

# Implementing AI to Combat Fraud and Abuse

**We often think of fraud and abuse in government programs as violations committed by individuals: unscrupulous vendors or dishonest beneficiaries. But increasingly, benefit programs face attacks by organized fraud rings that rely on fake identities and outdated verification systems to siphon away billions of dollars.**

“This may seem like something out of a movie, but it’s a real problem that exists all across the country,” said Jordan Burris, Vice President and General Manager for Public Sector at Socure. It not only cuts into the funds available for program objectives, but can deprive legitimate recipients of their benefits.

Artificial intelligence (AI) and machine learning (ML) have shown value in modeling potential attacks to aid in their detection when they occur, said Solomon Abiola, AI/ML Policy and Governance Director for the state of Maryland. But the current environment needs more. “The real issue is the scale at which the activity occurs,” he said. With more advanced AI, “we might be able to identify something before it starts.”

By recognizing patterns of abuse and improving verification systems, AI could make it easier for rightful beneficiaries to access the services they need and for agencies to defend systems from powerful nation-state incursions, Burris added.

---

## Culture and Process Both Must Change

AI alone isn’t a panacea, said Taka Ariga, former Chief AI Officer and Chief Data Officer at the Office of Personnel Management and founder of Sol Imagination. “Most people think of AI as the ‘easy button,’” he said. “You deploy the AI, and somehow it can magically identify a set of gotchas to root out. But it’s not some sort of auto-magical solution.”

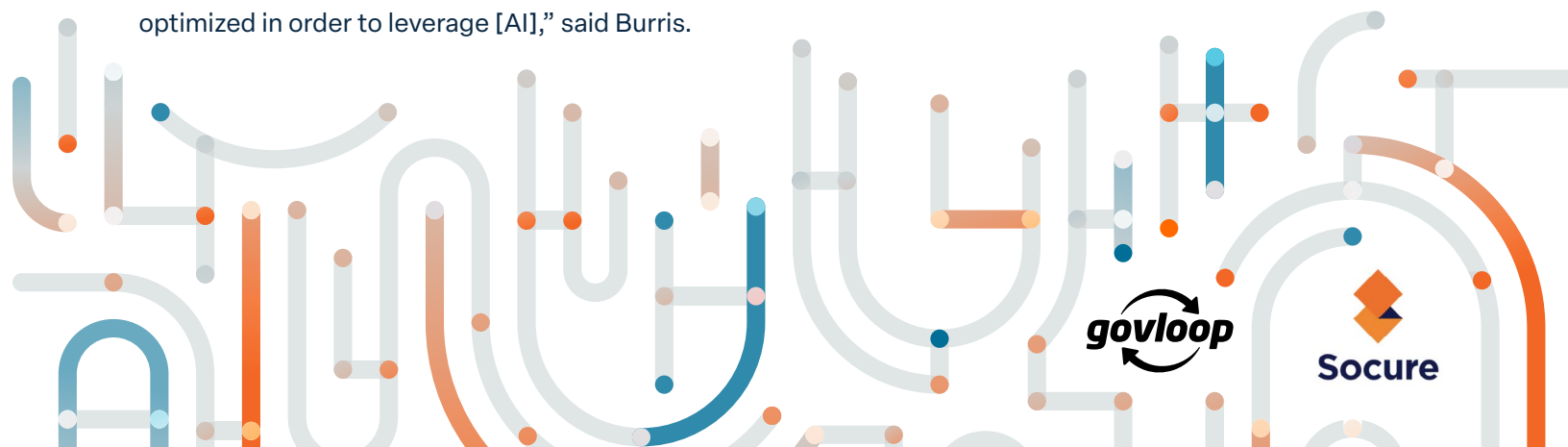
Instead, AI is an accelerator that can improve digital payment systems, processes and cybersecurity. “It’s really more like puzzle pieces that you put together,” he said.

In practice, that requires rethinking systems and processes to make the best use of AI. “Many of the processes that have been built today, the programs as they’ve been established, have not been optimized in order to leverage [AI],” said Burris.

Even rules that take AI into account may not be keeping up. The first step, he said, is “a mindset shift and thinking and understanding that you have to adapt everything to incorporate.”

That’s more than just adding AI on top of existing workflows, said Abiola. “We don’t want to accelerate and compound [negative] issues in these workflows. We want people to be able to reimagine what it is they’re actually trying to accomplish,” he said.

The solution may not be AI alone, or even AI at all. “We have to understand at a more granular level the actual problems people are facing,” Abiola said. “Is it an AI-shaped problem? Maybe it’s not. Maybe it’s just an automation or reimagining of a workflow that needs to occur.”



## Training to Navigate Probability, Not Certainty

Employees must know more about AI than how to word a good prompt or what data to keep away from public chatbots. Although there's plenty of training available on those topics, "what I see as a complete gap is, 'How do I use AI to combat fraud?' And specifically, 'How do I combat fraud using AI within my agency for this kind of mission?'" said Ariga. "That just categorically doesn't exist."

"If we want to use AI for fraud detection purposes, we need to develop our own bespoke training content" focused on the specific work of departments and even individuals, he added.

Employees need to understand that AI answers reflect likelihood, not certainty. "The question that always comes up is, 'How do you achieve 100% perfect classification and accuracy?' and the reality is, that's not the way this works," said Burris. "For us, it's about educating everyone on the fact that a lot of this is probabilistic in nature."

To cope with the uncertainty, agencies must involve human decision-makers. "Let's say I try to log into Social Security, and it denies me access," said Ariga. "And [the algorithm] says, 'Taka tried to log in with a 62% likelihood of fraudulent behavior.' What does that mean? Is that a fraudster or is it just Taka [making a mistake]?"

Such a finding must be interpreted in context — something humans do much better than AI. "If you rely on AI for some sort of adjudicatory function and you get it wrong, that's the lawyer's worst nightmare," Ariga said.

## The Right Policies Can Help AI Flourish

Agencies can avoid such pitfalls by establishing realistic policies designed for rapidly changing new technologies. "Policy needs to be adaptive and responsive," said Abiola. "They keep making new things, and you're not going to be able to have a policy for every single one of them. That's just the rate of change."

In Maryland, he encourages setting governance rules based on use cases, rather than specific technology — "just basic guidelines that allow you to evaluate a suite of applications as opposed to recommending one particular solution."

Ariga calls it "agile governance" — policy that is dynamic and evolves as the technology does. Government tends to spend a long time attempting to develop a perfect policy that will never change, he said, and that won't work for new technology.

He suggested using modular policy that adapts to current conditions. "The whole thing is going to change anyway, so let's not let the perfect be the enemy of the good. Evolve as the technology evolves," Ariga said.

Good AI policy encompasses more than a technical framework. "We're not just talking about algorithms or models behaving correctly," said Burris. "We're talking about the impact they have on public trust, national security, program integrity and, really, human dignity."

## The Cost of Doing Nothing

Burris also warned about "the unseen cost of inaction." Too much analysis can stymie innovation — and leave agencies vulnerable. "They [find] themselves unable to catch up with the more sophisticated types of identity fraud that could be caught today with the right type of program," he said.

It's possible to engage new technology faster without breaking the processes that are in place. "When done right, you're able to deploy AI at scale in order to promote transparency, promote access and combat what may be occurring in organizations when it comes to fraud, waste and abuse," explained Burris.

Although AI will continue to evolve, agencies shouldn't wait to begin understanding it.

"We're going to build with the technology, and it's through building that we'll learn [to] build safer and better things," Abiola said. "We're building this future together."

[Learn more about Socure](#)