Digital Identity in Public Benefits

CONTRIBUTING AUTHOR — SEPT. 2024

Elizabeth Bynum Sorrell
Senior Research + Engagement Manager, Digital Benefits Network

GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

People across the United States regularly apply for and manage their public benefits online. To use online applications and portals, they may be asked to create a username and account. In some cases, they may also have to prove who they are by verifying their identity. The Digital Benefits Network started researching digital identity in public benefits in late 2022. Our research so far has included:

- Landscape research documenting authentication and identity proofing practices in initial online benefits applications;
- A guide to federal government activities related to digital identity; and
- A review of promising digital identity design patterns.

We started this work because we recognize that digital identity can present challenges for public benefits applicants and beneficiaries. State agencies also face challenges protecting beneficiaries' information while balancing access. In this updated primer, we:

- Describe how identity proofing and authentication show up in public benefits applications; and
- Outline equity and security concerns raised by common identity proofing and authentication methods.

Identity Proofing + Authentication in Public Benefits Applications

Some online public benefits applications require users to make an account or prove their identities.

In some cases, the account registration process might be a quick sign-up with a username and password. Other processes are more involved, requiring phone numbers, addresses, and other details. Some portals also use further account security measures for account re-access, like:

- One-time passwords sent via text message or email,
- Security questions, or
- Third-party authenticator applications.

Authentication and Account Creation

Authentication is how a service provider tries to confirm that a person accessing an account is the *same* person each time. (Read more in our glossary).

Authentication processes rely on a user having established an initial account. The DBN is interested in both:

- Account creation/registration, or the initial process of establishing a user account with a service, like a benefits portal; and
- Authentication—the process of authenticating access when returning to an account.

Many benefits systems compare a person's identifying information with outside sources to help understand who an applicant is. (For example, the Integrity Data Hub for Unemployment Insurance (UI). There are also many data sources that agencies may use to understand individuals' and households' income and eligibility.) In some cases, applicants may also have to take active steps to prove their identities. Sometimes this involves knowledge-based verification (KBV). KBV presents users with questions based on their personal information, like credit history. In other cases, biometrics are used, and applicants or beneficiaries might have to upload a photo identity document and a selfie. That selfie is then compared by an automated system against the user's photo ID. Account creation and identity proofing, if used, often occur during an initial application process. However, in some cases, claimants may create an account after submitting an initial application, or be asked to undergo identity proofing after they've applied.

Prior to the COVID-19 pandemic, some benefits portals already incorporated account creation and identity proofing. The pandemic made online, remote access to benefits applications and systems more important than ever. As state agencies worked hard to deliver benefits during the pandemic, they also encountered new challenges. For example, state workforce agencies were targeted by organized criminal groups as new programs like Pandemic Unemployment Assistance (PUA) were created and existing safeguards, like employer verifications, were removed. Many state workforce agencies responded by instituting new identity proofing checkpoints.

There is not much public data on how identity proofing impacts beneficiaries, in UI or other programs. There is, however, significant evidence from media and advocates that identity proofing in UI programs created barriers for claimants during the pandemic. Conducted primarily through contracts with private-identity vendors, identity proofing created delays for claimants, introduced obstacles for people who lacked strong internet access, exacerbated language access issues, blocked individuals who lacked ready access to identity documents, and raised due process questions as well as data security and privacy issues.

Outside UI, in their work with the Internal Revenue Service's (IRS) Volunteer Income Tax Assistance (VITA) program in 2020, Code for America found that 88 percent of clients abandoned the process when asked to complete identity verification through an external portal. As legal scholar Michele Gilman argues, groups who lack access to identity documentation or have fewer resources to navigate online processes may be most impacted.

How identity proofing and authentication operate matters not just at the moment of an initial application, but during renewal and recertification processes as well. This became especially clear during the Medicaid unwinding, when it was imperative that beneficiaries could easily re-access accounts and cases to submit information. For more on issues related to identity proofing in Medicaid, see this publication from the Center on Budget and Policy Priorities.

In 2023, the DBN published a report and open dataset cataloging authentication and identity-proofing practices in online benefits applications. We established a data-sharing partnership with Code for America to facilitate our research and support their Benefits Enrollment Field Guide. Our research identified key trends across SNAP, TANF, MAGI Medicaid, Childcare, WIC, and UI applications:

Across programs, most online applications require users to create an account before they can apply for benefits.

+ Two-thirds of those account creation processes require users to provide an email address.

About a third of online applications require or prompt identity proofing steps during the application.

+ Identity proofing is most common in UI applications. Outside unemployment insurance, identity proofing was most common for applications that included MAGI Medicaid.

Identity proofing methods vary across programs.

+ We found evidence that 22 labor agencies were using biometrics for identity proofing.
+ Other programs used KBV rather than biometrics.

Code for America compared their 2023 Field Guide to the assessment of online applications they conducted in 2019. They found a 75-percent increase in identity-proofing requirements or nudges in 2023 as compared to 2019. The DBN will be releasing an updated version of our dataset in late 2024.

Methods Matter

Security and Equity Challenges

KBV questions can create obstacles for people with limited credit history. KBV may also be a barrier for immigrant parents applying for services on behalf of their children. Because of data breaches, answers to KBV questions may also not be secret. The National Institute of Standards (NIST) has outlined limits on the use of KBV. In 2019, the Government Accountability Office recommended several federal agencies stop using KBV. Approaches to identity proofing—like KBV—which rely on a private company holding large amounts of information about individuals, also raise privacy concerns.

Use of biometrics for identity proofing also presents potential issues. Facial recognition technologies (FRT) refer to digital tools used to perform different kinds of tasks on images or videos of human faces, from determining if a face is present in an image to determining whose face is present. The use of FRT, whether for "face verification" or "face identification," raises broader questions about privacy, data sensitivity, and surveillance, including:

- Who has access to facial images;
- How is that data stored and used; and
- How long is this type of data held.

1:1 COMPARISONS	1:MANY COMPARISONS
An image or recording of a face is compared against an existing image of a person's face to verify a person is who they claim to be.	An image or recording of a face is compared against many other faces in a gallery to find a match and identify someone.

When information like a password or username leaks in a data breach, it's possible to change it. It may be harder to re-secure your private data if leaked information includes biometric data. Questions about data security and privacy can become especially urgent when private companies own the data. Growing use of artificial intelligence means there are also potentially new security challenges for FRT systems from deepfakes.

Beyond data security, FRT can pose equity problems. Research (from NIST and other academics) found biases in commercially-available facial recognition algorithms. These biases mean these tools may be less good at identifying faces of Black, Asian, and Native American individuals. Although accuracy may be improving, social scientists have raised concerns about the ways that FRT may reify racial and gender categories. False positive and false negative outcomes produced by biometric systems can also be serious. In the public benefits context, a false negative may block an eligible applicant from applying.

There is no comprehensive federal regulation or legislation related to biometrics. However, federal agencies are evaluating biometric technologies and their use for identification. For example:

- The General Services Administration is currently conducting an equity study of remote identity proofing. The study's report, examining performance of proofing checks, like facial verification across different sociodemographic factors, will be released in fiscal year 2025.
- In early April 2023, the U.S. Department of Labor's (DOL) Office of Inspector General released an alert memo pointing to "urgent equity and security concerns" regarding the use of facial recognition technology in unemployment insurance programs.
- DOL's Employment and Training Administration released Unemployment Insurance Program Letter (UIPL) No. 11-23 in July 2023. The letter "encourage[d] states to carefully review ID verification/proofing solutions that use biometrics such as facial recognition" and noted that states using facial recognition technology for identity proofing "must test the system for biases."
- In April 2024, the Government Accountability Office released a report examining the state of biometric identification technologies and pathways to address areas of concern about their use.

"Lower friction" methods to evaluate applicant's activity online—like fraud detection tools—also present challenges. In early 2024, the Electronic Privacy Information Center brought a complaint to the Federal Trade Commission arguing that a fraud detection tool commonly used by states may regularly be inaccurate.

While identity proofing is more often discussed as a barrier for applicants and beneficiaries, account creation and authentication practices matter too. Having reliable, secure access to an online account can enable users to:

- Log back into a portal later;
- Save their progress and complete an application over multiple sessions;
- Check their application status;
- Provide additional documentation; or
- Manage their case after they have been determined eligible for benefits.

We know from research in other contexts that burdensome authentication practices might nudge users to avoid applications or find workarounds. When authentication is deemed important for a particular interaction, public benefits programs should align authentication strategies with wider security best practices. This might mean not requiring passwords with special characters, or regular password updates. It's also important to consider usability for specific populations. For example, will a third-party authenticator application work well for a particular group? Additionally, authentication strategies need to conform with program requirements. For example, the U.S. Department of Agriculture's Food and Nutrition Service (FNS) has previously stated that applications for SNAP cannot require users to submit an email address, and any account registration must provide a simple system to set up usernames, application numbers, and/or passwords.

Conclusion

As we outline here and in other publications, there is some consensus about the challenges agencies and beneficiaries face when it comes to digital identity in public benefits.

Going forward, the DBN is eager to collaborate with partners and state agencies to evaluate programmatic needs and risks. We believe state agencies should use resources like the NIST guidelines and risk assessment framework to determine whether and at what level authentication and identity proofing solutions are necessary for a given benefits program context. State agencies should consider what data is available to streamline verifications, including for identity when relevant. We hope to explore how clearer guidance and implementation materials can empower state agencies to effectively assess their digital identity practices to prioritize access and information security.

GET IN TOUCH

In our future work on digital identity, we will focus on the public benefits space, while keeping the larger landscape in mind. To engage with the DBN on this topic, please visit our Digital Identity Community of Practice page, or reach out via digid@georgetown.edu.