WRITTEN TESTIMONY OF

JORDAN BURRIS

HEAD OF PUBLIC SECTOR

SOCURE, INC.

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Hearing on Emerging Fraud Threats and the Evolving Fraud Landscape.
July 15, 2026

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

I want to begin with a blunt truth. The way the federal government verifies identity today was built for a threat that no longer exists, and every day we defend it as though it still does, we are handing fraud rings a head start at taxpayer expense.

The United States is facing an identity fraud crisis at a scale that should command this Subcommittee's attention. Start with the number the Government Accountability Office has already put on the table citing federal fraud losses of between $233 billion and $521 billion every year. During the pandemic, roughly $79 billion in fraudulent payments across just three major relief programs traced back to stolen or invalid Social Security numbers alone. Those are not accounting errors. They are taxpayer dollars diverted away from the people Congress intended to help, and they should have been sounding an alarm about how exposed our identity infrastructure had become.

While there has been grand rhetoric and some have sounded the alarm, there has yet to be the urgency to adopt a fundamentally different approach. I raise this because the threats generating those numbers has since accelerated in scale and speed in ways no annual report can fully capture, and by the time the next set of GAO estimates catches up to today's reality, the number will already be out of date again – and it may be double or triple today's estimate.

For two decades, the federal government's approach to identity verification has been organized around a static idea: confirm that a name, date of birth, and Social Security number belong together, check that combination against a handful of authoritative files, and treat a match as proof of identity. That model was already showing its age before generative AI. It is now close to obsolete.

The adversary behind this fraud has changed as much as the technology has. We are no longer dealing primarily with individuals filling out a false form.

We are confronting organized, increasingly transnational fraud rings, sometimes backed by nation states, that combine stolen identities, synthetic identities, fabricated contact information, residential proxies, and automated application attacks, and that now have generative artificial intelligence at their disposal.

Inside the identity industry, some of my colleagues have started calling this moment World War Fraud, and I understand why. Generating a new email address, a synthetic identity, and a convincing pattern of legitimate user behavior no longer takes a skilled criminal days of work.

It takes minutes, at a cost approaching pocket change. This is, in effect, a fourth generation of identity fraud. Where earlier generations relied on stolen paper documents, then stolen data, then manually operated fraud rings, this generation is defined by AI-driven scale and speed that first-generation, one-time identity checks were never built to withstand.

The answer is not to make government services harder to access for everyone. The answer is to make identity verification smarter, faster, and more adaptive.

Congress should move federal programs away from static, point-in-time checks and toward real-time, risk-based identity decisioning that evaluates identity across the full lifecycle of an account, before money goes out the door and as risk changes over time. That means broader signals, better analytics, continuous testing, stronger data-sharing authorities, and accountability for outcomes: whether systems actually stop stolen and synthetic identities while allowing legitimate Americans to access the services they need.

Thank you for the opportunity to testify on a subject that will determine in no small part whether Americans can trust their government in the digital age.

My name is Jordan Burris, and I am the Head of Public Sector at Socure.

Socure was founded in 2012 on a simple premise: verifying someone's identity online should be fast, accurate, and fair, not a bureaucratic guessing game built on a name and a Social Security number. From the outset, Socure was built as a data science company, applying artificial intelligence and machine learning to identity rather than retrofitting those tools onto systems designed for a world of paper documents and credit files.

That approach has scaled: Socure today serves more than 3,000 customers in over 190 countries, across financial services, government, healthcare, gaming, telecommunications, and e-commerce, including 18 of the 20 largest U.S. banks, four of the world's largest technology companies, more than 600 fintechs, and over 150 public sector organizations at the federal, state, and local level.

In some of the highest-risk populations we serve, our models capture up to 99 percent of fraud while still verifying as many as 98 percent of legitimate applicants, including people who would be invisible to a system built around a thin or nonexistent credit file. Socure was built to be the next generation of identity verification, in contrast to a first generation of tools built around static compliance checks and legacy credit and data-broker files. That distinction, between a system engineered for yesterday's fraud and one engineered to keep adapting to tomorrow's, is the organizing idea behind my testimony today.

Before joining Socure, I served as Chief of Staff in the White House Office of the Federal Chief Information Officer across two presidential administrations, where I helped oversee execution of the federal government's technology and cybersecurity portfolio, including a budget of more than $90 billion.

That work put me in the room for three moments that are directly relevant to what this Subcommittee is examining today.

- In 2019, I was a principal author of OMB Memorandum M-19-17, the policy that reset how federal agencies manage identity, credentials, and access government-wide.[1]

- In 2020, I was part of the team inside the White House that made real-time decisions on how the federal government would verify the identity of Americans seeking emergency benefits online during the early, chaotic months of the COVID-19 pandemic, when the tradeoffs between speed and assurance were not theoretical; they were decided in real time, with real consequences.

- Beginning in late 2020 and into 2021, I was also part of the team that led the federal government's response to the SolarWinds breach and helped lay the policy groundwork for the government-wide shift toward Zero Trust architecture that followed. I have carried the lessons of all three of those moments into this hearing today.

These three moments taught me a key lesson. The adversary we are up against is patient and cunning and has consistently adapted faster than the technology landscape inside the government has been allowed, or able, to move. When that gap opens, it is not an abstraction. It is the public that pays for it, in stolen benefits, denied services, and the erosion of trust that follows.

I left the government out of a sense of duty to close that gap from the outside: to find and help implement better ways to defend taxpayer dollars and unlock the promise of digital services for the Americans who depend on them.

I have spent the last fifteen years working on this challenge from both inside and outside the government. The question has never changed: how does the government know, with confidence, that the person on the other side of a digital transaction is who they claim to be?

That is why I am here today.

I will cover four topics in my testimony.

First, why the threat has outpaced a model that still treats identity verification as a single front-door checkpoint rather than something to be evaluated across the full lifecycle of an account, continuously and in real time.

Second, why this problem is bigger than any one platform and should be treated as national infrastructure.

Third, why the standard government holds itself to must shift from compliance to confidence, and get ahead of where the threat is going rather than chasing where it has been.

And fourth, the evidence that a different approach already works, and the concrete steps this Subcommittee can take to make it the default.

I. Fraud 4.0: The Threat Has Outpaced the Model Built to Stop It

For two decades, the federal government's approach to identity verification has been organized around a static idea: confirm that a name, date of birth, and Social Security number belong together, check that combination against a handful of authoritative files, and treat a match as

[1]Office of Management and Budget, Memorandum M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 21, 2019.

proof of identity. This legacy model is fundamentally broken, and is exploited by our adversaries on a daily basis.

Artificial intelligence has moved identity fraud from a cottage industry into an industrial one.

Tasks that once required time, technical skill, and coordination across criminal networks can now be automated end to end.

In one documented case, a ring tracked by Socure executed 38,241 transactions across 465 organizations in 30 industries within a single 90-day window. This is, in effect, a fourth generation of identity fraud. Where earlier generations relied on stolen paper documents, then stolen data, then manually operated fraud rings, this generation is defined by AI-driven scale and speed that first-generation, one-time identity checks were never built to withstand, and fail under the industrialized scale of attacks.

What has changed since those figures were first reported is not the presence of fraud; it is its speed and sophistication. Socure's fraud research team, drawing on analysis of more than 80 million transaction records over a two-year observation period, documented a case in which a single fraud ring purchased 340 internet domains, used generative AI to manufacture 24,148 distinct synthetic identities, and launched 35,894 separate application attacks against government and commercial targets, all within roughly 30 days, with many attacks following identity creation by less than 48 hours.[2] That is not a criminal exploiting a gap; it is an assembly line of fraud.

This is not confined to the commercial sector. In a case Socure's researchers documented against U.S. public sector agencies, a single fraud ring executed more than 60 attacks across multiple government programs in roughly five weeks, using stolen but genuine identity information paired with fabricated email addresses, foreign VPN infrastructure, and phone numbers linked to multiple unrelated identities, targeting victims across eight states.[3] A second, unrelated ring ran 36 fraudulent applications against government programs over a four-month span using the same basic method: real stolen identities, fabricated contact information layered on top. These were not opportunistic attempts. They were operations, run with the discipline of a business process or a military campaign.

The identity signals the government has relied on for a generation are also eroding in real time, and not by accident. In one case, a single fabricated phone number was linked to 987 separate applications tied to 207 synthetic identities across 25 states in a single month.[4]

Nearly a quarter of fraudulent attempts now show materially compressed distance between a claimed address and the IP address used to apply, as fraud rings increasingly route through illegally accessed residential proxy infrastructure rather than the hosting providers and VPNs that used to expose them; residential-flagged traffic in fraud populations rose from roughly two-thirds to more than 80 percent over the same two-year window.[5] Fraud rings are deliberately engineered around the very patterns, such as reused emails, reused devices, and geographic distance, that legacy fraud detection depends on to notice repeat offenders. A verification model built to catch reuse and geography cannot catch an adversary that has already engineered both away. What is left to find them is the connective tissue between signals: how

[2]Socure, "Fraudsters Are Changing Playbooks — and the Data Proves It," Fraud Insights Report, March 2026, based on analysis of more than 80 million transaction records, including approximately 40 million confirmed fraud and high-risk applications, over a two-year observation period.
[3]Socure, "Fraud in Focus: Exposing Organized Fraud Patterns in Government Programs," Identity Risk Insights Report, 2025.
[4]Socure, "Fraudsters Are Changing Playbooks — and the Data Proves It," Fraud Insights Report, March 2026.
[5]Ibid.

identity elements, device and email infrastructure, digital behavior, and historical outcomes relate to one another across the full lifecycle of an account, not whether any single one of them matches a file. That is a fundamentally different engineering problem than the one federal identity systems were designed to solve, and it is why point-in-time, single-source checks are no longer a sufficient defense on their own.

This is the environment every identity system now has to operate in, including platforms like Login.gov that were built to a formal government standard. A framework built around a single verification moment, checked once at enrollment and then treated as durable proof for as long as the account exists, was never going to keep pace with an adversary that iterates in hours.

The lesson is not about any one platform's compliance record. It is that identity cannot be treated as a front-door problem, solved once at onboarding. It has to be evaluated across the full lifecycle of an account, continuously and in real time.

This is the fundamental shift in conceptualizing the challenge and the solution that we need to make.

II. This Is Bigger Than One Website: Identity as National Infrastructure

Login.gov, in fact, is a prime example of why this matters at national scale, not because of any single compliance finding, but because of how much our nation now depends on it.

Tens of millions of Americans use it to access federal benefits and services, and its role continues to grow. The Department of Homeland Security designated identity management as one of the nation's 55 National Critical Functions in 2019, defined as functions so vital that their disruption would have a debilitating effect on national security, economic security, or public health and safety.[6] Identity verification is quietly becoming the substrate underneath nearly every interaction Americans have with their government: benefits, tax administration, veterans' services, disaster relief, and credentialing for critical infrastructure. When identity assurance is treated as a one-time front-door check rather than a continuous discipline, the risk does not stay contained to one place. It travels everywhere that determination is trusted.

Some of the programs most exposed to this risk are also among the least modernized. FEMA's disaster assistance programs and CMS's Medicare and Medicaid systems, to name just two, still lean heavily on identity approaches that have not fundamentally changed in decades, even as they process some of the highest-volume, highest-value, and most urgent transactions in government, often for people who have just lost a home, a job, or a loved one. Those are precisely the moments when the pressure to move fast collides hardest with the need to verify correctly, and precisely the moments when a stale identity model does the most damage, to both the taxpayer and the applicant.

The same dynamic plays out in the national security context. Identity is now a contested domain in its own right. Socure's own research into fraud against public sector agencies has tracked international fraud rings targeting U.S. government programs from China, Russia, Poland, India, South Africa, the Philippines, and elsewhere, responsible for between 2 and 12 percent of all incoming applications to the programs studied.[7]

---

[6]U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, National Critical Functions Set, designating identity management as one of 55 National Critical Functions, 2019.
[7]Socure, "Fraud in Focus: Exposing Organized Fraud Patterns in Government Programs," Identity Risk Insights Report, 2025.

These fraud rings treat U.S. government identity systems as a target of first resort, not because the money in any one program is uniquely large but because access is uniquely valuable: at least 25.2 percent of documented fraud attempts against government targets, roughly one in four, hit more than one agency simultaneously, and once a fraud ring successfully establishes a stolen identity, it is reused against the next attack in as little as three weeks and, in some cases, the same day. Fraudsters targeting government programs also favor stealing a real person's identity over fabricating one entirely, by a margin of almost four to one, precisely because it lets them reach a real person's existing benefits and payments.[8] Treating each program's identity verification as a separate, siloed procurement decision all but guarantees that fraud rings will keep finding the weakest link, moving through it, and breaking the chain protecting taxpayer dollars.

I would also urge the Subcommittee not to let this conversation collapse into a tradeoff between security and access. Some of the communities most dependent on federal programs, including younger Americans, recent immigrants, rural residents, and people who have experienced housing instability, are disproportionately underrepresented in the credit files and commercial data sources that much of the identity verification industry still relies on as its primary evidence. A model that verifies identity through broader, more inclusive data and real-time signals, rather than a thin credit history, can close that gap rather than widen it.

After 15 years in this work, I have come to the belief that access and security are not competing priorities in identity verification. They are the same objective, measured two different ways: does the system correctly say yes to the people who should get through, and correctly say no to the ones who should not.

III. From Compliance to Confidence: Standards Must Get Ahead of the Threat

I would ask the Subcommittee to draw an important distinction that I believe should organize our nation's approach to this entire policy area. It's the difference between identity validation and identity verification. Validation confirms that a data combination, such as a name, a birth date, and a Social Security number, exists somewhere and is internally consistent. Verification confirms that the specific person in front of the system, right now, in this transaction, is the rightful owner of that identity. A stolen identity can pass validation perfectly. Only continuous, adaptive verification stops it.

Much of the federal government's identity infrastructure, and a great deal of the identity verification industry serving it, was built on the validation model: match a submitted identity against a credit file or a commercial data broker's holdings, and treat a hit as sufficient.

That approach has three structural weaknesses this moment has exposed.

First, credit and data broker files are themselves frequently compromised; the same breaches that put Americans' data at risk in the first place are often the very source data fraud rings use to defeat these checks.

Second, that model performs unevenly across the population it is meant to serve: Americans with thin credit files, including younger people, new arrivals, and residents of underserved communities, are disproportionately unable to clear it even when they are exactly who they say they are.

[8]Ibid.

Third, and most relevant to this hearing, it treats identity as a front-door problem: verified once at enrollment, then assumed durable for the life of the account. It says nothing about whether the identity is still behaving like itself five minutes, five days, or five months later. Fraud does not stop at the front door, and identity verification cannot either. It has to span the full lifecycle of an account and be evaluated continuously, in real time.

The starkest example of this problem is still in active use across parts of government today, knowledge-based authentication. That's the practice of confirming someone's identity by asking for information such as a mother's maiden name, a previous address, or the make of a first car.

This approach rests on the assumption that only the real person would know the answer. After more than a decade of large-scale data breaches, much of this information is now searchable, purchasable, or simply public. Relying on knowledge-based authentication today is not a modest gap in an otherwise sound system. It is a lock guarding a taxpayer-funded benefit when fraud rings have long since been handed the key.

This gap between what a technique appears to guarantee and what it can actually withstand is not unique to knowledge-based authentication. It runs through much of what currently counts as sufficient identity verification across government.

There is a simple market test this Subcommittee can apply to see that gap clearly, and I would encourage it to use it: look at where the identity verification approaches relied on widely across federal programs actually get used to back real financial risk in the private sector, not just to satisfy a compliance requirement. In the vast majority of cases, the private sector has moved well beyond knowledge based authentication to adaptive verification. When private funds are at stake, companies choose modern approaches to identity.

In government, however, these approaches are treated as adequate because the downside of getting it wrong is diffuse: a benefit paid to the wrong person, a loss absorbed by a trust fund, a cost spread across taxpayers. Ask instead whether a bank underwriting a loan, a card network authorizing a transaction, or an insurer pricing a policy is willing to put its own balance sheet behind that same identity decision, and in most cases the honest answer is no.

That gap, between what is accepted as good enough for the government and what the private economy is actually willing to stake real money on, should concern this Subcommittee more than any single platform's certification status. A standard that cannot survive contact with people who lose their own money when it fails is not a standard. It is a hope.

The alternative is not a new checklist. It is a dramatically different architecture: real-time, risk-based identity decisioning that draws on a much broader set of signals, including document authentication, biometric and liveness comparison, device and behavioral analytics, and machine learning models trained continuously against emerging fraud patterns, applied at the moment of the transaction and reapplied as risk changes, rather than certified once and assumed forever. Done well, this approach does not trade security for access. It improves both at once, because it lets agencies apply friction only where risk actually warrants it, rather than imposing the same burden on every applicant regardless of risk.

I recognize this Subcommittee may hear this problem framed primarily as a question of certification and enforcement: which standard a vendor is certified against, and how aggressively fraud is prosecuted after the fact. Certification and prosecution both matter, but neither is sufficient on its own.

A system can be built toward a rigorous certification and still find that the certification alone does not keep pace with how fraud actually evolves in production, and prosecution only ever recovers a small fraction of what is stolen; federal recovery of pandemic-era fraud losses remains in the low single-digit billions against total losses estimated in the hundreds of billions.[9] A standard that only describes what fraud looked like when it was written will always be a step behind.

Congress cannot and should not legislate its way to safety through certification requirements and recovery mandates alone if the decisioning model those certifications describe is not tested against how fraud actually behaves today, and continuously updated as it changes tomorrow. The standard has to be an outcome, set ahead of the threat rather than in reaction to it. It should ask whether this system can tell a real identity from a fabricated one, in production, against current adversary tactics, and across every demographic it serves, rather than whether a document says it can.

IV. Proof That a Different Model Works

This Subcommittee need not take this different approach on faith. There is a growing body of evidence, inside and outside government, that prevention-first, real-time identity decisioning works at scale.

The Department of Education's Federal Student Aid office embedded real-time, risk-based identity screening directly into the FAFSA application this cycle, evaluating identity before aid is disbursed rather than trying to recover it afterward. The Department estimates this protected more than $1 billion in taxpayer dollars in a single cycle, with legitimate applicants passing through automatically at a rate above 92 percent.[10] Socure supported FSA in building this capability, and the effort went from initial engagement to production in a matter of weeks, a pace that is unusual in federal technology delivery and one I believe should be the expectation rather than the exception.

Meanwhile, the Department of the Treasury's expansion of the Do Not Pay service tells a similar story on the data-access side of this problem. The first year of a pilot using the Social Security Administration's full death records returned $113.5 million in prevented or recovered improper payments against pilot costs, roughly a 23-to-1 return.[11] Yet as of fiscal year 2024, only about 4 percent of federal programs had completed the legal steps required to access the full suite of Do Not Pay data sources.[12] The tools are proving themselves. Adoption, not invention, is the bottleneck.

These examples share a structure that the Subcommittee can drive adoption of: prevention embedded before payment, risk-based rather than one-size-fits-all friction, and continuous rather than point-in-time verification. None of them required Congress to pick a technology. They required Congress and the agencies it oversees to change what they measure and reward.

V. Recommendations

[9]U.S. Government Accountability Office, "Unemployment Insurance: Estimated Amount of Fraud During Pandemic Likely Between $100 Billion and $135 Billion," September 2023.
[10]U.S. Department of Education, "U.S. Department of Education Launches Comprehensive, Nationwide Federal Student Aid Fraud Prevention Effort," Press Release, April 27, 2026.
[11]U.S. Department of the Treasury, Do Not Pay pilot results using the Social Security Administration's Death Master File, cited in GovNavigators/Socure Roundtable Report, January 2026.
[12]Ibid. As of fiscal year 2024, only approximately 4 percent of federal programs had completed the legal requirements to access all Do Not Pay databases.

Based on what I have seen work, and what I have seen fail, I offer the Subcommittee five recommendations.

First, replace point-in-time compliance certification with continuous, outcome-based performance testing for any identity verification system used by the federal government. A system should have to demonstrate, on an ongoing and independently verified basis, that it can distinguish real identities from fabricated or stolen ones across current attack patterns and across demographic groups, not simply attest once that it was built to a standard. That standard should evolve continuously alongside the threat, rather than being fixed at a single point in time and revisited only when something goes wrong. As a starting point, Congress should direct agencies to formally sunset knowledge-based authentication for identity-proofing purposes government-wide. It is a legacy technique whose core premise, that the answers are secret, has not held for well over a decade.

Second, require agencies to evaluate identity risk across the full lifecycle of an account, not only once at enrollment. Real-time, pre-disbursement identity screening should be the default posture for federal benefit and payment programs, not an optional enhancement layered on after a fraud event, and that same real-time discipline should extend to activity on an account well after onboarding is complete. The FAFSA experience shows this is achievable within a single application cycle when agencies are given both the mandate and the flexibility to move quickly.

Third, make permanent and expand the data-sharing authorities that are already proving their value, starting with full Do Not Pay access across all federal agencies and programs, and remove the legal and procedural friction that has left the overwhelming majority of programs without full access years into this effort. Congress should extend that same logic beyond government. An example: the Social Security Administration's Electronic Consent Based Social Security Number Verification service already lets financial institutions ask, with a consumer's consent, whether a name, date of birth, and Social Security number match, without ever exposing the underlying data itself. This could be expanded well beyond the SSN and close one of the most significant gaps in the fight against fraud today.

Fourth, align oversight and budget incentives with prevention rather than recovery. Programs and agency leaders should be measured, and rewarded, for fraud dollars that were never disbursed in the first place, not only for the much smaller share ever recovered after the fact.

Fifth, treat identity verification as dynamic infrastructure that must be resourced to evolve continuously, not a system built once, certified once, and left in place for a decade. The fraud rings I described earlier iterate in hours. Federal procurement and budget cycles measured in years cannot defend against that unless Congress explicitly directs agencies to fund continuous adaptation, not a one-time system replacement.

VI. Conclusion

I called this problem World War Fraud earlier because I think this Subcommittee should treat it with that level of seriousness. The United States has the technology, the data, and now the hard evidence to stop treating identity fraud as an inevitable cost of doing business and running programs at scale.

What has been missing is not capability. It is the expectation, set clearly by this body, that government identity systems be judged by whether they actually work against the fraud we face today, not by whether they were once certified against the fraud we faced a decade ago.

This is not a story about any one platform. It is about whether our government treats compliance and confidence as the same thing, when they are not, and whether it treats identity verification as a single check at the front door rather than a discipline that has to span the full lifecycle of an account, continuously and in real time.

Closing this gap is one of the most consequential things this Congress can do for the millions of Americans who depend on federal programs working correctly quickly.

I am grateful for the opportunity to support this effort, and I welcome the Subcommittee's questions.