Digital Identity in Public Benefits Applications: Balancing Equitable Access + Risk Reduction

In the U.S., when someone applies for benefits online, they may encounter different login processes and requirements designed to validate their identity.

When an applicant is asked to log in to apply for services, requirements can range from a quick sign-up with a username and password to a more involved registration process that requires various pieces of information including phone numbers, addresses, and other information. Different login protocols also use various forms of authentication security such as one-time text message codes, required security questions, or third-party authentication applications.

Some applications may also require an applicant to take additional steps to confirm their identity. In a benefits application process, identity checking steps can range from background-level comparisons of an individual's self-asserted personal information with outside databases to knowledge-based verification (KBV) questions that present users with a series of questions about their private information like credit history to biometric comparisons using facial recognition technologies. (To read more about the multiple distinct steps of identity proofing, see definitions in our glossary on digital identity terms).

Contributing Author

Elizabeth Bynum Sorrell
Researcher, Digital Benefits Network, Beeck Center for Social Impact + Innovation
Process Matters

The processes that agencies incorporate into applications matter. Login requirements may allow users to return to a partially completed application at a later time, but those same sign-up procedures and login requirements could also become barriers. Although their study looked at government employees rather than benefits seekers, researchers have suggested that repeated authentication requirements can become burdens for users and recommend instituting more user-centered, implicit authentication requirements. Complex password requirements may also make it more difficult for users to access their accounts.

Identity proofing requirements and automated fraud detection incorporated into benefits applications may help prevent theft, but some solutions also create new challenges for eligible claimants. For example, automated fraud detection processes may be relatively frictionless for many users, but as explained in the U.S. Digital Response’s Identity Proofing for UI report and New America’s Playbook for Improving Unemployment Insurance Delivery, detection mechanisms, like flags on multiple claims submitted from the same address, may block rightful claimants and disproportionately affect marginalized communities.

While the overall data related to identity proofing obstacles is limited, there is evidence to suggest benefits administrators need to think carefully about how identity proofing steps are incorporated into benefits applications. In their work with the IRS Volunteer Income Tax Assistance (VITA) program, Code for America found that 88% of their clients halted the application process when they were asked to complete identity verification steps using an external portal.

Knowledge-based verification questions — sometimes also referred to as remote identity proofing or RIDP — can create obstacles for people with limited credit history, as well as immigrant parents applying for services on behalf of their children. Additionally, because of data breaches, answers to these types of questions, which include questions about cars owned, previous loans, or past addresses, may not actually be secret. The National Institute of Standards (NIST) has outlined limits on the use of knowledge-based verification questions for identity proofing. In 2019, the Government Accountability Office also issued guidance recommending that several federal agencies discontinue using knowledge-based verification practices and strengthen their identity proofing processes.

The use of biometric comparisons for identity verification, such as facial comparison software to evaluate a selfie against a government ID — a technique introduced by many state workforce agencies during the pandemic and proposed by the IRS — can present accessibility and equity issues for individuals who are unable to successfully complete the process. Such use cases also raise broader questions about privacy and transparency.
The most recent comprehensive analysis of authentication and identity proofing practices across major benefits programs comes from Code for America. Their 2019 assessment of online application processes including the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), Special Supplemental Nutrition Program for Women, Infants, and Children (WIC), Low-Income Home Energy Assistance Program (LIHEAP), and Medicaid programs in U.S. states found that, at the time, about 75% of available online applications did require registration or login. Approximately 15% of applications required identity proofing.

Given the increased need for remote access during the pandemic, it is very possible that the use of login and identity proofing practices in benefits programs has shifted in the past few years. The Digital Benefits Network team is also working with Code for America to produce updated analyses of identity proofing and login requirements in SNAP, WIC, TANF, and child care applications which will be released next year.

**Identity Proofing Impacts in Unemployment Insurance**

The case of unemployment insurance during the pandemic illustrates the potential impact of identity proofing processes. In an effort to respond to national needs, the government established the Pandemic Unemployment Assistance (PUA) program in 2020, for which a record number of people were eligible. The surge in unemployment applications generally and new pandemic programs meant states faced heavy workloads, leading to backlogs in claims processing. Attempts to get money out the door quickly, however, created opportunities for fraud. Media coverage has detailed fraud in pandemic programs. New York State, for instance, lost $11 billion in potentially fraudulent unemployment payments. The U.S. Department of Labor Office of the Inspector General recently increased their estimate of potentially fraudulent unemployment insurance program payments to $45.6 billion paid out between March 2020 and April 2022.

The scale of fraud indicates a clear need for programmatic adjustments. However, efforts to curtail fraud and institute new safeguards and identity proofing checks may also create accessibility issues and contribute to longer wait times and delays for claimants in a system that already faces backlogs. These efforts can also make identity verification processes a de facto part of eligibility determinations and raise complex issues around privacy and data security, especially when identity proofing relies on biometric verifications such as facial recognition. As legal scholar Michele Gilman argued, these harms may be most significant for already vulnerable groups, who may lack access to identity documentation and have fewer resources to help them navigate new processes.
The future of successful online access to benefits applications will require solutions that navigate accessibility and fraud prevention challenges, without sacrificing usability and equity. In our ongoing research on digital identity, the Digital Benefits Network (DBN) will continue documenting and advocating for new approaches to identity proofing and authentication that minimize burdens on applicants and create a smoother experience for beneficiaries and frontline workers. You can read more about digital identity on the Digital Benefits Hub, and find our other introductory resources including:

+ A glossary of digital identity terms,
+ An overview of digital identity broadly,
+ An overview of federal interest in digital identity.

Agencies and individuals interested in our research about digital identity can subscribe to the DBN and follow updates. If you would like to discuss our research further, or are interested in sharing your own experiences administering identification and authentication processes in a benefits program, we encourage you to reach out to us at digitalbenefits@georgetown.edu.