Why Modern Identity Authentication is Key to Fighting Fraud

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

IDENTITY AUTHENTICATION CREATES OPPORTUNITIES FOR AGENCIES

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.

IDENTITY AUTHENTICATION CHALLENGES FACING GOVERNMENT AGENCIES

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.