A **GOVERNMENT** TECHNOLOGY HANDBOOK

Think Like a Fraudster, **Adapt Like an Expert**

Attackers continuously adjust their methods. Stopping them requires a fast, flexible and always-evolving approach to identity verification.

SPONSORED BY Socure™

Introduction

Identity-based fraud — the act of exploiting someone's personal information to gain something of value — is a significant and growing threat to the integrity and mission of government services.

Fraudsters are targeting weaknesses in digital services with increasing sophistication using stolen, fabricated or manipulated identity information. Each new fraud control implemented by government agencies prompts bad actors to adapt their methods. Agencies need proactive, dynamic solutions that respond to these patterns.

Ultimately, fraud is a business, with a core incentive structure and an end goal. Understanding a fraudster's motivation equips agencies to counter today's fraud — and the full spectrum of attacks they will face in the future.

The task at hand: Think like a fraudster in order to stop them.

Modern identity verification platforms thrive within this bigger picture. Machine learning (ML) and targeted AI can assess risk accurately and efficiently, catching obvious bad actors quickly and requiring additional proof of identity for more difficult cases. This approach makes life harder for fraudsters and easier for honest constituents seeking public services. It lets agencies adjust friction based on risk.

To help agencies develop adaptive fraud defenses, this guide explores:

- **Effective fraud countermeasures**
- **Top motivations for fraudsters**
- **Key varieties of digital identity fraud**
- **Identity verification fundamentals**
- **A "just right" approach to ID verification**

No matter what kind of fraud you face today, you'll face new and more advanced fraud tomorrow — a direct result of your efforts to fight back. It's vital to understand what's coming next so you can implement defenses that stretch beyond your current fraud challenges.

The Shifting Fraud Landscape

Your fraudster is a real person. Let's call him John Doe, or JD for short. During the COVID-19 pandemic, JD and others like him fleeced government programs out of tens of billions of dollars.

Today, JD has easy access to AI tools that increase his efficiency and help him scale his efforts. He may be acting alone, or he may be part of a large fraud organization.

"We need to start thinking about fraud organizations as for-profit companies," says Neal Gallucci, head of solution consulting – public sector for Socure. Like legitimate businesses, fraud organizations or individual fraudsters seek to exploit opportunities, maximize profit, manage risk, optimize productivity and evolve to overcome obstacles.

Social safety net agencies face mounting pressure from Congress to implement effective fraud defenses against JD. But their intuitive response — tightening fraud controls — risks locking honest people out of essential services. Agencies need a fraud prevention strategy that responds to escalating threats while preserving access to vital public services.

AI's rising impact. Smart automation enables a new class of small-scale bad actors. Certainly, large fraud organizations use generative AI (GenAI) and other advanced tools. But these technologies are also readily available to individual fraudsters, making it easier for almost anyone to conduct sophisticated attacks. "It doesn't have to be a complex criminal conspiracy," Gallucci says. "You can now run a high-scale fraudulent operation by yourself." Gallucci has seen the fraud landscape mature first-hand. Before joining Socure, he led efforts to modernize identity infrastructure at the state level.

> **"We need to start thinking about fraud organizations as for-profit companies."**
>
> **Neal Gallucci,** Head of Solution Consulting – Public Sector, Socure

AI lets attackers ramp up their activity with ruthless efficiency, enabling them to submit thousands of fraudulent benefit applications a day. They only need a sliver of these applications to succeed. "AI achieves a scale and velocity that allows big profit margins because the underlying operational costs are extremely low," Gallucci says.

State and local agencies often have insufficient defenses for these types of attacks. "I've encountered government environments where anti-fraud controls were minimal to non-existent, especially in legacy benefit programs and systems," says Deborah Snyder, a senior fellow at the Center for Digital Government (CDG) and former chief information security officer for New York state. Smaller cities and counties may approve benefits with only minimal verification, she says, leaving the door open for fraud.

Preserving safety net access. Letting good people in while keeping bad guys out is a difficult challenge, particularly for agencies delivering vital food and health assistance to residents. Online government portals are designed to give applicants

“I’ve encountered government environments where anti-fraud controls were minimal to non-existent.”

Deborah Snyder, Senior Fellow, Center for Digital Government

fast, convenient access to benefits. Trouble arises when fraud risk prompts them to tighten their identity verification controls, adding extra friction to the application process and causing people to give up in frustration.

Applicants may lack a driver’s license or a permanent address, two common ID verification requirements. Some only have internet access through public computers at places like libraries. But fraudsters use these same public computers to hide their identities.

As a result, it’s hard to tell the difference between a legitimate applicant and someone committing fraud.

“Logging in from a library computer is a normal user journey for seeking benefits,” Gallucci says. “But it can also be the normal user journey of a fraudster.”

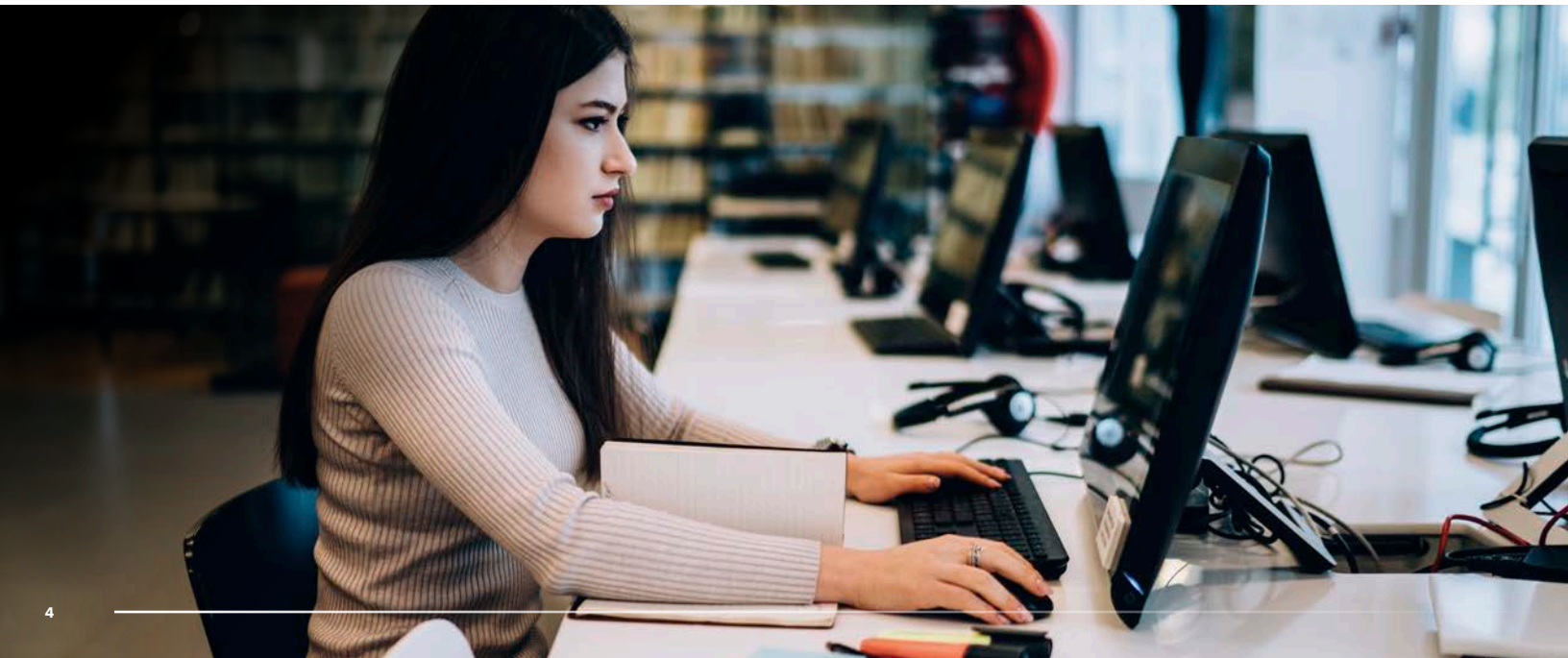
These challenges can make traditional identity checks less effective. Modern tools — like ML–based risk scoring — preserve access to benefits for people who need them while stopping bad actors.

More federal scrutiny. State agencies face growing regulatory and political pressure to rein in costs that include fraud. New rules in H.R. 1 passed by Congress in 2025 change how the federal government funds SNAP agencies and impose penalties for inaccuracies in benefits payouts.[1]

H.R. 1 requires states to have SNAP error rates below 6%, starting in 2028. States that fail to hit that threshold will lose a portion of their federal funding for SNAP benefits.[2] State error rates averaged almost 11% nationwide in 2024.[3]

Although most benefits errors stem from unintentional mistakes, the recent Medicaid scandal in Minnesota highlights the threat that fraudsters pose to public benefits systems. Early in 2026, the federal Centers for Medicare & Medicaid Services (CMS) deferred nearly $260 million of funding in Minnesota pending investigation of fraud claims.[4]

CMS officials also said the U.S. government’s priority is to use technology to prevent fraud before it happens rather than trying to respond after the fact.



The ‘Just Right’ Approach

There’s no one-size-fits-all defense against digital fraud. Lax identity verification controls open the door for significant financial risk. Overly rigid controls lock honest people out of crucial benefits. And identity and access management (IAM) software has limits because it doesn’t verify identity at the point of account creation.

The best controls balance access and oversight during identity verification. Here’s how these identity-control scenarios often shake out:

Too weak: Every internet user has been asked personal security questions that a fraudster supposedly wouldn’t be able to answer. What color was your first car? What was your grandmother’s maiden name? But so-called knowledge-based authentication (KBA) is no longer effective because fraudsters can easily track down this kind of personal data from social media posts and other online interactions. Also, legitimate users often forget the answers to the questions they created. The National Institute of Standards and Technology (NIST) discourages the use of KBA.[5]

Too strong: The tightest controls ask users to upload documents and undergo biometric scans to verify identity. These measures are appropriate if an agency needs to process transactions with a significant financial risk or deal with sensitive data that must be kept confidential. But these constraints typically create too much friction for everyday transactions.

Just right: Passive controls operate in the background and verify most legitimate users in seconds. Advances in AI/ML combined with sophisticated fraud detection techniques automate identity verification by analyzing dozens or even hundreds of variables. Data points include device type, IP address, physical location and standard PII such as name, address, phone and Social Security number.

Agency leaders are often skeptical about the effectiveness of passive controls. “States are constantly asking me, ‘How do you identify someone if you’re not making them do anything?’” says Socure’s Neal Gallucci.

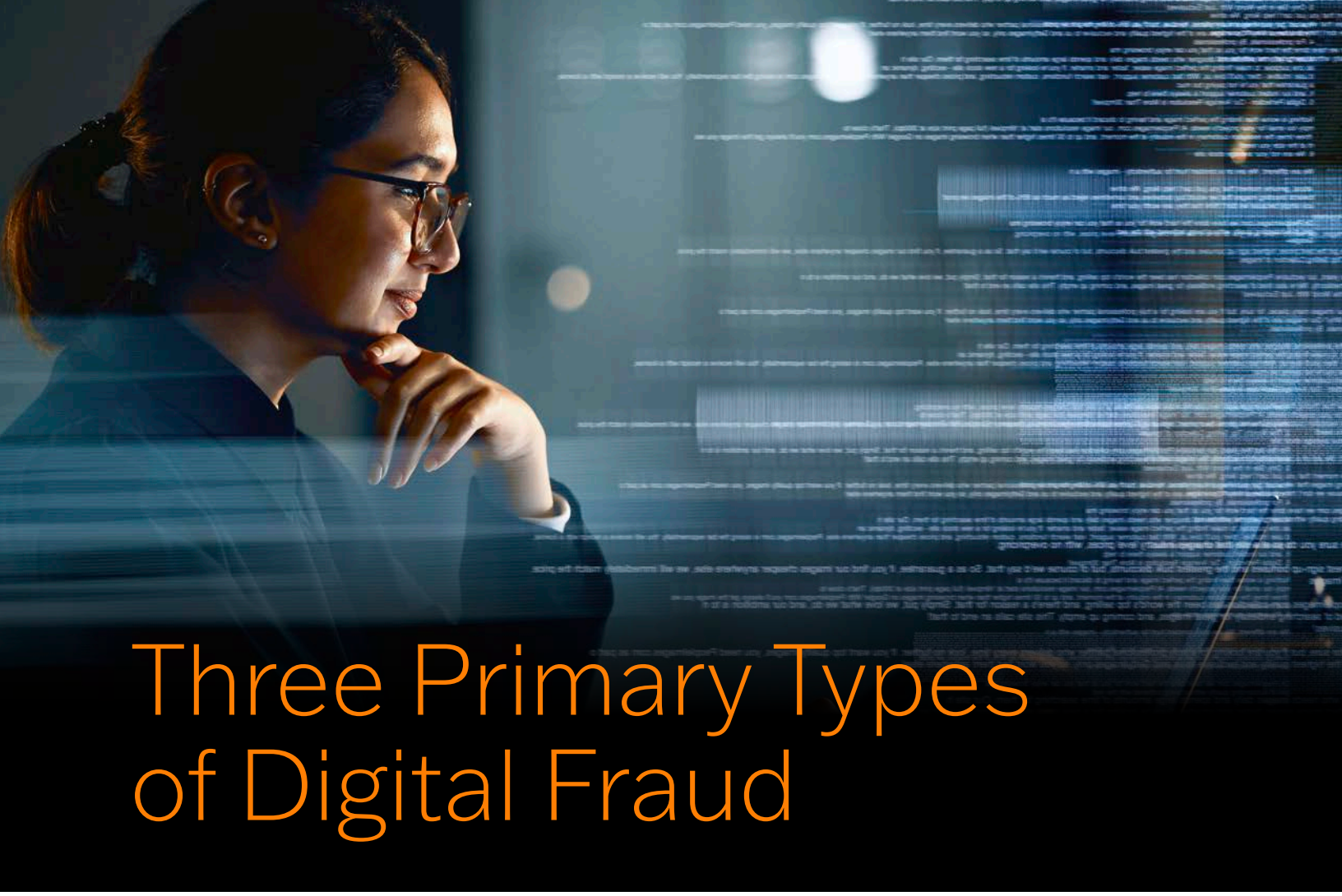
The answer lies in behind-the-scenes risk analysis technology. The first step is to uniquely identify the individual and establish who they are. From there, identity providers like Socure evaluate device risk, behavioral signals and network intelligence to understand how a user’s PII and device interact within a broader ecosystem. Using a range of data sources and purpose-built models, modern identity platforms assess whether the submitted PII correlates to a legitimate identity, assigning risk scores to each data point.

When collecting and verifying contact information, agencies should follow a few key best practices. For email, users should confirm they own the address by clicking a verification link. Agencies should also notify users when any profile changes are made.

For phone numbers, sending a one-time passcode helps confirm the user has access to that number. In some cases, silent network checks can be used as an additional layer of validation.

For physical addresses, older methods like mailing a one-time code are no longer practical. Instead, agencies can send a welcome packet after an application is submitted. This acts as a passive way to confirm the address on file.

Together, these steps make it harder for fraudsters to use real contact information. They are more likely to rely on fake or disposable emails and phone numbers, which can be flagged as higher risk. By combining these signals, agencies can better distinguish between legitimate users and potential fraudsters — allowing for faster, more confident decisions without adding unnecessary friction.



Three Primary Types of Digital Fraud

Digital fraud usually falls into three buckets: first party, synthetic and third party. This handbook focuses on third-party fraud because it poses the greatest risk to most state and local agencies. Moreover, understanding third-party fraud is a foundation for confronting the other varieties.

To see how these different types of fraud work, let's revisit JD.

First-party fraud. JD's fraud career started with an application for his county's general assistance benefits. He used his real identity data (name, address, Social Security number, etc.) to establish an account with the county agency. JD lied about his income to qualify but soon learned he didn't get enough free money to justify the time, effort and risk. JD had only one real identity; he calculated that using it too many times would get him caught.

Synthetic fraud. New GenAI apps got JD thinking: Why not use bots to create fake users that trick government safety net programs? It worked until it didn't. Identity-defense vendors soon teamed up with government credential-issuing agencies to provide tools to fight synthetic fraud. JD still had the tools to conduct synthetic fraud at scale, but easy wins became much more difficult. He started hunting easier prey.

Third-party fraud. While mastering the nuances of synthetic fraud, JD found illicit dark web forums where he could purchase stolen identity credentials and toolkits for attacking multiple government programs at scale. These credentials enable third-party account takeovers where JD logs into beneficiaries' accounts and changes banking information to divert payments to crypto accounts he controls. Modern ID verification tools can stop third-party fraud, but only if agencies deploy them.

First-person and synthetic-fraud risks should not be underestimated; they can do significant financial harm. But because third-party fraud can be automated and scaled by anybody with readily available tools, it often poses a bigger threat to public agencies.

Trending Attack Vectors

Contact center fraud. When you strengthen your digital front doors, fraudsters seek other ways in, usually human-centric ones. Contact centers are alluring targets because agents might not be sufficiently trained to fight fraud, and their systems most likely lack modern identity defenses.

A fraudster trying to take over an account has a constituent's basic information — name, address, phone number and biographical data to use in case of knowledge-based authentication. He calls the agency's contact center requesting a password reset. He has a well-rehearsed script telling the agent why he needs access right away and demands to talk to a supervisor if things go too slowly.

The agent's job is to satisfy the caller. If the contact center lacks strong identity controls and does not recognize the caller as illegitimate, the agent hands over control of the account to the caller, setting fraud in motion.

Fake job postings and applicants. Online help-wanted ads have an irresistible appeal for fraudsters.

A phony job posting imitates content from an agency's HR department. The goal is to collect personal data like names, associates and career histories from job applicants that can be used to create synthetic identities or enable account takeovers.

On the flip side, fake job applicants try to fool agencies into hiring them. They hope to gain trusted access to agency systems, data and funds. This tactic can hit agency IT departments especially hard because the talent they need might live across the country or overseas. As modern identity controls make your online applications more secure, bad actors will seek internal access to bypass these strengthened defenses.

API injection attacks. Fraudsters aiming to defeat advanced identity controls may resort to sophisticated system assaults.

Application programming interfaces (APIs) connect front-end application portals to back-end systems, allowing identity verification, eligibility checks and transaction processing. When a resident submits data online, APIs convey that information to identity-proofing tools that help agency systems determine if an applicant is trustworthy.

APIs can be slightly misconfigured in ways that let the fraudster bypass identity controls and communicate directly with back-end systems. An API injection attack probes for these flaws and exploits them by conducting unauthorized activities at scale in back-end systems.

Understanding the Fraudster's Mindset

Just as the great detectives of popular culture try to get inside the minds of criminals, state and local agencies must anticipate what fraudsters want.

"They're trying to find the weakest point, and they're not afraid to just keep going," says Curt Wood, a CDG senior fellow and a longtime security executive for the commonwealth of Massachusetts. Wood and his colleagues fended off massive fraud attacks during the pandemic. They brought in fraud experts from law enforcement and the National Guard to learn what made their adversaries tick.

These factors tend to drive a fraudster's activities:

Stealth. Attackers are primarily motivated by easy financial gain and avoiding detection. They rely on tactics that let them operate at scale while remaining hidden.

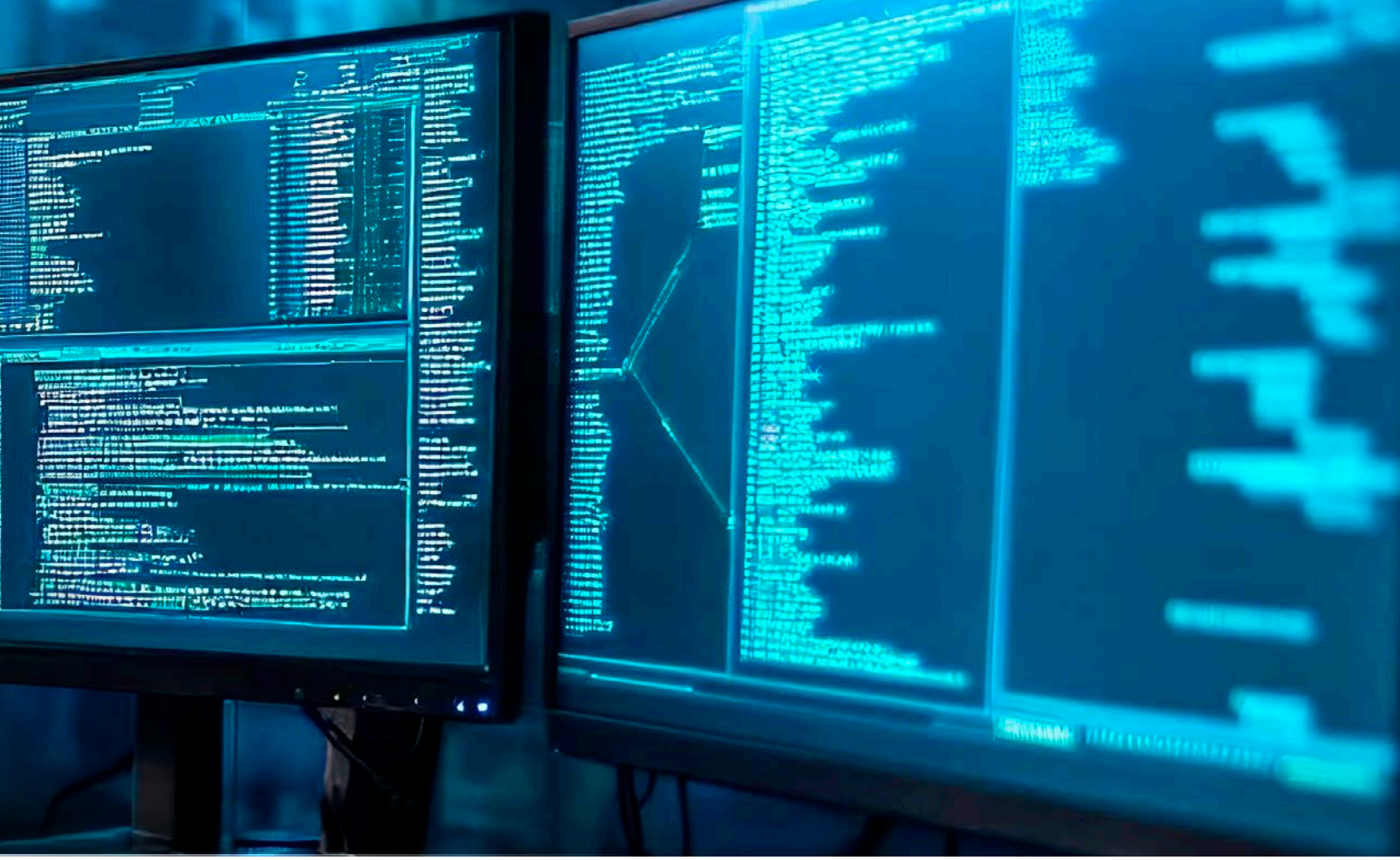
When possible, fraudsters exploit programmable temporary email domains and disposable email services to bypass email verification systems. Because they aim to conceal their true location, they frequently use anonymizing proxies. To circumvent phone verification and one-time passcodes, they may reuse the same phone numbers or rely on shared online SMS services.

> **"They're trying to find the weakest point."**
>
> **Curt Wood,** Senior Fellow, Center for Digital Government

The bottom line: If fraudsters can easily use tools that preserve their anonymity, they will take full advantage of them. Government agencies should treat users who engage in untraceable activity as inherently high risk.

Strong identity controls like device intelligence and consortium intelligence — shared information about known fraudulent activity — force fraudsters out of the shadows, making their behavior more visible, detectable and preventable.

Opportunity. Like a burglar casing a house, fraudsters look for vulnerabilities in online benefit application processes. During the pandemic, for example, Massachusetts agencies beefed up identity verification by requiring applicants to submit photos



of driver's licenses, passports and other physical documents. Honest people complied, but fraudsters did things like submitting random images. "The objective was just to see if the state would actually accept it," Wood says.

Fraudsters increase their chances of success by imitating legitimate behavior. An attacker might create an account with stolen credentials on Tuesday, come back on Friday to start an application and then wait a few more days to execute the application, just like a real person. In account takeovers, fraudsters must control authentic accounts and give the impression that they have devices (phones, PCs, laptops, tablets) connected to the accounts' owners.

Scale. It's never a single fraudster submitting one phony application for benefits. It's a numbers game. AI apps and robotic scripts let attackers apply for benefits at hundreds of agencies. They can make 10,000 application queries looking for one or two gaps to exploit. They can launch operations long enough to scoop up some cash and quickly shut them down to throw the authorities off the trail.

"At times, we had applications from a thousand people with the same address or apartment number," Wood recalls.

The dark web offers forums and toolkits to walk attackers through every phase. While your agency must serve every legitimate applicant and defend every attack vector, a fraudster needs only a few footholds to get closer to his goals.

Law enforcement agencies and private companies have amassed global intelligence of known fraud behaviors. They've documented the flaws in devices and software that fraudsters like to exploit. AI/ML applications use this data to put up stronger fraud roadblocks.

These measures prod fraudsters to get more creative.

Attackers use AI and robotic scripts to apply for benefits at hundreds of agencies, looking for gaps they can exploit.

Why Fraud Inevitably Evolves

Every new hurdle sends attackers looking for new ways to avoid detection and collect profits.

"It's never one clever trick — it's an assembly line of tricks," Snyder says. "They rapidly experiment, they scale fast and they are in constant iteration mode. They A/B test governments like companies test new product marketing, and they're successful at it."

Many agencies are still targeted with simplistic fraud attempts. Fraudsters start by submitting a dozen digital applications on the same day with usernames differing by one character (JohnSmith1, JohnSmith2, etc.). Once you start looking, these attempts are obvious. But when the agency fends off this tactic, another one takes its place. You need a solution to programmatically detect this type of behavior.

It's not enough to block what fraudsters are doing now. You need to anticipate what they'll do in the future and ensure the security products you use can handle the eventual final evolution.

Picture a rural county with a population under 50,000 with an online application for its program to help families facing hard times.

One Monday, a dozen new accounts are created. Each account's email address differs by one character, a classic fraud giveaway. This happens again on four successive Mondays. The county staffer authorizing benefits declines all these applications, so the fraudster tries something else.

A small staff can adapt to a few emerging fraud tactics, but they can't spend hours every day checking every application. Anti-fraud tools in a digital identity platform can scan application data and flag these obvious attacks automatically. And because these identity platforms are designed for the most sophisticated attacks, they enable jurisdictions to continue to mitigate fraud as it evolves.

Larger jurisdictions also see fraud mature in response to countermeasures. Fraudsters might create a network of smartphones that makes it difficult to pinpoint the location of their attacks. If agencies get wise to fraud tactics used in online applications, attackers might begin calling contact centers or visiting physical offices. If agencies notice fraud coming from foreign domains and impose a rule blocking overseas applicants, fraudsters can disguise domains to appear domestic.

"You'll never get fraud down to zero," Gallucci says. "But modern identity tools enable agencies to evolve at the speed of fraud, minimize attacks as they emerge and adapt proactively."

At the same time, stronger anti-fraud controls can't jeopardize access for legitimate applicants.

"High-risk things like library computers and prepaid phone numbers may be evidence of fraud, but they're also evidence of your normal user base," Gallucci says. ML algorithms in modern identity platforms digest a broad array of variables to verify legitimate applicants faster and more accurately.

Executive Guidance for Modernizing Identity

Successful anti-fraud strategies balance access for beneficiaries and strong measures for identity verification. These tips will help your agency strike that balance.

Widen your perspective. Identity isn't a one-time fix. It's a holistic, shared infrastructure that should be consistent across an agency. Think of identity protection as a business problem, not an IT problem.

Formulate a strategy. Create a plan that accounts for the varied identity needs of agencies and users. Make sure somebody is accountable for identity and that identity leaders understand the need to balance control and accessibility.

Prioritize agility. Prepare for innovative adversaries who will find any vulnerability. Robust online defenses may prompt fraudsters to target in-person or call center interactions. Look for identity verification tools with low-code interfaces that let you quickly adjust controls in response to evolving needs and threats. Make sure tools provide interoperability across your technology stack.

Assess your environment. An identity-verification vendor can analyze your application data, show active fraud footprints and identify weak points. When you can see the fraud in your environment, you'll be better positioned to convey the urgency for modernization to elected and executive leadership. Emphasize financial loss, reputational risk and erosion of public trust.

Use passive detection. AI/ML tools and risk scoring that work in the background can deliver fast, accurate ID verification without the friction of uploading documents, taking selfies and other intrusive measures.

Look for identity verification tools with low-code interfaces that let you quickly adjust to evolving threats.

Creating Friction for Fraudsters

Modern identity platforms reduce friction for legitimate applicants and dramatically increase friction for fraudsters. Here are some key capabilities:

Collect risk signals. Every online interaction creates digital data that can be logged, analyzed and visualized via graphics and dashboards.

Identity verification tools analyze a range of signals, including the devices individuals use, their physical locations, online movement patterns and whether they rely on virtual private networks (VPNs) to mask their activity. Fraudsters may attempt to generate hundreds of these signals to appear legitimate. But each additional signal increases the likelihood of exposing inconsistencies. One incorrect signal, such as having a time zone setting from the Middle East, calls into question the legitimacy of all the other signals.

The more signals that are evaluated, the greater the probability of identifying fraudulent behavior.

> **"The more data you collect, the more likely you're going to catch fraud."**
>
> **Neal Gallucci,** Head of Solution Consulting – Public Sector, Socure

"The goal is to capture as many signals as possible across the user's online journey," Gallucci says.

Fraudsters will attempt to disguise their actions, but the very act of creating these ruses becomes a signal in itself. They must also rely on automation to operate at scale, and automated behavior produces patterns that legitimate users simply do not generate. In other words, the tactics fraudsters depend on to succeed ultimately create the signals that expose them.

"The more points you protect, the more data you collect, the more likely you're going to catch fraud," Gallucci says.

Maintain secure processes. Poor data flow between systems can weaken identity verification. For example, a resident may verify their identity through a state identity portal and be approved as a trusted user. But if they apply for benefits through a separate system that cannot access that verified identity data, the user may be asked to enter the same information again.

This gap doesn't only create unnecessary friction; it can be exploited for fraud. A fraudster using stolen personal information might pass the initial identity check. The benefits system assumes the identity is valid but allows changes to key details. The fraudster can keep the victim's name but change information like the mailing address — redirecting payments to themselves.

"The data you use for identity verification has to be the data you use in downstream processes," Gallucci says. "You shouldn't recollect it."

Fraudsters often use automation to find and exploit weak points like this. Closing these gaps adds friction to deter attacks.

Use advanced insights to gain context. Identity verification providers collect immense volumes of real-time fraud data. Data science and AI/ML provide the only practical means of understanding the clues fraudsters generate.

With AI/ML, you might notice a trusted user has a new email. Perhaps their device is an iPhone today, but they had a Samsung last week. Or global fraud intelligence shows a new account user is behaving exactly like a fraudster in Southeast Asia.

To make sense of these data points, AI/ML-powered identity verification systems use dynamic risk scoring. When someone creates a new account, the system gives every data point a numerical risk score. Most innocent or legitimate activities have low scores because AI/ML systems already know what good behavior looks like.

A young person's thin credit history or a homeless person's lack of a permanent address might generate high risk scores on their own. But AI/ML can scan

Data science and AI/ML provide the only practical means of understanding the clues fraudsters generate.

dozens of adjacent behaviors and data points to see if anything else aligns with common fraud behaviors. If the other behaviors exhibit low risk probability, the risk score typically stays low enough to consider the person harmless.

AI/ML also assesses the context of user journeys to ensure agencies are adding friction for fraudsters but keeping things easy for everybody else. "As the risk goes up, the friction should go up as well," Snyder says.

Understanding context lets agencies employ multifaceted tactics wherever bad actors might show up. "Fraud isn't stopped by one control," Snyder says. "It's stopped by control depth, driving layered defenses down the stack."

Flag anomalies that expose fraudulent behaviors. Fraudsters must come out of the shadows long enough to apply for an agency's benefits. No matter how much they try to disguise themselves, they'll create clues that are visible to advanced fraud prevention software.

Analytics and visualizations from these tools can reveal deviations from the norm in striking detail. Gallucci recalled a medical services agency that detected a sudden spike in 50- to 55-year-old applicants. The anomalies pointed to automated attacks where the same age appeared in multiple interactions with the agency's online services.

"At the end of the day, fraud will evolve into increasingly complex forms," Gallucci says. "Agencies must ensure they are protecting online applications in real time as these threats adapt." The more sophisticated an agency's controls, the better positioned it will be to detect anomalies early, intercept fraud at the point of entry and prevent improper payments before it is too late.

Moving at the speed of fraud

It's not enough to mitigate the attacks your agency is experiencing today. Your fraud defenses need to be ready for increasing scale and sophistication. They must continue to impose more friction on bad actors and less friction on qualified benefits applicants — even as fraudsters ramp up their efforts.

Combating today's fraud and tomorrow's threats requires a layered, intelligence-driven approach that moves beyond reactive defenses. Agencies must focus on four foundational capabilities:

Persistent identity as the foundation. Effective fraud prevention begins with establishing a persistent, resolved identity. To stop third-party and synthetic fraud, you must move beyond surface-level checks and truly understand who an individual is, what attributes are consistently tied to them, how they present across channels and whether they represent a real person. "You have to know who they are to know when it's not them," Gallucci says.

This means shifting from evaluating isolated signals, like whether an email domain is risky, to confirming whether the provided identity elements align with a known, trusted individual. When identity is resolved at this level, inconsistencies become immediately apparent.

Furthermore, deploying solutions that move beyond credit-based identity intelligence and use multiple data sources to achieve near 99% identity resolution is important. Solutions with a weak identity graph — a database that links together multiple elements of identity — will lead to ineffective signals.

Local graph intelligence to detect emerging patterns. Once identity is established, agencies must analyze behavior within their own ecosystem. Local graph analysis detects suspicious velocity and reuse patterns, such as the same phone number appearing across multiple applications, or sudden spikes in activity from previously unseen email domains. These insights are critical to identify coordinated fraud attempts and inconsistencies that would go unnoticed in siloed evaluations.

Consortium intelligence for broader fraud context. Bad actors don't operate in isolation, and neither should you. Consortium-based graph intelligence expands visibility beyond your organization, providing insight into how identities, devices, emails and phone numbers behave across a broader network. This allows agencies to answer key questions early in the decisioning process:

- Has this phone number been recently associated with fraud?
- Is this identity being reused across multiple schemes?
- Has this address or device shown suspicious patterns elsewhere?

Adaptive risk scoring and workflow orchestration. Agencies need flexible tools and workflows to operationalize these insights. AI/ML-driven risk scoring should be applied at critical interaction points — such as onboarding, account recovery or payment changes — leveraging signals across identity, device, email, phone and address intelligence. Configurable workflows then determine how to act on that risk, tailoring responses based on identity confidence and transaction context. This ensures the right level of friction is applied, minimizing burden for legitimate users while escalating scrutiny for higher-risk scenarios.

Together, these capabilities create a proactive fraud prevention framework that identifies threats early, adapts to evolving tactics and maintains a seamless experience for legitimate applicants. With the right tools, you'll be ready when fraudsters show up — and when their tactics shift.

1. "H.R.1 – An act to reconciliation pursuant to title II of H. Con. Res. 14," *U.S. Congress*, accessed April 13, 2026, https://www.congress.gov/bill/119th-congress/house-bill/1/text

2. Medora Lee, "An end to SNAP? Why it may happen in a couple of years in some states," *USA Today*, accessed April 13, 2026, https://www.usatoday.com/story/money/personalfinance/2025/12/03/lose-snap-states-errors-pay/87553328007/

3. Katie Bergh and Dottie Rosenbaum, "Congressional Delay of SNAP Cost Shift Urgently Needed to Protect Food Assistance for Low-Income Families," *Center on Budget and Policy Priorities*, accessed April 13, https://www.cbpp.org/research/food-assistance/congressional-delay-of-snap-cost-shift-urgently-needed-to-protect-food

4. "Trump administration prioritizes affordability by announcing major crackdown on health care fraud," *Centers for Medicare and Medicaid Services*, accessed April 13, 2026, cms.gov/newsroom/press-releases/trump-administration-prioritizes-affordability-announcing-major-crackdown-health-care-fraud

5. Jeff Shultz, "Replacing knowledge-based authentication is long overdue," *Socure*, accessed April 13, 2026, https://www.socure.com/blog/replacing-knowledge-based-authentication-is-long-overdue

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

government technology

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

Socure™

Sponsored by Socure

Socure is the leading platform for digital identity verification, compliance and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust and mitigate risk. Leveraging AI and machine learning, Socure's industry-leading platform achieves the highest accuracy, automation and capture rates in the industry. Serving more than 3,000 customers and 190+ countries across financial services, government, gaming, healthcare, telecom and e-commerce, Socure's customer base includes 18 of the top 20 banks, four of the Mag 7, the largest HR payroll and workforce providers, the largest sportsbook and prediction market operators, 130 organizations across the public sector, and more than 600 fintechs. Leading organizations trust Socure to deliver certainty in identity across onboarding, authentication, payments, account changes and regulatory compliance.

www.socure.com

ADOBESTOCK/AI GENERATED