A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

AI & the New Front Line of Government Fraud Defense

SPONSORED BY

CONDUENT

With a boost from AI technology, willful misrepresentation committed against government programs is becoming more industrialized. What was once limited to localized instances of theft now moves more fluidly across digital storefronts, agency call centers and residents' devices, often powered by sophisticated criminal networks that operate across state lines.

With annual federal fraud losses estimated at between $233 billion and $521 billion,[1] and $162 billion in improper payments reported in fiscal year 2024,[2] government programs must choose the right strategy to combat fraud, waste and abuse.

"It's like a game of chess," says Russ Nichols, a senior fellow at the Center for Digital Government. "You make a move to address the situation, then your opponent does the same. It just keeps developing."

FRAUD TACTICS

Today, the chessboard spans every channel. A compromised terminal at a local retailer, for example, can expose recipients to physical card fraud. An online credential attack can undermine program integrity through unauthorized transactions or duplicate accounts. A spoofed phone call can exploit interactive voice response systems and overwhelm contact centers.

Each channel introduces new vulnerabilities, and each point of access becomes another front to defend.

Legacy IT systems built for a different era are confronting a modern fraud economy. Unfortunately, it's the constituents that count on essential services who suffer.

Fraudsters have new capabilities such as voice-changing technology and biometric data to create convincing fake identities that interact with state systems.

Online benefit theft drains accounts before recipients realize they have been targeted, locking them out of resources they rely on.

According to the Federal Trade Commission, reports of identity theft involving government documents or benefits surged dramatically in 2020 following the rapid expansion of pandemic relief programs.[3]

"Public expectations drove services online, then multiplied those operations using AI," says Chris Carter, vice president and head of fraud at Conduent.

With this new technology, fraudsters have new capabilities. They use voice-changing technology and biometric data, for example, to create convincing fake identities that interact with state systems.

The FBI's Internet Crime Complaint Center tracks AI as a distinct fraud enabler. AI-related complaints accounted for nearly $900 million in reported losses, driven by voice cloning, synthetic identities and AI-generated impersonation schemes.[4]

Once bad actors gain access, they move across programs and evade detection.

THE CRITICAL ROLE OF DATA

Real-time visibility is now essential for spotting emerging threats early and responding before issues become costly problems.

“In a world of needles and haystacks, you can’t take out all the needles,” Carter says. “But maybe you can make that haystack a lot smaller.”

Reducing the haystack requires more than stronger detection. It depends on giving agencies faster, broader access to data. Yet legacy policies and disjointed organizational structures often restrict sharing, leaving critical information siloed.

MOVING FORWARD

For the first time, agencies have access to a new generation of powerful tools that meet modern fraud threats with greater speed, intelligence and precision. Real-time analytics, automated validation and advanced risk detection can improve visibility into suspicious activity, helping agencies respond faster with greater precision.

Yet no single fraud solution fits every organization, and agency leaders must make strategic decisions about where to invest. For agencies with limited budgets, the question is no longer whether to act, but when and where.

Fortunately, not every modernization initiative must be carried out right away. Instead, successful organizations often focus on developing a strong foundation and customizing it to their unique needs.

The most effective agencies are adopting measures such as multifactor authentication and cardholder tools that include PIN reset and real-time alerts.

Here are four steps to get your organization started:

1. **Understand the risks.** Effective fraud defense begins with understanding where risks are most immediate. For many agencies, that starts with identity verification and authentication while setting up the technology needed to address data, integration, real-time monitoring and other capabilities when resources allow.

2. **Measure your progress.** Beyond tracking fraud alerts, organizations can measure broader operational gains by monitoring loss prevention, resolution times and staff satisfaction.

3. **Collaborate with peers.** Strong outcomes depend on sharing intelligence and aligning strategies across teams, agencies and jurisdictions. Partnerships can help reduce vulnerabilities and speed improvement.

4. **Leverage third-party technology and expertise.** The right partnerships help agencies close gaps faster. By applying industry expertise, leaders can avoid building from scratch and modernize quickly via proven solutions, stronger team onboarding, and better connections across programs and organizations.

FLEXIBLE AND AGILE

Combating government fraud requires a layered defense strategy. The most effective agencies are adopting multi-layered measures, including multifactor authentication, cardholder tools that include PIN reset and real-time alerts, and continuous monitoring of terminals.

Likewise, AI-driven risk scoring, validation and anomaly detection help agencies identify threats earlier.

“There’s not a single silver bullet,” Carter says. “As soon as you get one fraud scheme figured out, the next one is right behind it.”

Building on top of a strong technology environment can help agencies stay ahead of risks and strengthen constituent trust. Ultimately, the greatest defense against evolving threats is flexible solutions that adapt before it’s too late.

1. gao.gov/products/gao-24-105833
2. gao.gov/products/gao-25-107753
3. ftc.gov/system/files/documents/reports/protecting-consumers-during-covid-19-pandemic-year-review/covid_staff_report_final_419_0.pdf
4. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

This piece was written and produced by the Government Technology Content Studio, with information and input from Conduent.

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

IMAGES PROVIDED BY: ADOBESTOCK/AI GENERATED