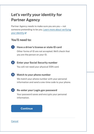
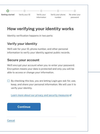
LOGIN.GOV

External use
Updated: July 18, 2024

Identity proofing with a state-issued ID





The user begins identity proofing.

They sign in or create an account before getting started with verifying their identity.

The user uploads their state-issued ID.

They can use their phone or computer to upload images of the front and back of their state-issued ID.

The user's images are sent to a vendor to be validated.

Login.gov checks the authenticity of the ID for security features and alterations to the image.

The images are discarded after checking the authenticity of the ID.

If the check fails 5 times, they must wait 6 hours to try again. They may also choose to verify in person at a U.S. Post Office.

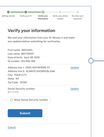
For identity proofing with a biometric comparison...

The user uploads their state-issued ID and takes a photo of themselves.

They must use their phone to take images of the front and back of their state-issued ID and their face.

The user's images are sent to a vendor to be validated.

The user enters their SSN.



The user verifies that their name, date of birth (DOB), address, and SSN are correct.

We obtain their name, DOB, and address from their ID. They can only edit their address and SSN.

Login.gov validates the name, DOB, and SSN against issuing or authoritative sources, and verifies that they belong to a single person.

If the check fails 5 times, they must wait 6 hours to try again. They may also choose to verify in person at a U.S. Post Office.

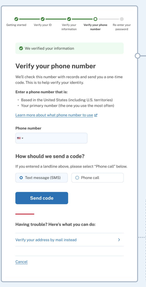
Does the user have a valid phone number tied to their name, DOB, and SSN?

YES

The phone number must be a U.S. number.

NO

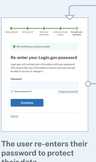
If the user has a valid phone number...



The user enters a one-time code to prove they have possession of the phone.

Login.gov verifies that the user's name, DOB, and SSN match the phone number by sending this information to authoritative sources.

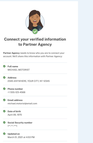
If the check fails 5 times, they must wait 6 hours to try again. They may also choose to verify in person at a U.S. Post Office.



The user re-enters their password to protect their data.

Login.gov provides the user with a personal key to use if they forget their password.

The user must confirm that they saved their personal key in a safe place to continue.



Identity proofing is complete.

Login.gov encrypts the user's PII. Only the user can decrypt and access it.

The user provides explicit consent to allow us to share any data with a service provider.

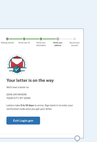
If the user does not have a valid phone number...

*Not available for biometric identity verification

The user confirms that they want to receive a letter to their address on file.

We obtain their address from their ID.

The user re-enters their password to protect their data.



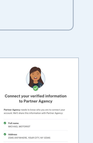
Login.gov sends the user a letter with a unique verification code and instructions by mail.

This verification code is valid for 30 days.

The user signs in to Login.gov and enters the verification code they received by mail.

Login.gov provides the user with a personal key to use if they forget their password.

The user must confirm that they saved their personal key in a safe place to continue.



Identity proofing is complete.

Login.gov encrypts the user's PII. Only the user can decrypt and access it.

The user provides explicit consent to allow us to share any data with a service provider.