

Analysis: Authentication and Identity Proofing Requirements in Unemployment Insurance Applications

On February 28, 2023, the [Digital Benefits Network](#) (DBN) released a [dataset](#) documenting authentication and identity proofing requirements that unemployment insurance (UI) applicants encounter across the United States.

In this document, we share high-level observations from our data on unemployment insurance applications and more information about our research process.

You can view the [dataset](#) for unemployment insurance applications as a spreadsheet or as a gallery organized by the 53 states and territories (listed below as states) that administer the program.

We invite you to provide input on this dataset using our [feedback form](#).



Contributing Authors



ELIZABETH BYNUM SORRELL
Researcher, Digital Benefits Network

As part of our ongoing research into [digital identity](#) in public benefits, the DBN is also working with Code for America to support similar analyses for SNAP, WIC, TANF, and child care applications, which will be released later this year. In our data collection, we aim to answer several questions, including:

- + When and how do residents need to create an online log-in to apply for benefits?
- + What kinds of personally identifiable information (PII) are applicants required to share when applying online?
- + When and how are front-end identity proofing steps incorporated into application processes?
- + What identity proofing methods are applicants asked to use?

Through this work, we hope to:

- + Create an easy-to-consult and readily updatable resource documenting the landscape of authentication and identity proofing practices benefits seekers may encounter when applying to programs across the country.
- + Make it easier for labor agencies, advocates, technology implementers, and federal agencies to see what other states and territories are doing.
- + Develop our own understanding of the varied approaches to login and identity proofing across agencies.

High-level Findings

The findings below outline our current understanding of authentication and identity proofing requirements and practices in unemployment insurance applications, as documented in publicly available information. As we continue to solicit feedback and update our dataset, these numbers may change. These points should also be understood as general observations to help users quickly make sense of this dataset.

Login/Registration Requirements

Most UI portals require users to register and create an account before applying.

- + 46 labor agencies required UI claimants to register or login before starting an application. The seven remaining agencies required users to create a login later to return to their claim or create a login later in the claims process.
- + 36 applications required users to enter an email to create an account.
- + We found evidence that 41 agency portals had some additional account security measures in place, including: security questions, email validation links, and authentication codes sent via email or SMS. Most applications that have additional authentication measures in place use more than one type/option.
- + Nine agencies use a state-wide single sign-on (SSO) system as the login for their unemployment portal. Three other agencies were using a federated identity management approach in which users accessed the portal using existing credentials from other providers (e.g. Google, Facebook, ID.me, etc.).

“Active” or “Front-end” Identity Proofing Requirements

Many labor agencies require claimants to complete some type of active identity proofing process (see more on our description of “active” or “front-end” identity proofing steps below).

- + Publicly available information indicated that 30 labor agencies required UI claimants to take active steps to prove their identities at some point before, during, or following the claims filing process.
- + For 13 agencies, it was unclear whether a program required identity proofing, or whether they required it for all claimants. Based on information in claimant guides and other documentation online, we found five agencies that do not require claimants to take active identity proofing actions. Based on available evidence, four other agencies require identity proofing only in some cases (Maine, Virginia, West Virginia, Wisconsin).
- + Of the 30 agencies that require identity proofing, we found information indicating that 10 mandate identity proofing actions before claimants could initiate an application and 11 incorporated identity proofing during the application process. Two state labor agencies (Nebraska and Oregon) require identity proofing after application submission, and two other state labor agencies (Iowa and Kansas) used or allowed for identity proofing after application submission, in addition to pre-application or in-application pathways. For the other five agencies that require active identity proofing actions, it was unclear when identity proofing would take place.

Identity Proofing Vendors

Many agencies are using or have used ID.me, but have incorporated the service into their process in different ways.

- + Many agencies (27) are currently using or have used ID.me. (As of late 2022, [ID.me](#) lists 24 state labor agencies as clients, and in our research, we found five agencies where it was unclear whether they are still using ID.me’s services—see our notes in the identity proofing vendor column).
- + Agencies have also integrated ID.me processes into their applications in very different ways. Nineteen states currently or previously using ID.me appeared to require all new claimants to verify with the service. (Two other labor agencies, Maine and Virginia, appeared to require verification with the service only in some cases, and the use of the service was unclear for six other agencies.)
- + Of the 30 agencies that require identity proofing, we found information indicating that 10 mandate identity proofing actions before claimants could initiate an application and 11 incorporated identity proofing during the application process. Two state labor agencies (Nebraska and Oregon) require identity proofing after application submission, and two other state labor agencies (Iowa and Kansas) used or allowed for identity proofing after application submission, in addition to pre-application or in-application pathways. For the other five agencies that require active identity proofing actions, it was unclear when identity proofing would take place.
 - + Of the 19 state labor agencies that currently or previously required all users to verify with ID.me, seven included the requirement in front of the application (meaning users could not initiate a claim without first verifying through ID.me). Seven agencies direct users to ID.me’s service during the application submission process, and one agency requires verification after the user submits a claim. (For four other labor agencies, it was unclear when during the claims process a user needed to verify with ID.me).
 - + Two state labor agencies (Idaho and Kentucky) also required applicants to use ID.me login credentials to access the claimant portal.
- + We found evidence that four state labor agencies (Iowa, Kansas, Rhode Island, and Wisconsin) are using LexisNexis Risk Solutions for knowledge-based verification (KBV), although [other research](#) shows this number is likely higher. We found information about LexisNexis contracts with Tennessee, Ohio, and Maryland, but were not able to confirm how LexisNexis service’s were being used.

- + The Illinois Department of Employment Security is using [Experian](#) Verification Services through the ILogin SSO and identity proofing service.

Identity Proofing Methods

There are a range of identity proofing methods in use, although the most common appears to follow the model of uploading identity documents and a video/live selfie.

- + Across labor agencies, we found that the most common “active” or “front-end” identity proofing method involved uploading identity documentation and a video selfie (observed for 23 agencies).
- + We found evidence that 10 state labor agencies used KBV as an identity proofing method.
- + We found evidence that nine agencies allowed claimants to mail, fax in, or present identity documentation in person.
- + Five state labor agencies (Arizona, Arkansas, Iowa, New Jersey, Oklahoma) appear to offer claimants choices in identity proofing methods; for example, Iowa appears to allow users who choose not to complete KBV, or cannot complete it, to upload or mail in their identity documentation.

State-specific Solutions

Some labor agencies are using state-specific solutions for their sign-on or identity proofing processes.

- + Nine state labor agencies had integrated their state’s single-sign-on (SSO) solutions into their UI claimant portal (Alaska, Illinois, Michigan, New York, North Dakota, Ohio, South Dakota, Utah, Washington). This means users could access the claimant portal with a login they might use for other government services in the state.
- + Some agencies were also using state-specific identity verification tools, like Illinois’s Department of Economic Security which was using ILogin (the state’s SSO) for sign-in and identity proofing for claimants. ILogin appears to use [Experian Verification Services](#) for identity proofing, using KBV questions.
 - + Other agencies, like the Oklahoma Economic Security Commission, did not have a state-login solution but were using in-house identity proofing solutions, [OKVerify](#).
- + We also found several agencies that had their own document uploaders for submitting identity documentation, but for some, it was unclear whether or how those were still being used.

PII Required to Submit

Driver’s license number or state ID number is frequently a required piece of PII for UI claimants.

- + In our digital identity data collection, we are interested in what types of personal identifiable information (PII) users must submit during an application process (not necessarily as part of a document upload for identity proofing). Claimants must provide a Social Security Number (SSN) to apply for unemployment insurance (see section [1137\(a\)\(1\)](#) of the Social Security Act). However, we were also interested in understanding when a driver’s license number or state ID number were required within the application process. For 18 unemployment applications, driver’s license number or state ID number appeared to be required. For nine agency applications, it appeared to be omissible or optional. For 24 agencies, we found information indicating that a driver’s license number or state ID number was not required within the application. For two agencies, the requirement was unclear.

Process + Protocol

Between October 1 and November 20, 2022, we collected publicly available information on unemployment insurance applications (from agency websites, application portals, claimant guides, news coverage, vendor websites, and contracting repositories). For UI applications, a valid SSN is often required early in the claims process. Because some state labor agencies appear to immediately check the validity of SSNs entered, we decided to not enter false SSN information or other “dummy” applicant data into these systems. We also did not register for accounts with these portals.

We spent approximately 90-100 minutes reviewing each state labor agency’s unemployment compensation application during initial data collection and quality checks. After completing an internal review of the data in early December 2022, we shared this dataset with members of the [UI Technology Coordinating Coalition](#) for feedback and made small modifications based on responses. When entering information into our dataset, we erred on the side of leaving fields blank or marking specific columns as “unknown” if there were contradictions or ambiguities in the information we found. We have also used the “Public notes” column in our dataset to document those complexities and open questions.

In our data collection, we differentiated between processes that cross-check user PII on the back-end, and “active” identity proofing steps that users must complete to successfully apply. For that reason, our dataset includes multiple data collection fields to capture information related to the identity proofing process and checks of identity data.

Identity-related Fields

Data Field	Entry Options	Details
Is a driver’s license or state ID # required?	“Yes,” “No,” “May be optional”	Documenting whether a driver’s license or state ID # appears to be required information in the application process (separate from requirements to upload images of a driver’s license or other photo identification)
Did we find information on visible parts of the application or website indicating that the system will run back-end checks or comparisons on PII to confirm identity/eligibility?	“Yes,” “No”	We can assume that many applications are comparing self-asserted PII to other sources. Through our data collection methods, we were not able to gather detailed information about how agencies are checking PII against other data sources, but want to document how uses of PII are made explicit to applicants. We recognize that because we were not completing UI claims, we may not be able to fully capture how this type of information is presented/when.

Data Field	Entry Options	Details
Database/source comparisons (back-end)	Text Entry	If we know an agency is checking applicant PII against other sources, what data sources do they say they are using?
Active identity proofing required?	<p>“Yes,” “No,” “Optional,” “Not Always,” “Unknown”</p>	<p>In this column, we want to document when applicants are required to take active steps on the front-end to verify their identity. There may not be sufficient information to assess this, in which case we marked this field “unknown.” When marking this column “No” (meaning no identity proofing required) this determination is based on information about the process (e.g., instructional video, claimant guide) that makes it reasonably clear that there is no active identity proofing required.</p>
When may active identity proofing methods be used?	<p>“Before initiating application,” “During application submission,” “After application submission,” “Optional,” “Unknown,” etc.</p>	<p>This field was a multi-select field, allowing us to select multiple options where relevant. For example, sometimes identity proofing is required during the application, but a user may also be able to complete a verification process later.</p> <p>“Before initiating application” capture cases where we found evidence to suggest that a claimant would need to verify their identity before creating an account on a portal, during account creation, or immediately after registering an account. “During application submission” captures cases where we found evidence indicating the identity proofing process might happen at some point during the claims filing process, but after an initial registration.</p>

Data Field	Entry Options	Details
Active identity proofing methods	E.g., Video selfie + ID document upload, KBV, etc.	Here we document all the front-end identity proofing methods for which we found evidence.
Choice in identity proofing	Checkbox	We used this field to capture whether a user appears to have a choice in the method of identity proofing they undertake, if identity proofing is used. Check mark indicates “yes, there is a choice.”

Feedback

This data represents a point-in-time. We also know that the public information we were able to access may not reflect the most up-to-date experiences of claimants, and that these application requirements and processes can be complex. We are publishing this dataset openly at this stage of our research to help share knowledge and also to solicit feedback and engagement. We hope that users who visit the dataset will help ensure the accuracy of the data, fill in gaps, and share ideas for further extensions of this research.

To submit feedback about a state or territory’s application included in the dataset, you can use our designated [feedback form](#). We are grateful for the feedback and input we have already received from members of the [UI Technology Coordinating Coalition](#) and others working on UI improvements, and we are eager to continue soliciting additional feedback. If you have other questions or comments, or interested in talking more about this work, we encourage you to reach out to us at digitalbenefits@georgetown.edu.



Get in Touch

Our Digital Benefits Network team is here to help!

Visit us at the [Digital Benefits Hub](#)

Please contact us with any thoughts, questions, or potential collaborations via email at digitalbenefits@georgetown.edu