HOW MODERN IDENTITY PLATFORMS HELP STATES STOP FRAUDULENT CLAIMS

Instead of losing millions to fraudulent claims, states can protect their budget dollars and improve citizens' online access to services with a modern identity and access platform.

StateScoop Report

As state and local agencies continue to make critical investments to digitize citizen services, they're also having to devote greater attention to mitigating the increasing rate of fraud. From unemployment insurance to rental and food assistance programs, and various other public welfare programs, fraudulent claims pose a growing burden on the ability of state governments to serve their most vulnerable constituents.

As much as $39.2 billion in funds handed over to states through the Coronavirus Aid, Relief and Economic Security (CARES) Act were paid out improperly, including fraud, as of January 2, 2021, according to a May 2021 Department of Labor *inspector general's report*. Moreover, the report found 40% of states did not perform required and recommended improper payment detection activities, attributing much of the failure to antiquated IT systems and inadequate staffing.

By the end of 2021, individual state audits highlighted that the longstanding challenge of identifying and stopping fraudulent claims and payments was no closer to being solved. Inundated with requests during the COVID-19 pandemic, states like *Colorado* identified $73.1 million in potentially fraudulent benefits payments between March 1, 2020, and April 30, 2021, while *Ohio* filled approximately $477 million in fraudulent unemployment assistance claims over a similar period, according to respective state auditors.

The severity of the IT problem to secure and respond to cyberthreats requires a more coordinated effort to modernize IT systems. That's why federal institutions, including *Congress*, the *White House*, the *Department of Labor*, the *Department of Justice*, and the *Department of Homeland Security* have all increased funding grants that support federal, state and local governments' initiatives in these efforts.

"The success of these initiatives and the ability to deliver efficient services digitally will depend, in part, on stronger citizen identity proofing," suggests Ryan Schaller, Senior Developer Specialist, Citizen Identity and Access Management (CIAM) at Okta.

"As states move closer towards a purely digital service the footprint with which fraud could happen will only grow more prevalent. The way individual cybercriminals and growing crime syndicates are organizing to expand their reach shows that threat actors are ramping up efforts against organizations that prove to be easy targets," Schaller explains.

He urges state officials to concentrate on two cybersecurity strategies to prevent most fraud attempts from occurring. The first involves developing a zero-trust environment. The second calls for deploying identity authentication that requires more than one login factor. Those two steps alone would significantly limit most instances of fraud.

A layered approach to identity security

Last year the White House released the *Executive Order on Improving the Nation's Cybersecurity*. While not a mandate for states, this framework can be a valuable roadmap for IT and security leaders to implement zero-trust strategies that improve security without sacrificing citizens' digital experience.

The goal of modern CIAM is to prevent bad actors from entering state systems in the first place. To coordinate these efforts, security leaders recommend a platform approach that can lay across states' existing infrastructure and connect their various tools and applications.

"Working with an identity provider to build a layered security approach to identity and access management allows a single choke point to access government

> "As states move closer towards a purely digital service the footprint with which fraud could happen will only grow more prevalent. The way individual cybercriminals and growing crime syndicates are organizing to expand their reach shows that that threat actors are ramping up efforts against organizations that prove to be easy targets,"
>
> **- Ryan Schaller, Okta**

40% of states did not perform required and recommended improper payment detection activities, attributing much of the failure to antiquated IT systems and inadequate staffing.

- May 2021 Department of Labor Inspector General's Report

Colorado identified

$73.1 MILLION

in potentially fraudulent benefits payments between March 2020 - April 2021.

Ohio filled approximately

$477 MILLION

in fraudulent unemployment assistance claims over a similar period.

– State auditor reports

systems and improves overall visibility across the environment," says Schaller.

"A platform tool allows organizations to take simultaneous actions," says Schaller. "For example, cutting out basic IP traffic that is known to be coming from a proxy, out of state or out of the country so a state is only receiving legitimate traffic. And additionally unifying password management so agencies aren't storing 15 different passwords for various citizen services."

But eventually, the goal will be to move beyond passwords and integrate more than one login factor to validate a citizen is who they say they are.

Building up security roadblocks

There are several tactics a threat actor or criminal syndicate can use to submit fraudulent claims, thanks to the availability of databases of stolen identity credentials and passwords available on the dark web, after years of accumulated hacks from poorly protected systems.

A cybercriminal won't just use stolen credentials in one state agency. They will automate that action across multiple states and organizations until they successfully breach a poorly protected system.

Having an identity platform that gives organizations the maximum flexibility to integrate various login factors is critical because when the system detects an anomaly, this step becomes the last checkpoint before a user — or fraudster — gets access to data and resources.

"In addition to providing multifactor authentication capabilities, Okta continues to build up its multilayered approach with an ecosystem that draws on capabilities from partner organizations," explains Schaller.

For example, *LexisNexis* provides identity proofing services that utilize questions that only that constituent would have the answer to, such as, did the user own a certain car, apply for a loan or live at certain addresses in the past? LexisNexis solutions can be integrated into the Okta platform to facilitate more seamless proofing, credentialing, and ongoing access management processes.

And from a developer perspective, Okta's acquisition of *Auth0* gives agencies greater flexibility in the development stack for how they integrate and expand authentication. That enables them to respond appropriately to users with different levels of knowledge or experience — from young adults to seniors — based on how they interact with a platform.

"With these acquired capabilities, Okta's identity platform has become flexible enough to synchronize capabilities, which means that now states and all their agencies have an à la carte [approach to] how they want to solve their IAM challenges," Schaller says.

Getting collaborative about security

In the face of increasing security incidents, agency leaders have come to recognize that taking a reactive, after-the-fact approach to fraudulent activity can prove far costlier than investing in a modern CIAM platform.

Over the past two years, in particular, state agencies struggled to find the right balance between getting money out to people in need as quickly as possible, knowing that instances of fraud were occurring, yet were unprepared to defend against fraudulent claims promptly.

"In certain cases, if fraud is super-apparent and threat actors are just attacking your systems, that is what costs organizations a lot of money," says Schaller. "Running systems 100% of the time adds up with electricity, server bandwidth — all those things become contributing factors of what it is going to cost you at the end of the day."

If agency officials can alleviate some of those issues, they not only reduce risk but also infrastructure costs; and they get back time for their personnel to focus on mission-critical activities.

By upgrading their underlying identity platforms, state agencies also can gain greater levels of threat insight across their IT ecosystem, especially when they collaborate with an identity provider like Okta, which accumulates intelligence on IAM activity from a wide range of customers. So when malicious threats are detected, *that information can be shared with all platform customers*, as well as other states and their departments, helping them to mitigate fraudulent claims as well.

> "Working with an identity provider to build a layered security approach to identity and access management allows a single choke point to access government systems and improves overall visibility across the environment"
>
> **- Ryan Schaller, Okta**

The good news is that today's identity platforms can lay across the existing infrastructure and integrate identity into a single view, so it no longer matters as much as it once did whether each state agency has worked to build its identity systems.

That allows states to approach security, identity and access collaboratively, where each department operates using a minimum level of security standards that includes identity verification and multifactor authentication.

At the same time, it preserves flexibility across state agencies, allowing them to meet their own diverse set of requirements and customize security controls based on the needs of each agency.

Learn more about how Okta is helping government agencies reduce security risks.

This report was produced by StateScoop and underwritten by Okta.

okta STATESCOOP