NASCIO State IT Recognition Awards Submission

STATE: State of Kansas

AGENCY: Kansas Department of Labor

AWARD CATEGORY: Cybersecurity

PROJECT TITLE: Overcoming the Challenge of Fraudulent Unemployment Claims

PROJECT DATES: February 2, 2021 to present (rolled out and implemented in February as an ongoing security feature)

CONTACTS:

Allie Denning, Public Information Officer
Office of Information Technology Services
allie.denning@ks.gov
(785) 250-3837
1000 SW Jackson St., Ste 500
Topeka, KS 66603

Gerald Grasso, Communications Director
Kansas Department of Labor
gerald.grasso@ks.gov
(785) 296-5000 x7333
401 SW Topeka Blvd.
Topeka, KS 66603

Idea

When the COVID-19 pandemic began and unemployment numbers were on the rise, the Kansas Department of Labor (KDOL) also saw a dramatic increase in in unemployment claim fraud. Using stolen identities of Kansans who had not lost their jobs, fraudsters stole millions of dollars of state and federal benefits.

This crisis launched the idea and implementation of identity verification software including two-factor authentication. Using identify verification software for unemployment insurance accounts and claims, the system now requires two-factor authentication so that claimants will be able to more securely log in and access their account. Every claimant now must verify her or his identity by answering specific questions based on the person's credit history. Once an identity is verified, the system will prompt the claimant to setup two-factor authentication for her or his benefit account. This additional layer of security is an important factor in protecting KDOL unemployment.

Implementation and Impact

Rolled out on February 2, 2021, the identity system quickly enabled KDOL to transition analysts from fighting fraud to focusing on the real mission of the agency – getting legitimate claimants paid the benefits they are owed.

Within the first week of deploying the solution, KDOL announced the agency's new verification software system blocked over one million fraudulent login attempts and BOT attacks.

A fraudulent login is a criminal trying to access the KDOL software system to file a fraudulent claim. A BOT attack is the use of automated web requests to manipulate or disrupt a website, application or end-users online. Originally, these attacks were simple spam operations, but over time have become more sophisticated criminal enterprises. Stopping these BOT attacks reduces the strain on the KDOL unemployment insurance IT system, enabling the agency to more effectively analyze and service valid benefit claims.

Metrics from early May bear witness to this enhanced capability. As of 05/03/21 total claimants attempting authentication were approximately 160,000. Waiting for user action: approximately 9,000. Claimants who were proofed/approved: approximately 94,300. Claimants who have failed their ID proofing and would need to do it again/get help: 56,000. Claimants who experienced an error of some sort: approximately 130. In terms of BOTS and fraudulent login attempts KDOL has stopped, approximately 6.94M.

Other government agencies across Kansas have taken notice and are actively evaluating how they might use the platform for a myriad of use cases, from cybersecurity to identifying risks in financial transactions.