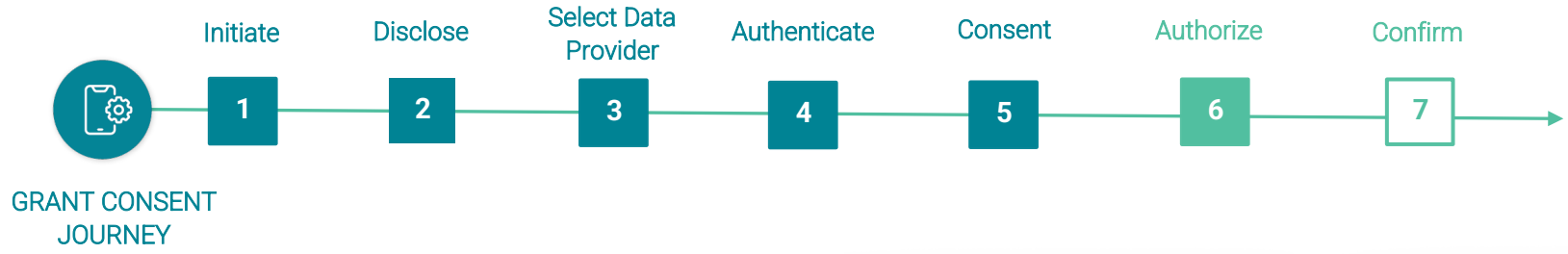
Required

- 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

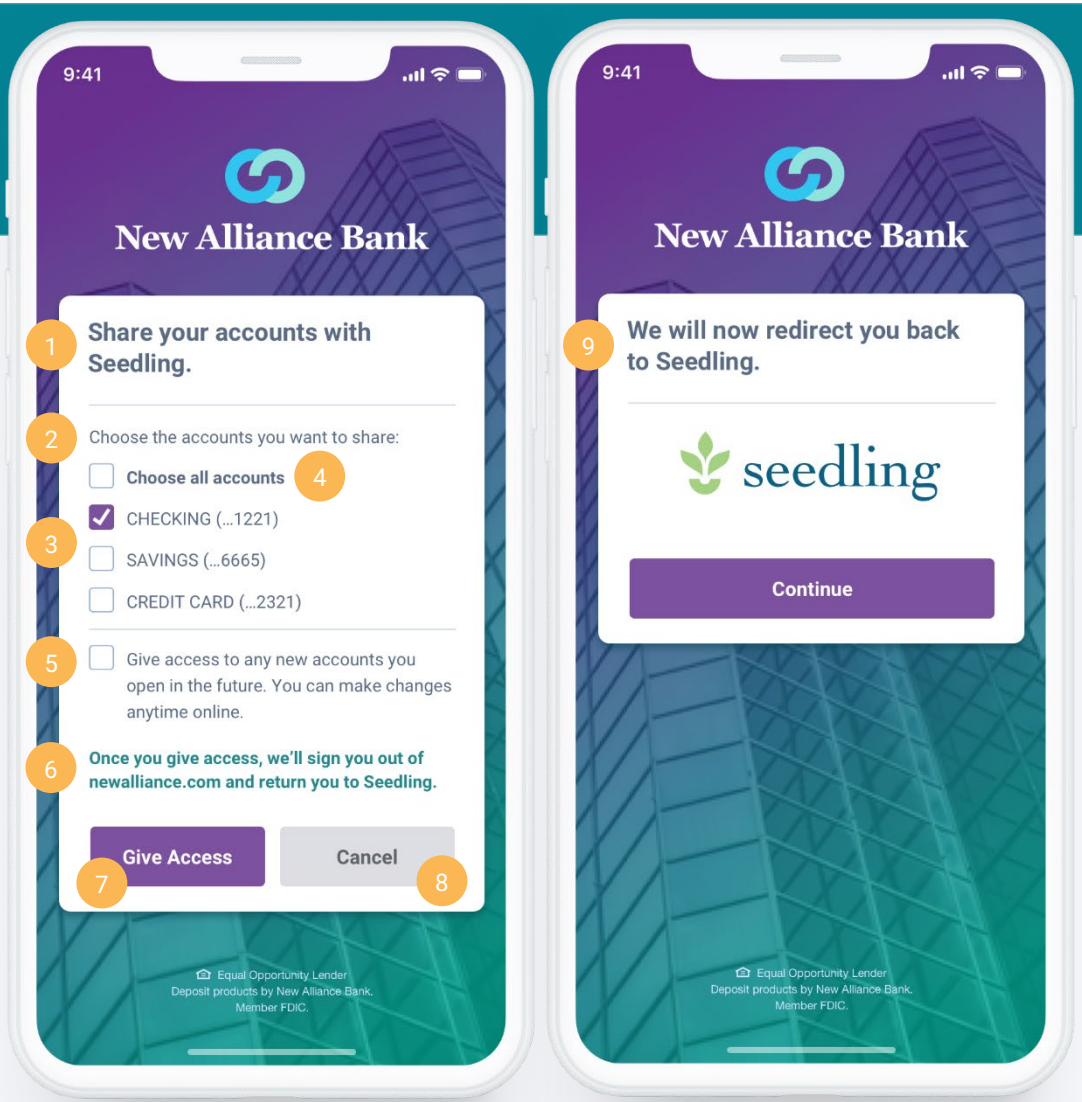
Recommended

- 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

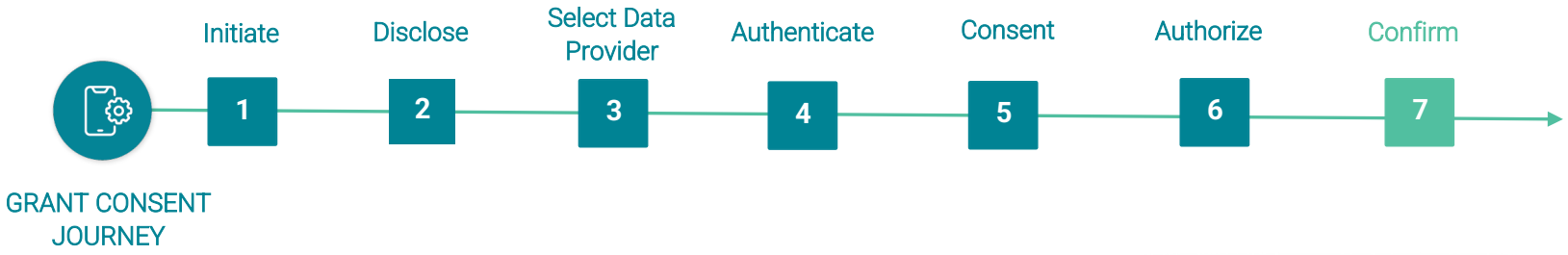
This step acknowledges to the end user that they have been redirected to the data recipient and that the access has been successfully established, or provides information why it has not.

Required

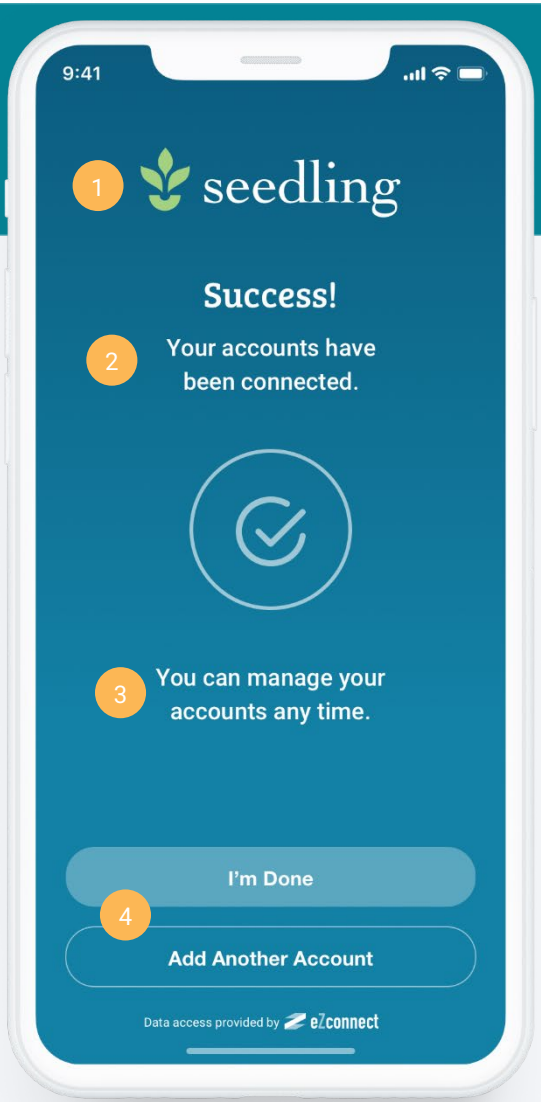
- A clear indication that the consent has been granted and that data sharing has commenced
- Confirm to the end user that they have been redirected to the data recipient if they successfully authorized the consent at the data provider
- If the process was aborted by the end user or fails, the data provider 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.

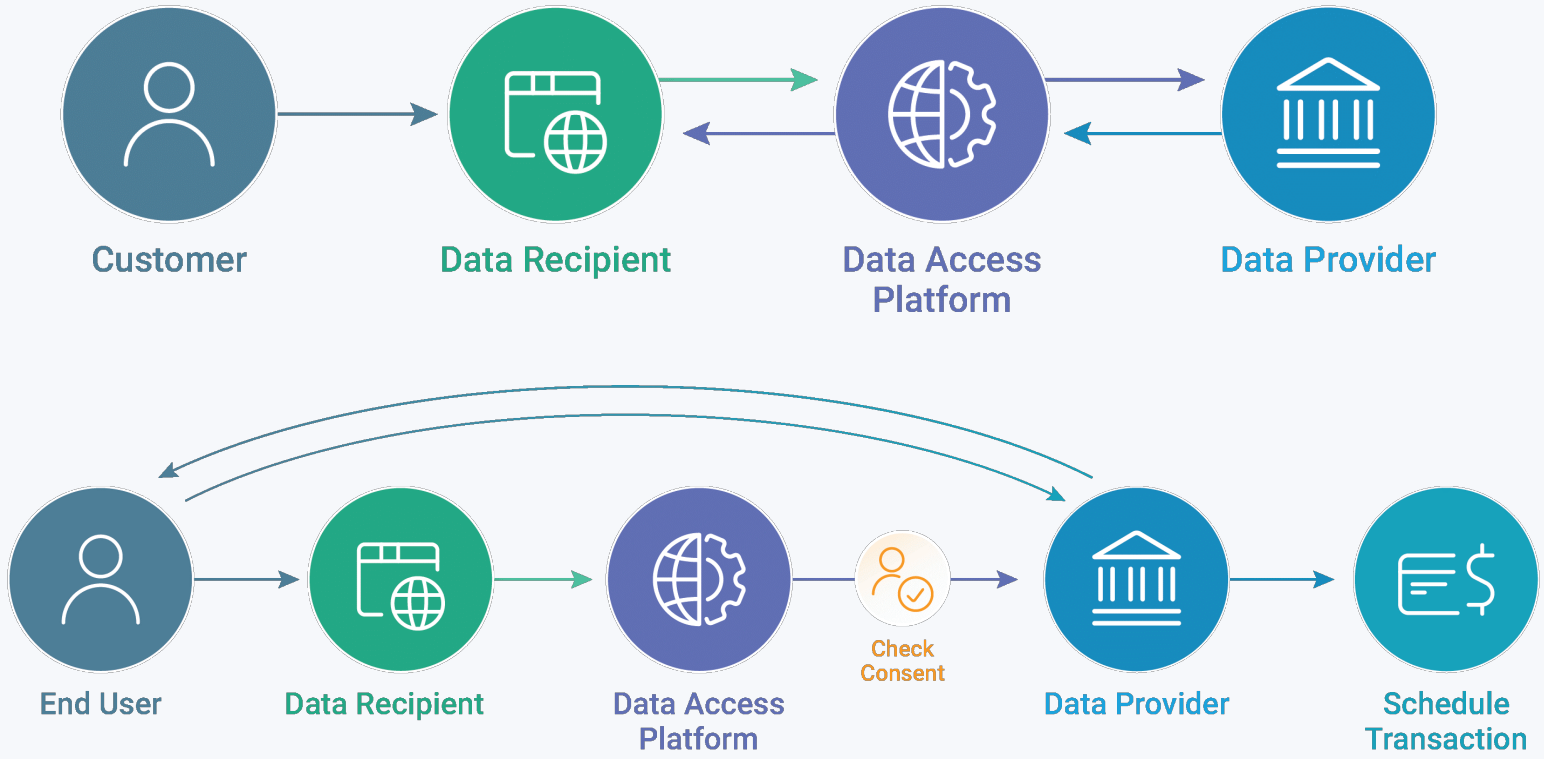
Once the consent has been granted, the end user is able to schedule payments or transfers and view related payment activity at the Data Recipient via FDX APIs. In some case, a Data Provider may require a step up authentication when scheduling a payment or transfer from the Data Recipient. The data cluster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

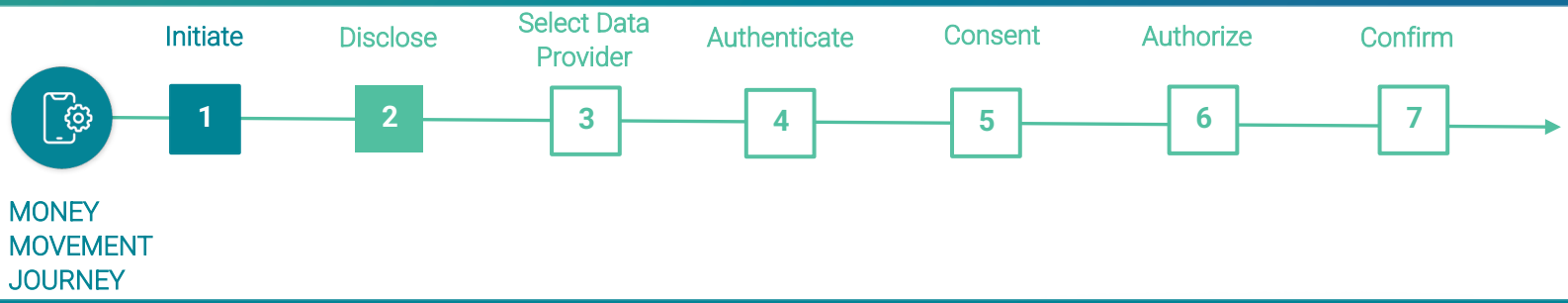
This section solely describes the Disclose and Consent steps of a money movement journey as they differ slightly from the standard grant consent journey above.

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:

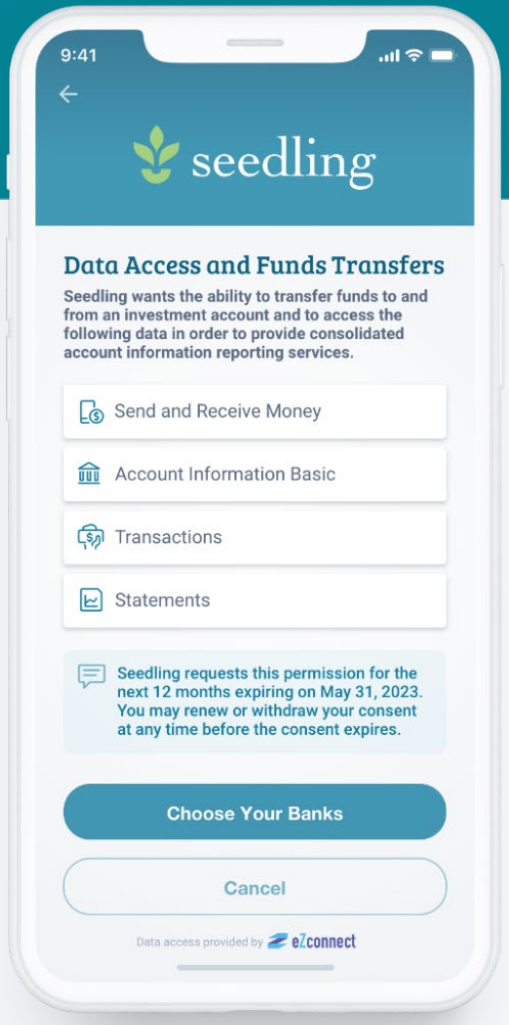




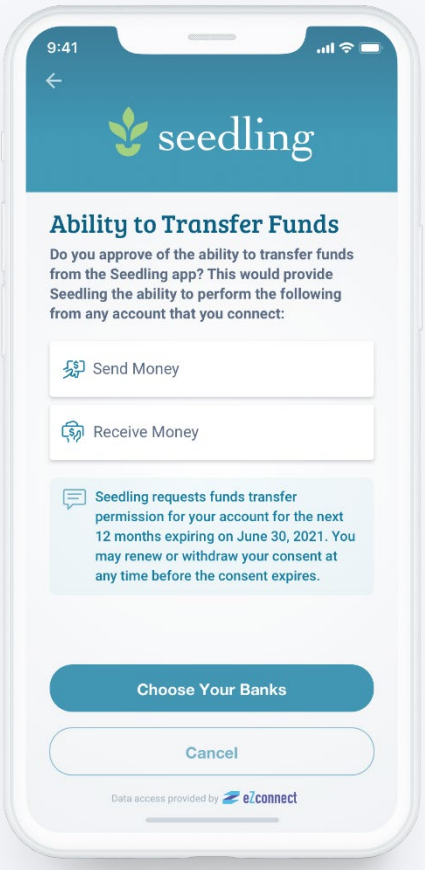
Disclose | Sample User Content

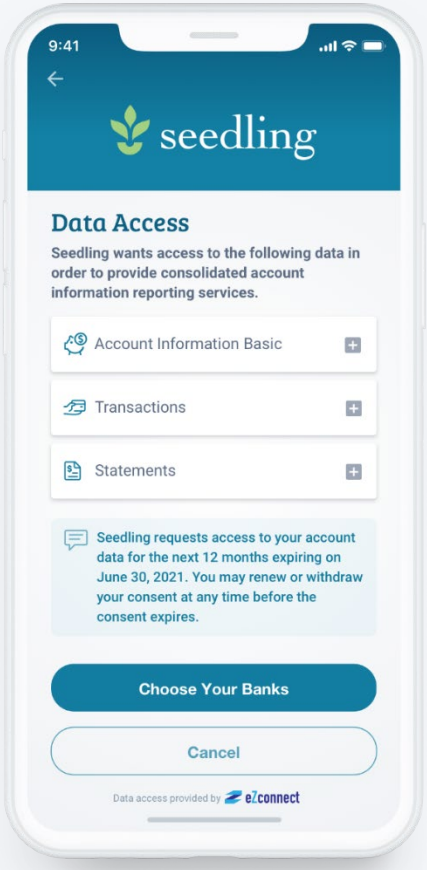
Following the same guidelines as the standard data sharing Consent Grant journey, the Data Recipient must explicitly communicate in the Disclose step that, in addition to the other data, they need to access the **money movement capabilities**, as shown here.

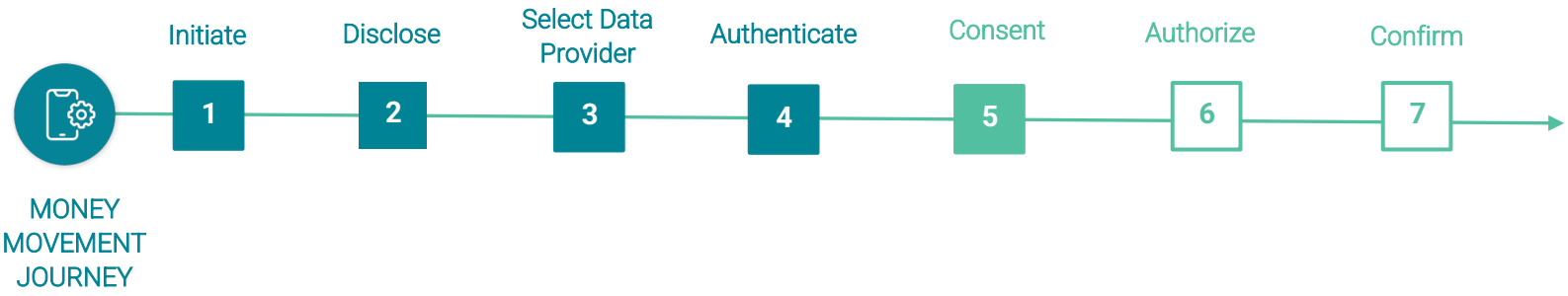
An optional Disclose implementation example is shown below.



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.

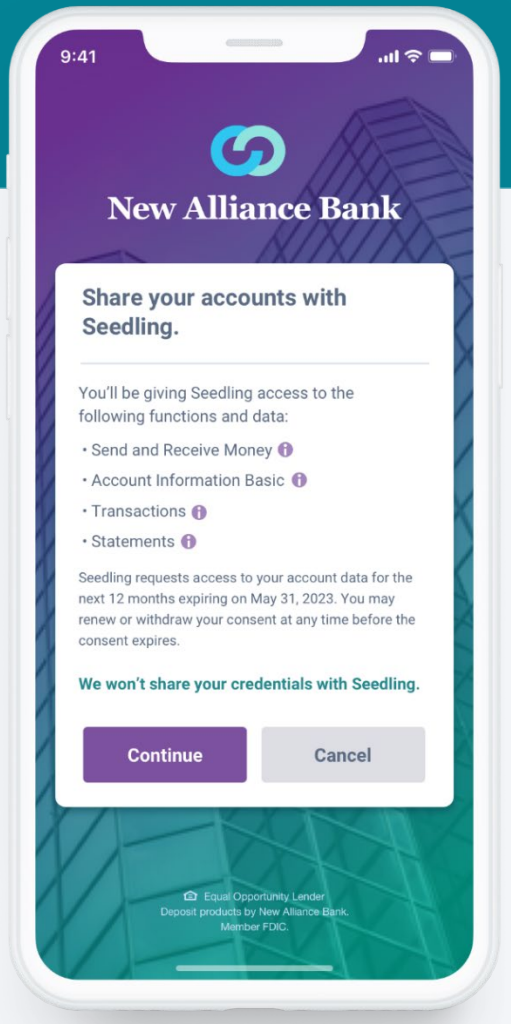






Consent | Sample User Content

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

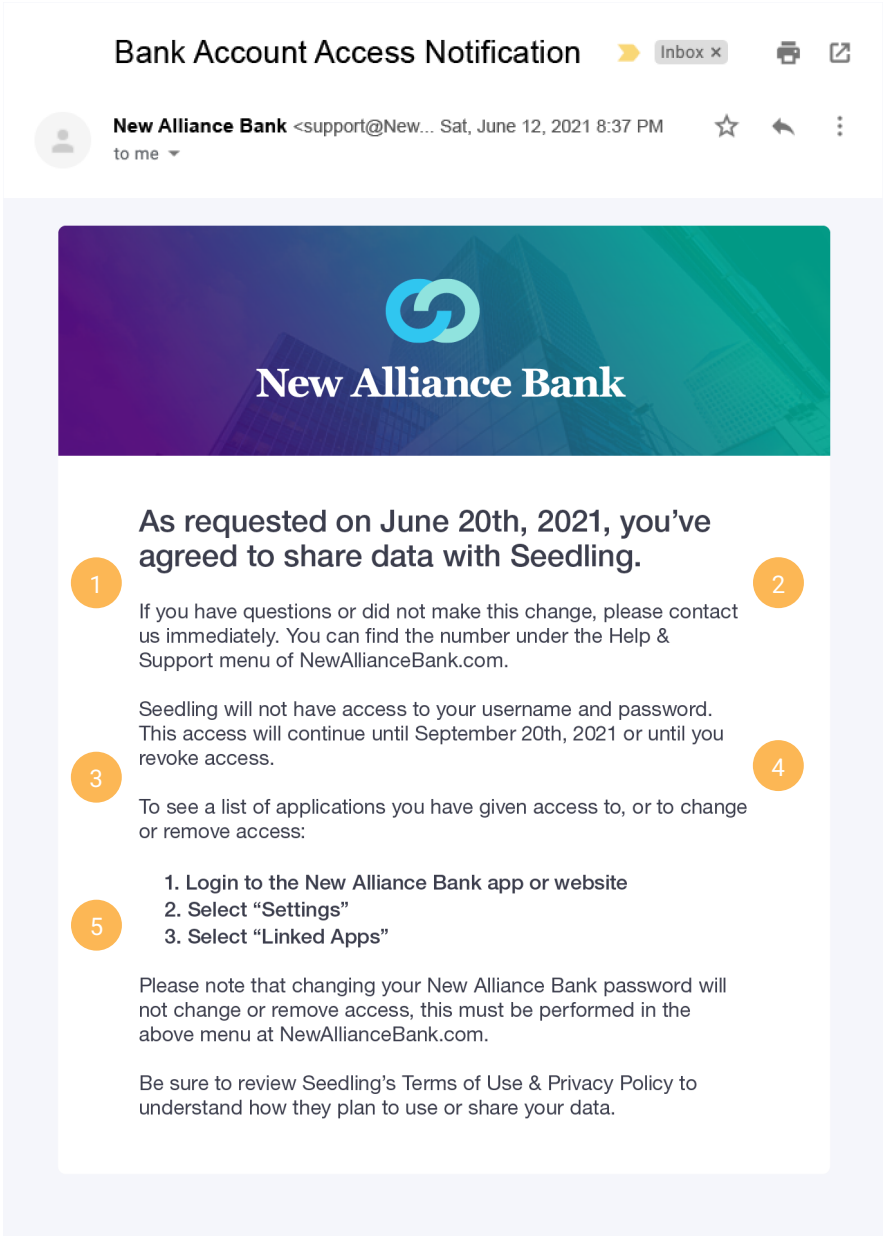
- Data Provider may allow an option for the End User to choose the notification delivery method including:
  - Email
  - Text message
  - Push notification to their Data Provider application
- The content of the notification to the End User:
  - May choose to indicate that changing their password will 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.

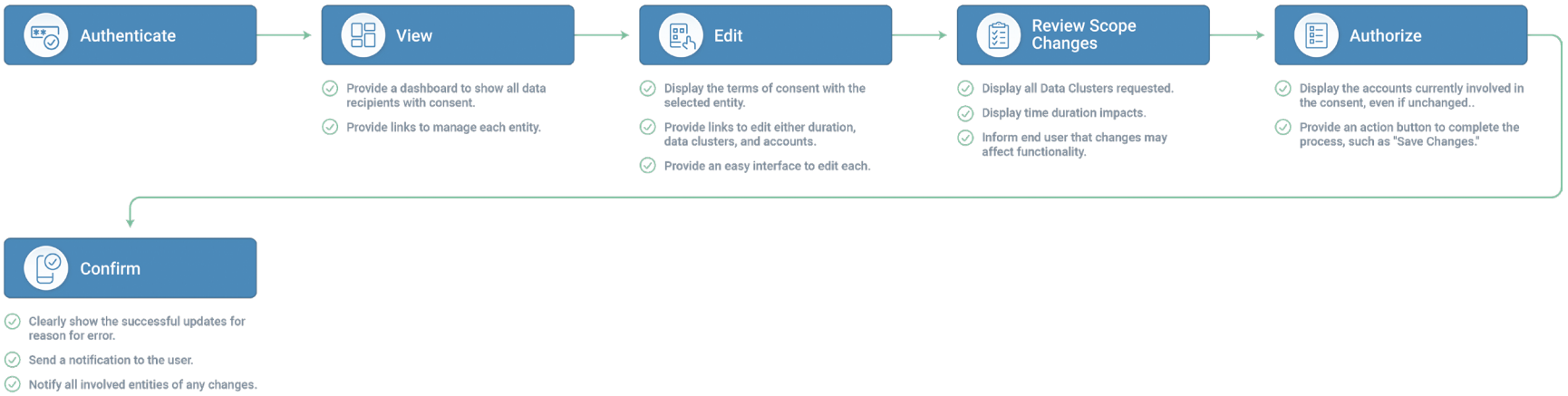
Entity Notification

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:

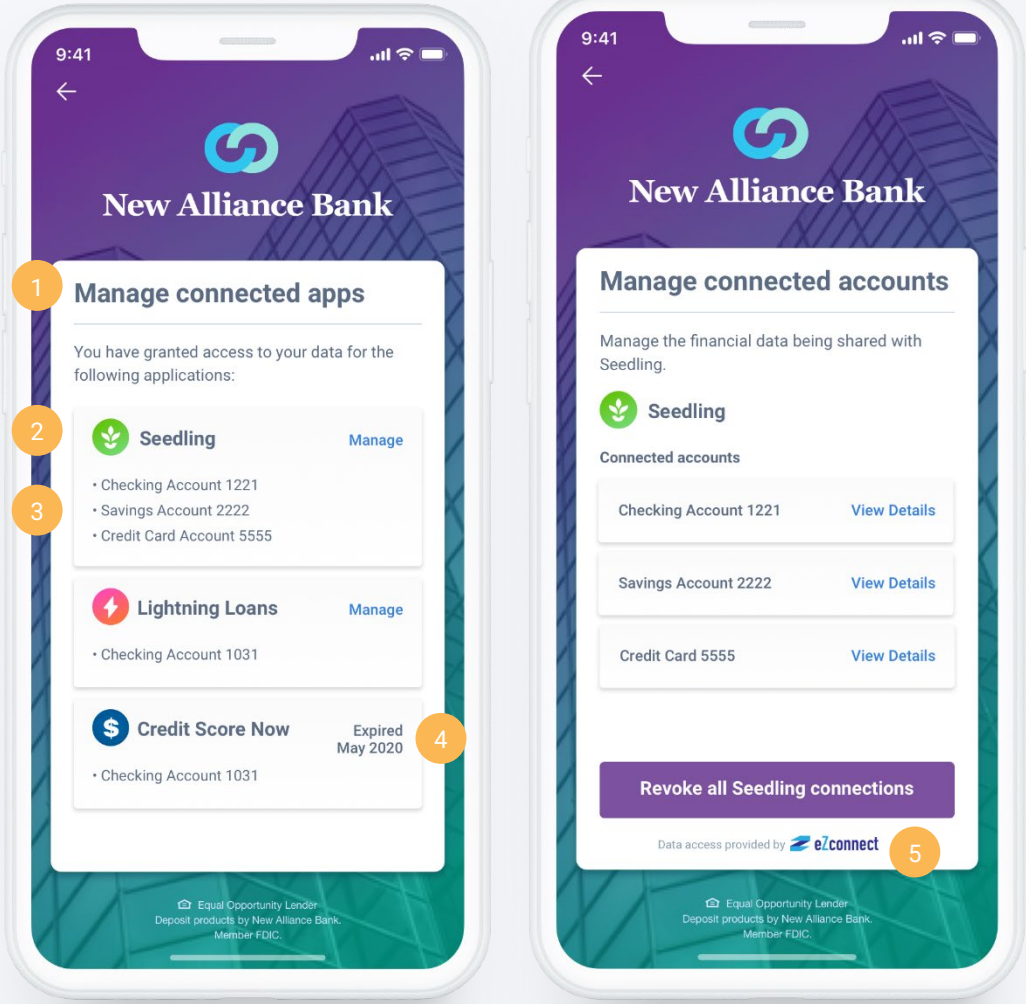
- The entities with which the data is being shared.
    - It should be indicated if one or more Data Access Platforms have access to the End User's data, along with the names of any Data Access Platforms involved in the Consent. Provide access to additional information about the Data Access Platform 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.

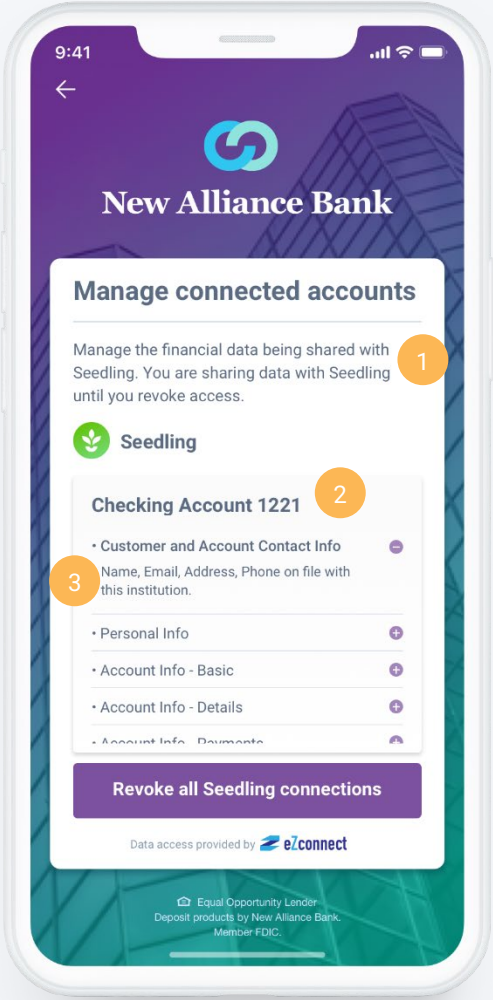


Consent Dashboard – Data Provider | Sample User Content

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

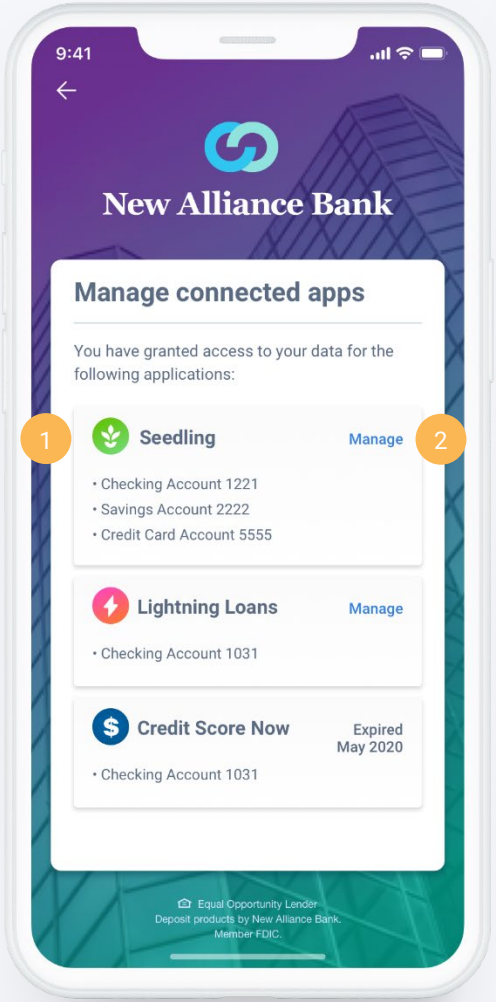
- An account owner removes access for another end user who previously had access, such that the other end user no longer has access to the account. This could occur in a a joint, authorized or delegated end user situation.
- The account is closed by the financial institution
- An end user closes the 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)

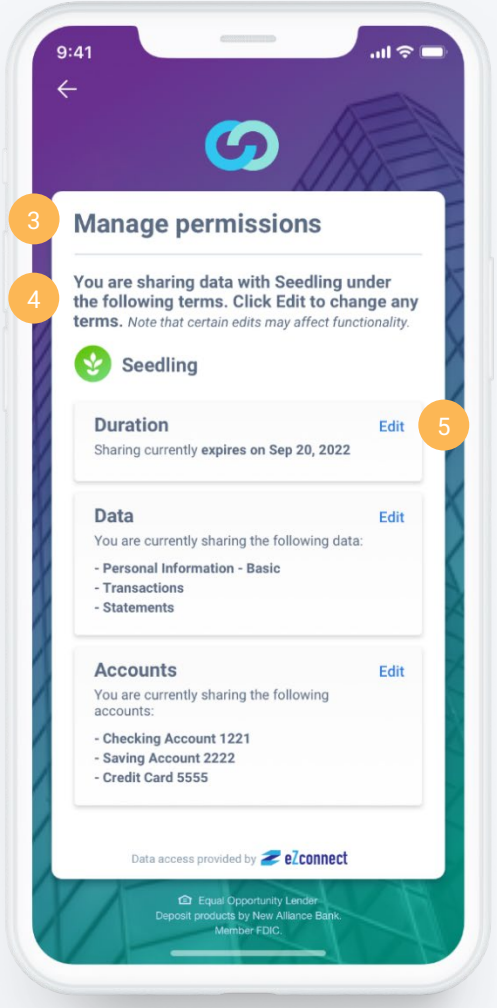
Consent Dashboard – Data Provider | Sample User Content

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:

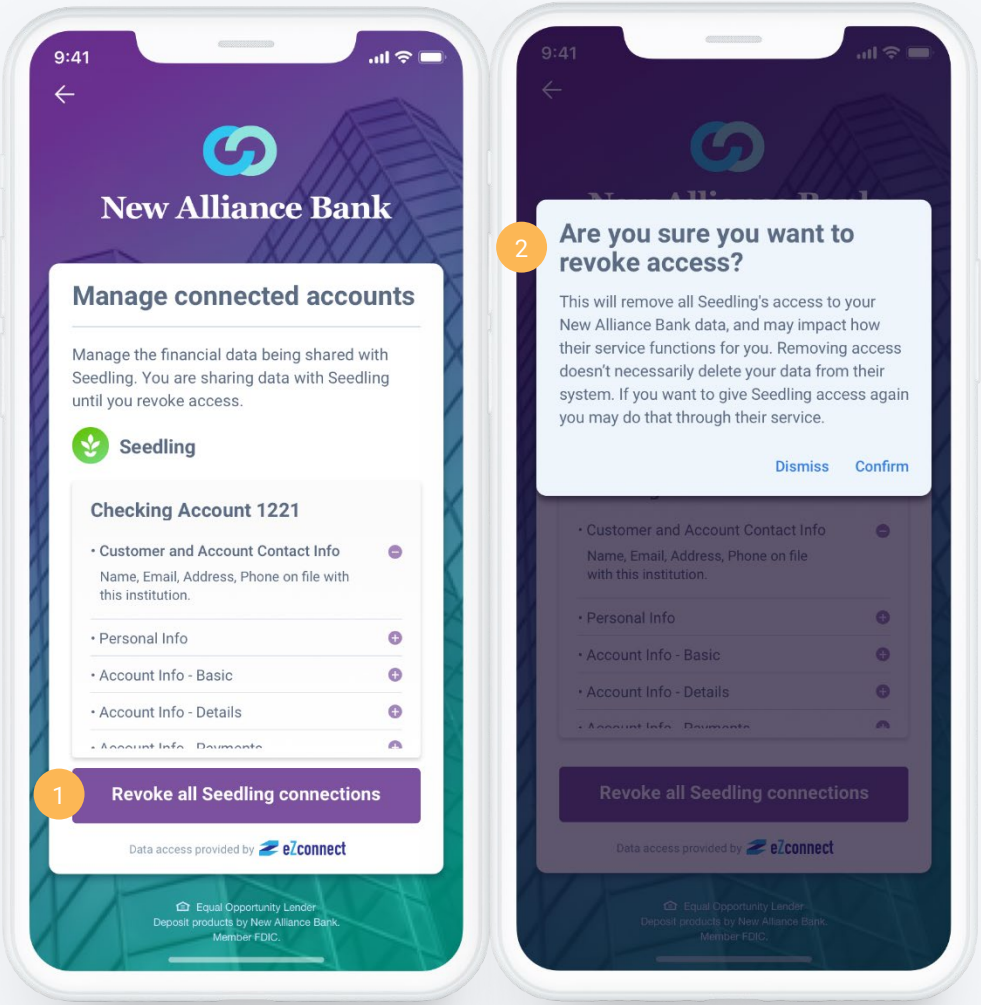
- Immediately revoke all access to their data from any specific entity
- Revoke all access from a specific Data Recipient and each Data Access Platform involved in the Consent
- Before revoking Consent to their data, notification should be provided to the End User that clearly explains the impact revocation 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:

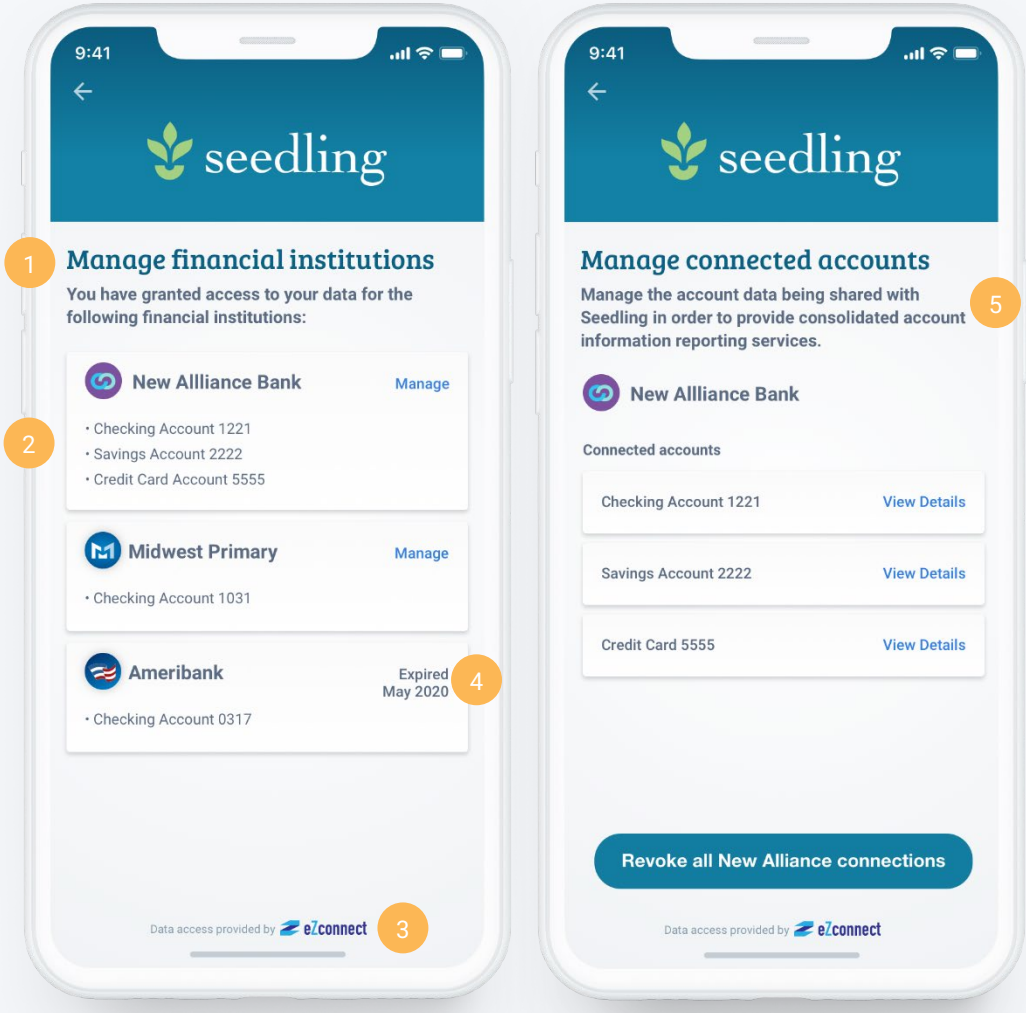
- The Data Provider and what accounts have authorized under the Consent.
- If a Data Access Platform is involved:
    - It should be indicated if a Data Access Platform has access to the End User's data and the names of all Data Access Platforms involved in the Consent or sharing of data. Provide access 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

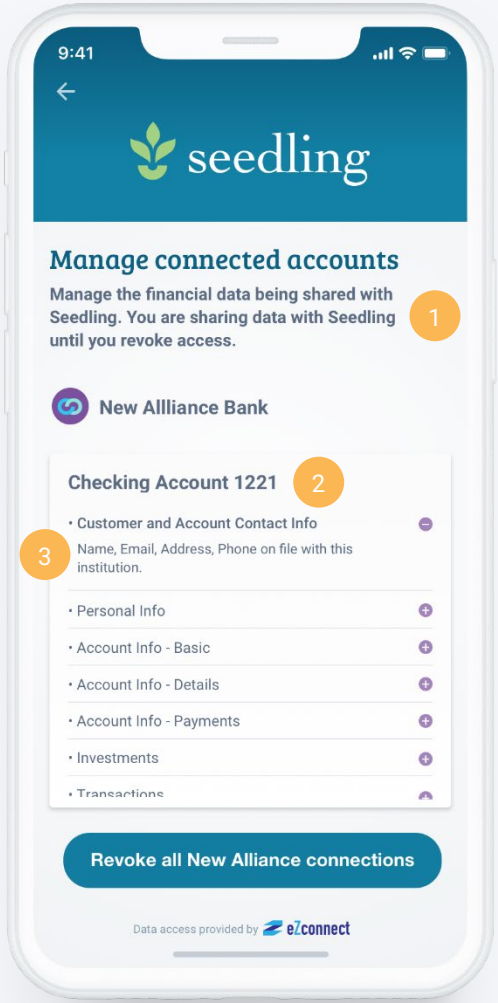


Consent Dashboard – Data Recipient | Sample User Content

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

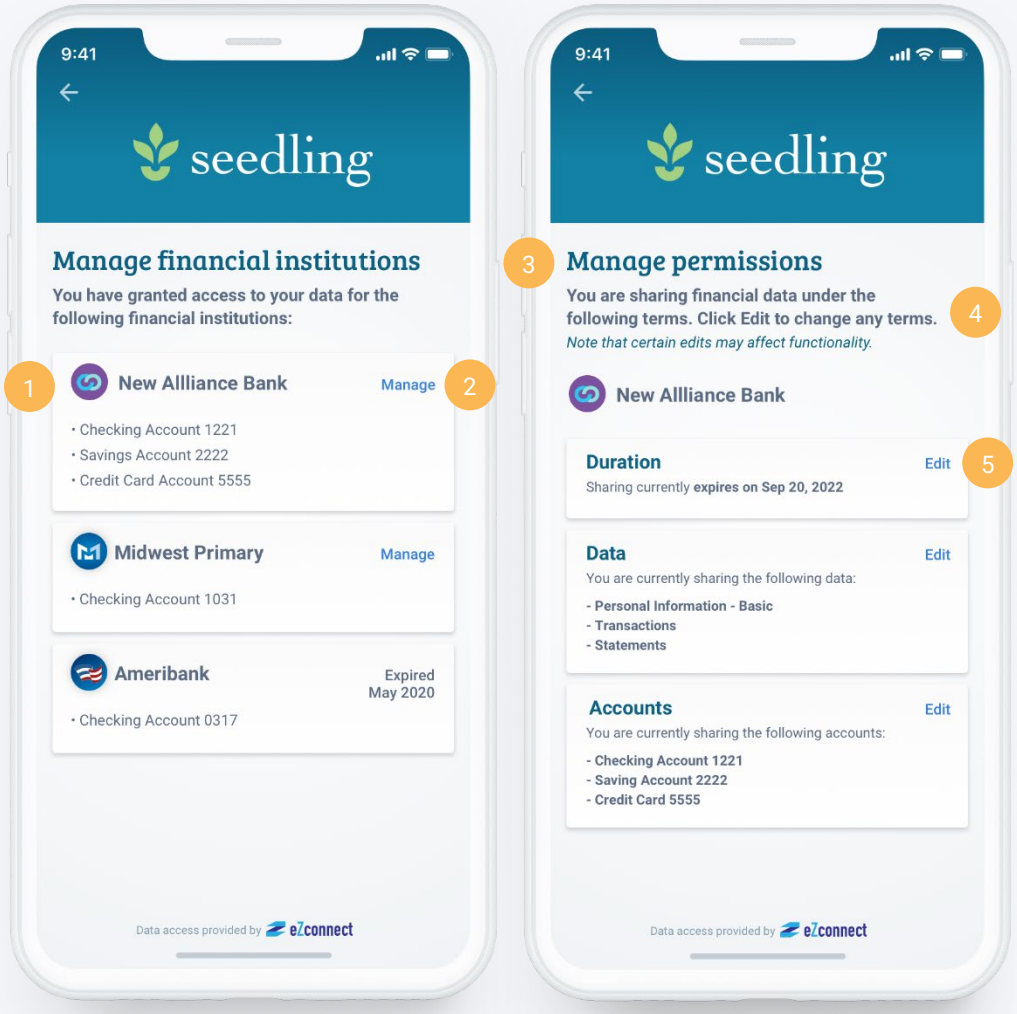
- Data provider change causes error that requires end user to re-consent. *MFA auth / password change / IT Policy / Expired Token

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.

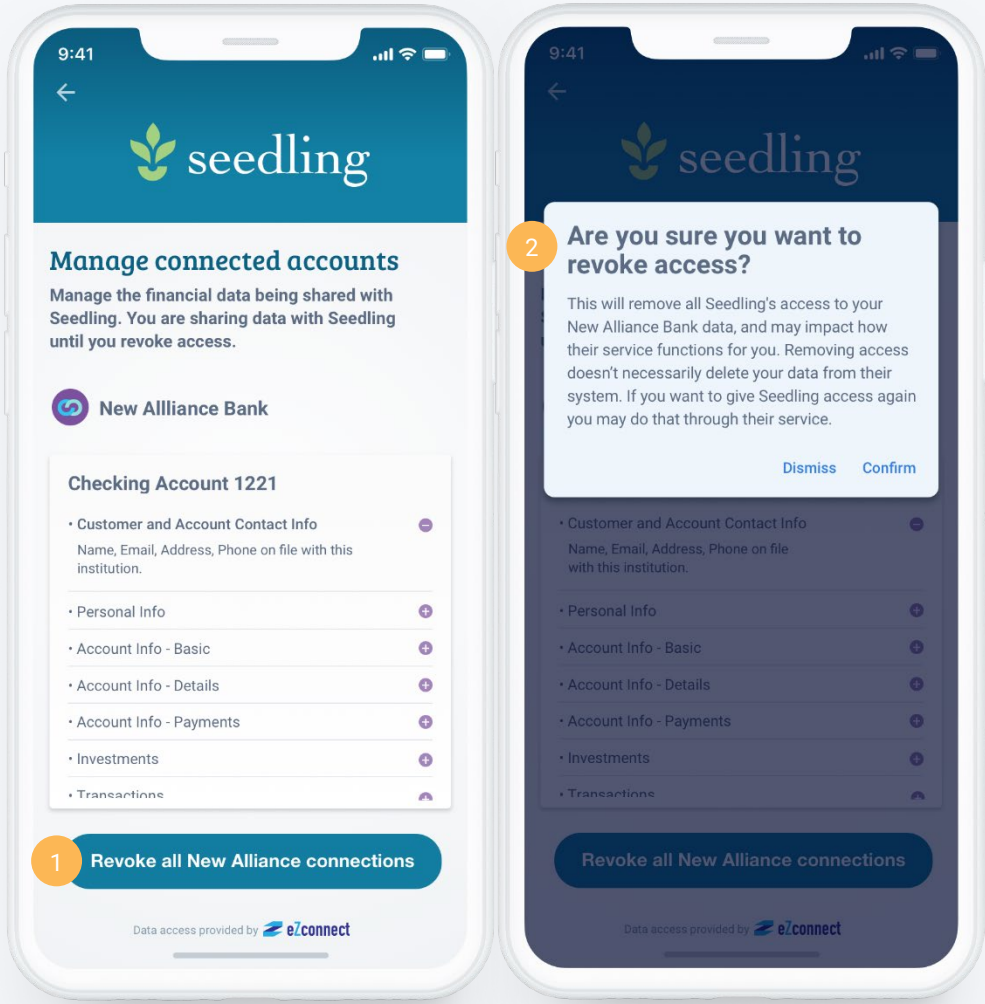
Consent Dashboard – Data Recipient | Sample User Content

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