SSA Authentication Process

Remote Enrollment Process

- User must first agree to the Terms of Service and Privacy Act statements.
- Next the user is prompted for the following information:
  - Name
  - Social Security Number (SSN)
  - Address
  - Date of Birth (DOB)
  - Phone Number (optional)
  - Financial account information (optional)
- SSA attempts to verify the user-entered information against our internal records.
- If Name/SSN/DOB combination passes in our records, the following information is sent to Experian:
  - Name
  - DOB
  - Address
  - Telephone Number (if provided)
  - Last 8 digits of credit card (if provided)
- Experian provides fraud alert if applicable, address matching information, and credit card matching information (if provided).
- The user's address is matched against internal SSA records and Experian records.
- Experian then provides Out of Wallet (OOW) Questions if they can be generated for the user.
- The user provides answers to the OOW questions.
- The user's OOW answers are sent back to Experian for scoring. If the user passes the quiz, he or she will be able to set up his or her account without extra security. If extra security was requested and those verifications passed, the user is also mailed an upgrade code that will allow him or her to add extra security once it is received.
- Account setup involves self-selecting a user name and password, and choosing and answering three password reset questions. (These are asked if the user forgets the password, and if answered correctly, enables the user to reset his or her password without customer service intervention.) The user must also enter his or her email address in order to receive account notification via email.

In Person Enrollment Process

- User provides valid proof of identity with unexpired:
  - U.S. State Driver's License
  - U.S. State ID card
  - U.S. Passport/Passport card
  - U.S. Military ID card (CAC)
  - U.S. government employee ID card

  Note: If the ID document does not contain address, the user can verbally provide it.
- SSA personnel record the identity document information and verify the information against internal records.
- If the address cannot be verified with internal SSA records, the user is asked to consent to an Experian verification. The address will be verified with Experian's records as long as the user consents.
- Depending on the type of ID the user presented and the results of the address verification, the user may leave the office with the codes necessary to set up an account, or need to wait for a mailing.
- The user will go through the account setup steps remotely. Once he or she receives the activation code (either handed to user in person or mailed to his or her address of record), the user may go online and provide name, SSN and DOB as well as an activation code issued during the in-person transaction. Once that information is verified, the user can follow the account setup process detailed in the Remote Enrollment process.

Account Maintenance

- Users may complete any of the following account maintenance functions:
  - Change password
  - Update contact information, such as email address
  - Change password reset questions and answers
  - Add or remove extra security
  - Deactivate account
- Additionally users may recall a forgotten user name by entering their name, SSN, and DOB.
- Users may also reset their passwords remotely by supplying their user name and successfully answering all three of their previously selected password reset questions. If the user cannot remember those answers, he or she may also have a temporary password emailed to him or her.

How this meets NIST Standards

- Level 2 – No extra Security
  - NIST requires us to collect and verify a government ID number. That is done in our records when we collect and verify the name, SSN, and DOB.
  - NIST requires us to verify an address, which we do. We collect the user's home address and either verify it internally or with Experian.

- Level 3 – With Extra Security
    - NIST requires us to collect and verify a government ID number. That is done in our records when we collect and verify the name, SSN, and DOB.
    - NIST also requires us to collect and verify a financial account number. We do that and verify either internally or with Experian depending on the type of financial account information that is supplied.
    - NIST requires us to verify an address, which we do. We collect the user's home address and either verify it internally or with Experian.
    - NIST requires us to issue the credential in a manner that confirms the address. We do that by mailing the upgrade code to the address of record. The user does not have a Level 3 credential until that upgrade code is used and a second factor is bound to the credential. In this case, the second factor is a text-enabled cell phone. The user is then required to enter the user name, password, and a randomly generated code sent to him or her via SMS at every login.
- In Person Issuance
    - NIST does not require a financial account check for in-person Level 3 issuance, so none is completed. We also follow NIST guidelines regarding the issuance of the credential based on how the address is verified.

<u>Data Retention</u>

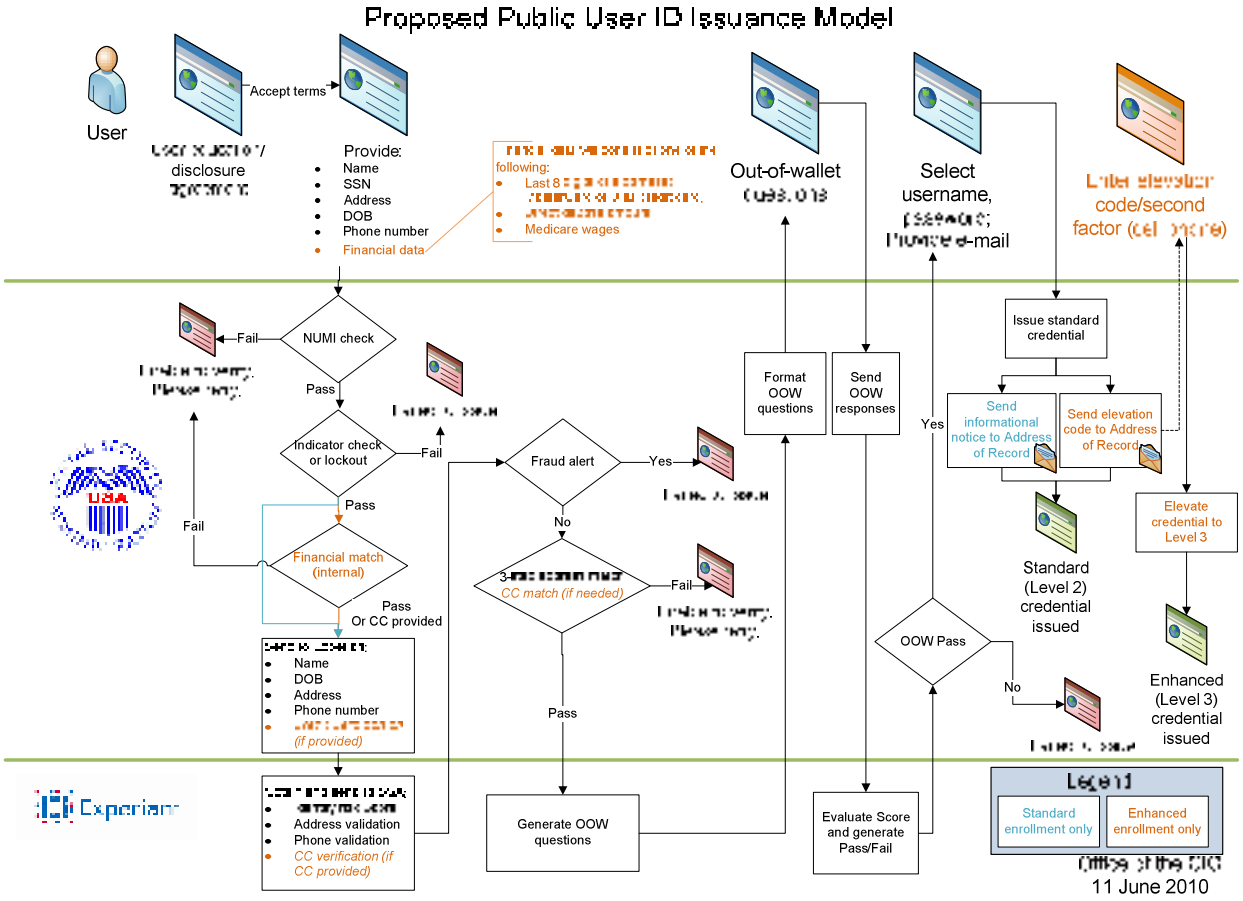
- SSA:
    - Uses existing authoritative agency records to confirm the user's name, SSN, and DOB. These are already stored in SSA records so they are not duplicated for the sake of ROME.
    - Retains email address to send account notifications to the user.
    - Does NOT retain the user's financial account information, nor do we retain OOW questions and answers.

- Experian:

    - Experian retains data that the user provides for limited purposes. SSA transmits information from the user (name, DOB, address, and phone number). Experian creates a PIN (internal linking key unique to the consumer). The PIN is used to pull various internal databases to allow for question generation, score calculation and other result codes. The consumer is presented with questions, provides answers and a decision is created for SSA. This information is stored in logs for 6 months online, then archived for 7.5 years.

    - Experian does this to satisfy legal requirements, in which case the PII data is only retrieved to support inquiries on individual consumers' behalf to investigate or dispute a decision. Experian cites the Fair Credit Reporting

Act and other regulations. NIST 800-63 guidance provides a retention period for federal agencies to keep registration data for Level 2 credentials a minimum of 7.5 years.


Proposed Public User ID Issuance Model
User
Accept terms
Provide:
Name
SSN
Address
DOB
Phone number
Financial data
following:
Medicare wages
Out-of-wallet
Select
username,
e-mail
code/second
factor
NUMI check
Fail
Pass
Indicator check
or lockout
Fail
Pass
Financial match
(internal)
Fail
Pass
Or CC provided
Name
DOB
Address
Phone number
(if provided)
Address validation
Phone validation
CC verification (if
CC provided)
Fraud alert
Yes
No
CC match (if needed)
Fail
Pass
Generate OOW
questions
Format
OOW
questions
Send
OOW
responses
Evaluate Score
and generate
Pass/Fail
Yes
OOW Pass
No
Issue standard
credential
Send
informational
notice to Address
of Record
Send elevation
code to Address
of Record
Standard
(Level 2)
credential
issued
Elevate
credential to
Level 3
Enhanced
(Level 3)
credential
issued
Experian
Legend
Standard
enrollment only
Enhanced
enrollment only
11 June 2010