

Why Modern Identity Authentication is Key to Fighting Fraud



Advanced identity authentication technologies are giving public agencies powerful tools to fight fraud as it streamlines the experience of applying for government benefits. It can't happen soon enough. The fallout from COVID-19 protections exposed widespread weaknesses in automated systems for disbursing government money across the United States. Fraudsters stole billions of dollars while millions of unemployed Americans endured frustrating, hard-to-use online applications. Fraud is just one example; bad actors are targeting and exploiting weaknesses across a variety of government systems.

This issue brief from the Center for Digital Government (CDG) explores the importance of identity authentication technologies for state and local governments as they protect themselves from fraud and cybercrime. Experts in government IT and identity authentication discuss the opportunities and challenges of these new tools — and the keys to deploying them effectively.

IDENTITY AUTHENTICATION CREATES OPPORTUNITIES FOR AGENCIES

In March 2021, the U.S. Department of Labor reported that states issuing unemployment benefits paid out more than \$88 billion improperly through fraud or error.

The bureau of COVID-related fraud left state officials reeling. "It was daunting, unbelievable," said Kelly Johnson, CEO for the Kansas Department of Labor, in a recent [interview](#). Labor his colleagues at state unemployment agencies across the nation, Johnson found evidence of both bots on websites and data. Johnson's staff worked with a vendor to develop a solution designed to distinguish between bots and real people. Within 10 hours of deployment, the new tool had blocked nearly a half-million attempts to breach the data.

"Needless to say, this was a huge relief for our agency," Johnson said. Modern identity authentication software like what the Kansas Department of Labor designed is multifaceted and takes advantage of multiple tools, including:

- **Bot detection** — Software designed to recognize bot activity
 - **Verification proofing** — The act of verifying an individual's identity based on information aggregated from public and proprietary data sources before issuing their benefits or providing them information
 - **Personalization** — A set of rules designed to enhance customer security by encouraging users to employ strong passwords and use their phones
 - **Device authentication** — A mechanism designed to ensure only authorized devices can connect to a given network, site or service
- It acts as an open platform that connects with other systems to create powerful capabilities — such as tapping into social databases

with machine learning algorithms that learn to search for patterns, revealing both bad actors and everyday people applying for government benefits.

Digital identity authentication can save agencies money and enhance public trust in government digital services. And it's a technology solution that many consumers are used to. Large commercial enterprises, such as banks and health providers, use identity management to protect sensitive services and accounts and offer their customers access through any point device (desktop or mobile). A well-thought-out system can streamline public services while reducing rates of botware and other cyberattacks. Moreover, public agencies can build and safety their centralized identity pools — consisting of good actors and bad actors — to reduce IDA, duplication and inefficiencies.

For instance, a data collection department could use identity authentication tools to confirm that survey members are eligible to vote online. These systems can also accurately establish the identity of people who lack bank accounts and other means of verification, which can be a major barrier to the neediest people.

IDENTITY AUTHENTICATION CHALLENGES FACING GOVERNMENT AGENCIES

What happened to unemployment systems can happen anywhere in the future. It's not just the result of a single attack, claiming taxpayer money. It's manual verification processes and slow, nagging user experiences in online applications which force users to find shortcuts and workarounds that create vulnerabilities.

While people in need wait too long for their funds, fraudsters circumvent the line. During the pandemic, agencies on the Dark Web deployed tools enabling identity theft on a global scale. The tools used personal information like addresses, phone numbers, and Social Security numbers stolen in cyber breaches and phishing scams. Real data enabled these benefits claims.

"We're seeing fraudsters in several states having billions of fraudulent claims for unemployment," says Ryan Schellen, senior solutions engineer at DMG, which specializes in identity and access management software.

And the threat is continuing. DMG's attacks and policy-based, brute-force attempts to secure passwords are among the tactics in the cybersec toolbox.

"It's happening everywhere," agencies are just inundated across the board," says Zach Webers, director of fraud and identity solutions

MODERN IDENTITY AUTHENTICATION SOFTWARE IS MULTIFACETED, TAKING ADVANTAGE OF TOOLS AND APPROACHES LIKE BOT DETECTION, IDENTIFICATION PROOFING, PASSWORD POLICIES AND DEVICE AUTHENTICATION TO ENSURE PEOPLE ARE WHO THEY CLAIM TO BE.

Advanced identity authentication technologies are giving public agencies powerful tools to fight fraud and streamline the experience of applying for government benefits. It can't happen soon enough. The fallout from COVID-19 protections exposed widespread weaknesses in automated systems for disbursing government money across the United States. Fraudsters stole billions of dollars while millions of unemployed Americans endured frustrating, hard-to-use online applications. Fraud is just one example; bad actors are targeting and exploiting weaknesses across a variety of government systems. This issue brief from the Center for Digital Government (CDG) explores the importance of identity authentication technologies for state and local governments as they protect themselves from fraud and cybercrime. Experts in government IT and identity authentication discuss the opportunities and challenges of these new tools — and the keys to deploying them effectively.