# **Scenarios**

The following scenarios leverage a shared service model for consumer identity proofing and/or biometric capture to support program or account enrollment.

## Scenario 1: User fails remote online proofing and performs in-person proofing through a shared service

While preparing to establish and manage a legal agreement, a customer begins remote online proofing. Unfortunately, the customer is unable to pass remote online proofing and is directed to find a local USPS post office to complete In Person Proofing (IPP). The customer brings the barcode provided from the initial remote session to the local post office where the clerk inspects the customer, their photo ID, and secondary documents. The clerk examines the security documents and completes the IPP event. The customer returns to the AGENCY application and completes the AGENCY online registration gaining access to the application.

In the background, the agency may complete a search to direct the individual to a USPS location. USPS sends the results of the IPP event back to the agency.

## Scenario 2: User supplies biometrics as part of enrollment in a program through a shared service

An applicant for a travel program requires a biometric capture in order to complete enrollment. The applicant is directed to find a local USPS to verify their identity and capture their biometrics. The USPS clerk inspects the customer, their photo ID, and secondary documents. The clerk scans the security documents, captures the biometrics, and completes the IPP event. The customer returns to the online registration and completes it.

In the background, AGENCY creates an identity record to be verified by USPS with an indicator to capture the biometrics. Once completed, the biometrics and identity proofing details are submitted back to AGENCY. In this scenario, USPS does not review or share the biometrics except with AGENCY.

## Scenario 3: User provides proof of identity while mailing a form or application

A customer completes a benefits enrollment application requiring identity verification. The customer goes to their local USPS where the clerk inspects the customer, their photo ID, and secondary documents. The clerk scans the security documents, completes the IPP event, and accepts their paperwork. The identity proofing event is recorded in USPS systems and a retrieval code is assigned that is included in the package by USPS. The benefits organization can view the results of the identity proofing event using the code for a limited period of time and limited number of uses.

## Scenario 4: Mail clerk/carrier performs identity proofing while delivering a hardware authenticator, binding the identity to the authenticator

A customer ordered a hardware authenticator for remote access for work (or banking, etc.). The package indicates to the USPS that the customer must prove identity prior to package receipt. The carrier inspects the customer, their photo ID, and secondary documents. The carrier scans the customer’s photo ID and the barcode on the package – tying the proofing event to the hardware authenticator. The records are delivered to the employer (issuing company).

## Scenario 5: User fails remote online proofing and performs in-person proofing through a shared service at the user’s home

While preparing to establish and manage a legal agreement, a customer begins remote online proofing. Unfortunately, the customer is unable to pass remote online proofing and selects mail carrier verification to complete In Person Proofing (IPP). The customer selects which day they would like to get their identity proofed and is presented with window of time when their carrier will arrive at their house. When the mail carrier arrives, the customer provides the barcode from the initial remote session and the carrier inspects the customer, their photo ID, and secondary documents. The clerk scans the security documents and completes the IPP event. The customer returns to the AGENCY application and completes the AGENCY online registration gaining authorization to submit the application.

In the background, USPS sends the results of the IPP event back to AGENCY.

****

****

**USPS is well suited to provide value to agencies because of its established identity offerings, proven In-person Proofing (IPP) capability, retail footprint, vetted personnel, and mailing solutions**



USPS currently offers Passport enrollment for the Department of State at 4,800 locations nationwide, facilitating 6,500,000 passport applications in 2017 and has a MOU with NIST giving USPS the authority to provide in-person identification services to federal entities



USPS currently offers in-person proofing as a service (IPPaaS) at 3,000 USPS locations nationwide to support Informed Delivery, proofing 34,000+ USPS customers in 2017 with a 97% success rate



More than 80% of the US population lives within 10 miles of a “Premier Post Office” that can be equipped to facilitate IPP transactions, with locations in all U.S. states and territories



Many of the 600,000+ USPS personnel are vetted with a tier 1 background investigation and trusted by the American people, making them perfect to administer IPP for the AGENCY. Built-in Federal Law Enforcement through the US Postal Inspection Service



Existing USPS solutions such as Informed Delivery and Informed Visibility can provide all relying UES stakeholders with the insight needed to drive response completion and provide enhanced levels of validation