FINANCIAL
DATA EXCHANGE

Certification Use Cases Specification

Version 1.0
May 2022

Legal Notice

Financial Data Exchange, LLC (FDX) is a standards body and adopts this Certification Use Cases Specification document 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 merges the previous Credit Management and PFM Use Case documents (RFC 0088 and RFC 0010) and incorporates RFC 0102 and RFC 0103 for Data for Account Owner Verification and Account Linking for Payments	May 2021

Contents

Introduction to FDX Certification Use Cases

FDX wishes to drive interoperability between data providers and data recipients via use case profiles, such that the data required for a business use case is made available. At the same time, FDX seeks to ensure that only the **necessary** data for the use case is shared in line with data minimization principles.

FDX Use case principles:

- A use case enables the notion of providing users access to their financial data in the application of their choice in order to accomplish a specific task. This defines a minimum set of data required to accomplish that task.
- It supports the data minimization principle by defining minimum and optional data for a given use case and the guideline that no other data should be accessed for that use case.
- It allows for the definition and implementation of specific rules or recommendations for a use case on top of the foundational principles of data sharing – access, control, transparency, security, traceability.
- Use cases will evolve over time – new ones are being added, some may change in their requirements, and others may decline in usage – but the framework should be constant and allow for evolution of use cases
- Having an FDX use case framework will allow FDX teams to more quickly evolve the specification and the certification program in support of a new or changing use case

Definition of required, conditional, and optional:

- **Required**: the data element or entity MUST be provided in order to be certified for the Credit Management use case
- **Conditional**: the data element or entity MUST be provided if a certain condition is met, such as a product type
- **Optional**: the data element or entity may be provided at the Data Provider's discretion. Provisioning such Data is not considered essential for certification

The certification of the use case will be carried out via the FDX Certification Program under development.

This document does not currently cover consent requirements, or the operational requirements. Those requirements may be added over time, if deemed necessary for improving secure interoperability within the ecosystem.

Refer to the *FDX Certification Use Cases v5.1.xlsx* spreadsheet for the recommended values of required, optional, or conditional for the data elements and corresponding use cases described in this document. The use cases comprise PFM, Credit Management and Servicing, Account Linking for Payments and Account Owner Verification.

Alternative methods

As alternative methods for satisfying the use cases are introduced in the API and the security RFCs, those methods (upon approval of updated use case RFCs) may be used to satisfy the use cases in the future. An example of such a method is Verification Query that is currently in the proposal form. An example of an approved method is end-to-end or app level encryption. Data Providers may use that method at the field level to protect sensitive data.

Another example of an approved method is the use of the Consent API to manage granular consent. That may be used to ensure that only the required data for the use case is sent to the recipient. The final example of an approved method is the use of a Payment Networks entity to supply a substitute account number. That method, since it is a part of the data API, is already incorporated into the proposal.

Credit Management and Servicing Use Case

Credit Management and Servicing is a major business use case that drives the need for financial data sharing. End users seeking to use credit management and servicing apps will want their FIs to share the necessary data to utilize the app functionality in a meaningful way. This use case allows for the return of account holder data that the current authenticated user has access to via digital channels.

This use case describes the entities and data elements in the FDX API v4.6 and above that are considered required for Credit Management. Some of the entities and data elements are marked as conditional, which means that those elements are considered required depending on the specified condition.

This proposal is a dual use case. The first is "Credit Management and Servicing" which covers data elements required in digital exchange of data for this industry segment. The second use case is "Statement History" which would require 24 months of actual statement history from the provider. This use case is required for certain lenders and lending segments.

In Scope

This is a use case that covers all of the lending and scoring industry. One of the primary guiding principles is to replace bank statements and other physical document requirements with digital data. The additional guiding principle is to support current innovation and progress that can be made in the lending and scoring industry through the use of digital bank data.

All of the information required to verify the account owner is needed along with additional account details as specified in the required elements spreadsheet. The use case also requires 24 months of transaction data or such lesser maximum amount as the Data Provider makes available to the applicable End User through any other digital channel. It is highly recommended

that Data Providers improve their transaction data to 24 months if they do not already do so to fully support the consumer use case. They otherwise risk degrading the consumer experience. There are multiple ways this data can be used, but primarily includes:

- Verification Of Deposit
- Verification Of Employment
- Verification Of Assets
- Mortgage Lending
- Non Mortgage Lending
- Cash Flow Analysis In Lending
- Fraud Prevention In Lending Through Data Examination
- Account Verification
- Current lender uses for data in underwriting today
- Scoring and Modeling to help include more people in financial inclusion that may be thin credit file or poor credit

Statement History

For bank statements there are still certain lenders and segments including business lending, that still require bank statements. This also could be required for certain lenders that are adopting digital lending by having statement auditing processes to help them transition from manual to digital processes.

Another example in which this could be used is lenders that have not adopted digital data for lending, but have determined that it would be more secure to receive statements directly from the provider instead of those provided by the consumer directly, which could be doctored documents. The use case requires 24 months of statement images/pdf's or such lesser maximum amount as the Data Provider makes available to the applicable End User through any other digital channel. The goal would be to phase out this use case over time as organizations adopt digital-only processes.

Considerations

Concerning PII Information

Use Of PII Information - The use of PII information such as name, address, telephone, and email are for identification of the account holder of an account. This information is then compared to information from the lender or credit bureau to assure only accounts with matching account holder data to the consumer is used for consideration in the lending and credit process. This is a compliance requirement for data use.

Support For Use Of Name and Address - There is complete agreement on the Name value as being a required data element. There is non a consensus as to the use of the address. It is proposed that address be required as there is clear precedence of the address being available on the bank statements and thus it would be a data element used in the current process of determining if a bank statement belongs to the consumer.

Support For Use Of Phone and Email - Phone number and Email are retrieved today by data recipients and are used as part of the account verification process. Several data recipients have expressed the concern of not being able to meet compliance requirements at a high enough success rate to make services marketable if access to these data points are removed.

Concerns To Be Noted With Phone and Email and Potentially Address - Providers have expressed the risk of data elements such as Phone, Email, and Address not being sourced by the financial institution. This information is also not audited for accuracy. This is a valid concern that can affect the success rate of current methods of matching data to consumers. The task force including recipients understands there will need to be proposals for identification methods that would be more successful and better for all parties in the future. In the meantime, as there are no other FDX-adopted alternatives the risk is understood and accepted by the data recipients.

Support For The Use Of Account Number - A full account number and routing number would be used in the process of loan funding to assure a valid account for issuing funds. This must be supported either in this use case or by the lender, or this needs to be facilitated in the money movement use case. That means lenders would apply for both this use case and also the money movement use case to facilitate their business.

Concerning Multiple Account Holders

It is the current stance of the taskforce that this use case should only return the account holder data that the data provider makes available to the currently authenticated user through any digital channel until such time as it needs to be revisited. There are many unsolved questions currently on this subject such as a primary holder's right to act on behalf of secondary account holders and what data they should be able to share from secondary account holders (if any) that are largely outside FDX's scope.

Concerning Statements

Support For Statements - There is currently not full adoption in all of the lending industry for use of digital-only data. There are mortgage buyers that are non-Fannie and Freddie providers (Non-Qualified) that require statements. It is also common in other lending segments like business lending to require statements currently. Even in these cases it would be better that statements are provided directly through the API as it would be easier for the consumer as well as reduce fraud because the statements couldn't be modified before being delivered to the lender.

Long Term Stance From Taskforce - The taskforce is in agreement that the long term future should not include exchange of statements for financial data delivery. We recommend that FDX members work together to encourage and push standards that would require use of digitally exchanged data for loan files instead of documents like bank statements. The task force is considering a push for digital adoption to replace statements within 5 years or sooner if possible.

Concerning Sensitive Data Elements

Certain data elements required by the use case may be deemed sensitive e.g., due to interpretation of applicable regulatory mandates. The provider can certify against the use case by providing such data as is, or by adopting one of the use case approved sensitive data security design patterns.

Out of scope

Extremely sensitive PII data - date of birth and tax ID - are currently **not** included in this use case.

Personal Financial Management Use Case

Personal Financial Management, or PFM, is the process of managing one's money. For a data recipient to be able to provide this service, the end-user needs to share account related data such as account details and transaction details for the accounts they hold at each Data Provider. This use case describes the entities and data elements in FDX API v4.1 (or higher) that are considered required for PFM. Some of the entities and data elements are marked as conditional, which means that those elements are considered required depending on the specified condition. The use case will be updated over time to keep pace with the more recent versions of the FDX API specification

In Scope

It includes tracking (360 Portfolio view), trends, budgeting, reducing debt, savings, and investment management. Many apps, a.k.a. Data Recipients, provide a service that allows end users to pull all of their income, expenses, assets, and debts to a single place in order to provide a view on where they spend their money, calculate their net worth, and get help with setting goals.

Out of scope

This use case does not cover money movement or tax-related needs.

Account Owner Verification Certification Use Case

Please see the accompanying **Certification Use Cases Specification v5.1** spreadsheet for the recommended values of required, optional, or conditional for the data elements for the Account Owner Verification and Account Linking for Payments Use Cases.

In Scope

The purpose of this dataset is to verify that the owner of the bank account matches the end user of the application. This involves matching the following user-provided information with the user and account information on file with their financial institution:

- Partial Account#
- Name
- Address
- Phone
- Email
- Balance

Example entities that are in scope are Customer, AccountHolder, AccountDescriptor, Account (Deposit only).

These entities may reference sub-entities e.g., Customer entity references or Address sub-entity. The entity will specify whether a given sub-entity is required for the use case.

Out of scope

Extremely sensitive PII data - date of birth and tax ID - are currently **not** included in this use case.

Account Linking for Payments Certification Use Case

The data specified in this use case profile is required by applications such as Google Pay, Venmo, Robin, loan servicing firms, financial institutions (loans & payments) so that their primary product e.g., a loan, money movement facility, trading facility, etc. can be linked to an end-user's bank account for the purposes of depositing or withdrawing funds.

Some other similar examples are person-to-person payments, checkout/purchasing via bank debits, prepaid cards, payroll set-up, bill pay, and tax refund. The money movement action may be performed directly by the app, or by a payment processor that the app contracts with to perform the money movement functions. Here are some examples:

- End-user opens a trading account with Robinhood or Coinbase. The financial app requests the user to link their bank account by logging into the bank, and authorizing the connection. The end-user logs into their selected financial institution via the FDX API, and selects one of the accounts to link to the app. The app can now withdraw money to fund trades, or deposit proceeds from trades back into the linked account.
- End-user opens a mortgage with their bank. As part of the lending process, the bank requests the end-user to select an account to auto-draft the loan payments. The end-user logs into their financial institution via the FDX API, and selects one of the accounts. The bank is now able to draft the loan payments from the specified account.

In scope

- Real time payments covered. This is covered via the ACH routing and account number.
- This use case should cover all ways that rely on routing and account number to facilitate money transfer
- Covers account linking for both withdrawing and depositing of funds
- Account/ Routing information - Whether the real number or a substitute virtual that can be used on the specified payment network without any need to change how the payment network accepts the information today.
- Simple holder name information to assure payment is not rejected for name mismatch
- Confirm micro deposits through transaction data (Backup for account number/routing data) (15 Days Or Less)
- Wire information for disbursement
- Transactions are currently used to verify microdeposits, provide certainty of payment and verify account standing. Balances are used as indicator of sufficient funds. It is the opinion of the taskforce that these solutions will be superseded by better API capabilities that make full access to transactions and balances redundant. Till such time, access to transactions and balances is necessary for the use case.

Example entities that are in scope are - Customer, AccountHolder, AccountPaymentNetwork, AccountDescriptor, Account (Deposit only), Balances, Transactions (Base only, not the derived entities)

These entities may reference sub-entities e.g., Customer entity references Address sub-entity. The entity will specify whether a given sub-entity is required for the use case.

Out of scope

- Data for Account Owner Verification is not a part of this use case. Although AOV may be performed as part of setting up money movement, the data required for AOV is part of a separate use case.
- Data for payment clearing assurance, confirmation and reconciliation is not in scope. Although these may be integral to money movement apps, the transaction data required for these purposes is expected to be provisioned via PFM use case.
    - Confirm payment clearing through transaction data (15 Days, Sufficient For Enough Business Days For Clearing)
    - Confirm balance information for purpose of better assuring clearing of the payment