WHY MODERN IDENTITY AUTHENTICATION IS KEY TO FIGHTING FRAUD

How a multi-layered approach helps government agencies ensure people are who they say they are

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.

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 $63 billion improperly through fraud or errors.

The tsunami of COVID-related fraud left state officials reeling. "It was becoming unbearable," said Kelly Johnson, CIO for the Kansas Department of Labor, in a recent webinar.

Like his colleagues in state unemployment agencies across the nation, Johnson faced swarms of bots bent on swindling the state. Johnson's relief arrived with a modern software solution designed to distinguish between bots and real people. Within 14 hours of deployment, the new tools had blocked nearly a half-million attempts to defraud the state.

"Needless to say, this was a huge relief to our agency," Johnson said.

Modern identity authentication software like what the Kansas Department of Labor deployed is multilayered and takes advantage of multiple tools, including:

- **Bot detection** — Software designed to recognize bot activity
- **Identification proofing** — The act of verifying an individual's identity based on information aggregated from public and proprietary data sources before issuing them creditials or providing them information
- **Password policies** — A set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly
- **Device authorization** — A mechanism designed to ensure only authorized devices can connect to a given network, site or service

It rests on an open platform that connects with other systems to create powerful capabilities — such as tapping massive databases with machine learning algorithms that scan in search of patterns revealing both bad actors and everyday people applying for government benefits.

Optimal identity authentication can save agencies money and enhance public trust in government digital services. And it's a technology solution that many constituents 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).

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

A well-thought-out system can streamline public services while reducing risks of ransomware and other cyberattacks. Moreover, public agencies can build and safely share centralized identity pools — consisting of good actors and bad actors — to reduce risk, duplication and inefficiencies.

For instance, a state corrections department could use identity authentication tools to confirm that family members are eligible to visit inmates. These systems can also accurately establish the identity of people who lack bank accounts and other means of verification, which can be a major boon 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 deluge of bots chasing taxpayer money. It's manual verification processes and slow, aggravating 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, operators on the Dark Web deployed bots enabling identity theft on a global scale. The bots used personal information like addresses, phone numbers and Social Security numbers stolen in cyber breaches and phishing scams. Real data enabled fake benefits claims.

"You're seeing headlines in several states having billions of fraudulent claims for unemployment," says Ryan Schaller, senior solutions engineer at Okta, which specializes in identity and access management software.

And the threat is continuous. DDoS attacks and proxy-based, brute-force attempts to secure passwords are among the tactics in the criminals' toolbox.

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

at LexisNexis Risk Solutions, which combines data and analytics technologies to thwart cybercriminals and other malicious actors.

Fortunately, the tools to address these challenges are rapidly maturing.

USING IDENTITY AUTHENTICATION TOOLS TO MITIGATE DIGITAL FRAUD

Identity authentication providers like Okta and LexisNexis Risk Solutions often pool their resources to fend off fraudsters. Why team up? Because cybercriminals deploy sophisticated networks of bots, beating them requires a modern approach.

"It takes a network to fight a network," Watkins explains. The two companies' technologies comb vast databases containing data like the IP addresses of known bad actors. Their solutions work in layers, aiming to stop intruders as soon as possible while enabling authentic users to pass through.

The first layer uses identity assurance tools that recognize the typical behaviors, locations and devices of authentic users before they even log in. "We do this from a consortium approach," Watkins adds. Everybody in the consortium has up-to-date data on likely fraud actors and tactics and uses it to weed out the bad actors before password attempts can be made.

Success at the identity assurance layer creates the necessary context for passing the user on to the authentication layer, where passwords and other data help establish the bona fides of the user. Once accepted past the authentication layer, the verification layer is next. Here, the software may send a one-time passcode (multifactor authentication, or MFA) to the authentic user's cell phone or land phone — which was entered when the account was originally created. MFA is a core component of Zero Trust architectures and happens via SMS, or a push to a mobile device or even a phone call. The more options that exist, the more inclusive an agency can make the service.

Once through the verification layer, identity proofing is the next layer. In this layer, the user passes through solutions that verify the Personally Identifiable Information (PII) of the individual before passing constituents to the final step of the authentication layer. In the authentication layer, the agency can choose which type of step-up authentication solution best fits the states' population. Step-up authentication can range from sending a one-time password to a verified mobile phone number to authenticating the driver's license of an individual against a selfie of that individual.

While it may seem like a lot of gates to pass through, modern identity authentication solutions are frictionless to a constituent and can bring an authentic user through all the layers in about a minute. And, it's an approach that can be deployed once and support many different government services and systems. For government agencies, this multi-layered approach provides a means to centralize their technologies to protect against fraud and streamline the user experience.

"It's like one single place to cut off malicious attempts," Schaller says. "It allows you to thwart attacks, stop the bleeding and then keep everything organized." Without this approach, agencies may have identity data and fraud-fighting attempts sprawled across multiple systems.

An identity authentication strategy must make it easy to adopt new frameworks or software development kits that are bound to arise as versions move from 1.0 to 5.0. Agencies also should look for tools with potential beyond their immediate needs.

"It's important to deploy something that you can leverage for other initiatives," Schaller says.

SUCCESSFULLY DEPLOYING AN IDENTITY AUTHENTICATION SOLUTION

The Kansas Department of Labor implemented its identity authentication in less than three weeks. "It was like night and day," Johnson said. With software blocking the botnets, IT systems ran like they were supposed to. CPU usage was back to normal for the first time in eight months. "The implementation was elegant because we did not have to do hundreds of hours of coding changes because the solution actually integrated into our internal databases," Johnson added.

Every agency will face unique fraud mitigation challenges, depending on its existing IT systems, the skills of its people and its security goals. The best identity authentication solutions orchestrate APIs to tap multiple databases and learning algorithms that understand the context of people's behavior when they log into a system. If somebody is applying for health benefits in Utah, then why are they using an overseas IP address?

The system must answer these kinds of questions accurately to best serve eligible beneficiaries while locking out everybody else. Constituents and agency staff will need training and education.

The key lies in finding the right partners who can map a solution to an agency's unique challenges. "One thing is always to leverage subject matter experts in the process," Schaller says. Partners should have extensive experience in delivering proven technology to government agencies, and a track record of fending off fraudsters.

Johnson said that executing identity authentication software does not have to be daunting or time consuming. The tools can be up and running on tight schedules — days or weeks vs. months or years. "The key to this was that we were able to use our current systems and only update our in-house databases," Johnson said. "It's effective, it's made a change for the people that we serve and it's been felt at all levels. So, I cannot say enough about the teamwork between our partners."

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Okta and LexisNexis Risk Solutions.

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

For: okta

State and local agencies can trust Okta to accelerate and modernize citizen service delivery. Learn about Okta's centralized, secure Zero Trust identity platform at www.okta.com

For: LexisNexis® RISK SOLUTIONS

For more information, visit: https://risk.lexisnexis.com/government or contact LexisNexis Risk Solutions at 1-800-869-0751