

AI vs. AI:

Defending Digital Trust in the Age of Intelligent Fraud

Uncover how government agencies can
recognize emerging AI-powered threats
and build smarter, more adaptive defenses.



AI Is Changing What Government Can Trust

Artificial intelligence is transforming how government delivers services. But it is also transforming how fraud is committed.

Fraudsters can use increasingly sophisticated AI tools to create convincing identities, generate realistic documents, impersonate trusted individuals and automate attacks at a speed and scale traditional defenses were never designed to address.

Every application, account, credential, payment and digital interaction depends on trust. Agencies must determine whether an identity is legitimate, whether the information and relationships behind it make sense,

whether risk is present and whether the resulting decision can be explained and defended.

AI is making those decisions harder.

A fake identity can look established.

A fraudulent document can appear authentic.

A cloned voice can sound familiar.

An authenticated account can still be compromised.

An automated attack can operate faster than human teams can respond.

The answer cannot simply be more friction, more manual review or another verification step.

It requires more intelligence and greater confidence in the decisions that intelligence supports.

The opportunity is to build a more dynamic model of digital trust, where trusted identity intelligence, authoritative data, relationship intelligence and transparent AI reveal risk earlier, strengthen decision confidence and preserve access for legitimate residents.

Because in today's AI-driven world, government does not just need faster answers.

It needs intelligent decisions it can verify, explain and defend.

Every Digital Doorway Creates a Trust Decision

A resident applies for benefits.

A driver requests an identity credential.

A beneficiary changes a payment method or account number.

Each interaction requires an agency to answer a fundamental question:

Can we trust this interaction?

That requires five increasingly important capabilities.



Trusted Identity

Establish confidence in every identity and interaction.



Responsible AI

Apply AI with governance, oversight and accountability.



Uncover Hidden Connections

Reveal hidden connections across identities, entities and risk.



Secure Transparency

Deliver transparent, defensible and auditable AI-driven insights.



Transform Outcomes

Turn trusted intelligence into better agency outcomes.

Together, these capabilities create a more complete model of digital trust, one designed not simply to detect fraud, but to support more confident government decisions.

FIVE WAYS AI IS CHALLENGING DIGITAL TRUST

Threat 1: Fake Applicants That Look Real

Synthetic Identity Fraud

Synthetic identities combine real and fabricated information to create personas that may never have belonged to an actual person.

A legitimate identifier may be paired with a fabricated name, address, phone number or date of birth. The identity can then develop a digital footprint over time, gradually appearing more credible before being used to obtain benefits, services, licenses, refunds or payments.

Traditional verification may confirm that individual pieces of information exist without determining whether those pieces legitimately belong to the same person.



GOVERNMENT IMPACT

- ✓ Fraudulent benefit enrollment
- ✓ Improper payments
- ✓ Fraudulent tax refunds
- ✓ Fake residents in agency systems
- ✓ Fraudulent professional licenses
- ✓ Account creation fraud



Building a More Robust View of Identity

Detecting synthetic identity risk requires looking beyond individual records.

Identity resolution and verification can help establish confidence in the identity itself, while relationship and network intelligence can reveal connections across identities, entities and attributes that may not be visible when signals are evaluated independently.

The technical shift is from confirming that individual data points exist to understanding whether they belong together and behave consistently as one identity.

Trust must be measured continuously across the online identity journey, not just at onboarding or login.

A valid identifier, address or credential does not necessarily mean the identity presenting it is legitimate.

The greater opportunity is to measure the identity's liveness, behavioral intelligence, and device risk intelligence to help eliminate any detected risk.

FIVE WAYS AI IS CHALLENGING DIGITAL TRUST



Threat 2: When You Can No Longer Trust a Face

Deepfakes and Biometric Spoofing

Seeing and hearing are no longer necessarily believing.

AI-generated faces, cloned voices, manipulated video and sophisticated injection attacks are challenging assumptions that once underpinned remote identity verification.

An attack may not even involve someone physically presenting a fake face to a camera. Digital content can potentially be injected directly into a verification workflow.

That changes the question from:

Does this look or sound like the right person?

to:

What combination of evidence gives us confidence that this is a legitimate interaction?



GOVERNMENT IMPACT

- ✓ False or “Ghost” enrollments
- ✓ Account takeover
- ✓ Digital credential fraud
- ✓ Call-center impersonation
- ✓ Compromised identity-proofing workflows



Building Layered Identity Assurance

Biometrics remain an important identity signal, but they should not carry the entire burden of trust.

AI Deep Learning analysis of liveness, biometric authentication and deepfake detection can expose sophisticated manipulation, while identity, device and digital intelligence expose fraud risk intelligence beyond biometric verification.

The goal is risk-based assurance across the identity journey:

More risk → More assurance

Less risk → Less friction

No single signal should determine trust.

As AI makes individual signals easier to imitate or manipulate, confidence increasingly comes from evaluating multiple independent signals together.

FIVE WAYS AI IS CHALLENGING DIGITAL TRUST

Threat 3: Documents That Pass Inspection, but Shouldn't

AI-Generated Document Fraud

Government agencies have historically relied heavily on documents as evidence.

Driver's licenses. Passports. Proof-of-address documents. Tax records. Supporting credentials.

Generative AI compromises that model because fraudulent documents can become increasingly realistic.

That puts front-line employees and manual-review teams in a difficult position: asking people who are not forensic experts to distinguish sophisticated digital fabrications from legitimate documents.



GOVERNMENT IMPACT

- ✓ Benefits administration
- ✓ DMV issuance and transactions
- ✓ Tax administration
- ✓ Licensing
- ✓ Residency verification
- ✓ Workforce eligibility

Looking Beyond Appearance

Document inspection remains important, but appearance alone is no longer sufficient.

Modern verification can combine AI-powered document authentication with trusted identity intelligence and authoritative data to evaluate both the document and the identity behind it.

The question changes from:

Does the document look real?

to:

Can the information and identity behind it be trusted?

Authenticity requires validating the information behind the document, not simply the document itself.

For CIOs, that means document authentication should not operate as an isolated pass/fail control. It should contribute to a broader identity and risk decision.



Protecting Access While Protecting the Program

Stronger fraud prevention should not mean making every legitimate resident work harder to prove who they are.

The objective is **risk-based intervention**, using intelligence to distinguish routine interactions from those that warrant additional scrutiny.

More risk → More assurance

Less risk → Less friction

Done well, this helps agencies protect public resources while preserving access for legitimate people.

FIVE WAYS AI IS CHALLENGING DIGITAL TRUST

Threat 4: Trust Becomes the Attack Vector

AI-Powered Social Engineering

Some of the most effective attacks do not defeat technology.

They defeat trust.

Generative AI can help fraudsters create highly personalized phishing campaigns, clone voices, impersonate officials and generate convincing interactions across email, chat, voice and digital portals.

The attack may also occur after a person has already been authenticated.

A payment destination may change. A trusted account may suddenly behave differently. An employee may receive a convincing request from someone who appears to be a colleague or vendor.



GOVERNMENT IMPACT

- ✓ Account takeover
- ✓ Credential compromise
- ✓ Vendor impersonation
- ✓ Payment diversion
- ✓ Constituent service fraud



Making Trust Dynamic

Digital and device intelligence can provide context about the environment behind an interaction.

Behavioral intelligence can identify activity inconsistent with expected human behavior.

Relationship intelligence can reveal connections that change how an interaction should be understood.

Real-time risk assessment can bring those signals together to determine whether the interaction should proceed, receive additional assurance or move to review.

Authentication is traditionally performed at a point in time. In an evolving risk landscape, trust must be reassessed continuously.

Trust is dynamic.

FIVE WAYS AI IS CHALLENGING DIGITAL TRUST

Threat 5: Fraud Moves to Machine Scale

Agentic AI Fraud

AI systems are beginning to make it possible to automate multiple stages of a fraud operation, from reconnaissance and identity creation to authentication testing, application submission and attack adaptation.

It lowers the point of entry for threat actors, increases the scale, and shrinks the time to compromise .

A human fraudster has limited time and capacity.

Automated systems do not operate under the same constraints.

As the effort required to launch sophisticated attacks declines, agencies may face greater attack volume, faster experimentation and increasingly adaptive tactics.



GOVERNMENT IMPACT

- ✓ Mass application fraud
- ✓ Automated account creation
- ✓ Increased improper payments
- ✓ Operational strain
- ✓ Greater audit exposure

Most importantly, machine-scale fraud can overwhelm defenses designed primarily around human review.



Building Defenses That Can Keep Pace

The answer is not simply more automation.

It is **intelligent orchestration**: evaluating identity, device, behavior, relationships and risk together, then dynamically determining the appropriate response while remaining transparent to the user.

Low-risk interactions can proceed with minimal friction.

Higher-risk interactions can trigger stronger assurance, additional verification or human review.

This allows technology to absorb scale while preserving human judgment for consequential or ambiguous decisions.

Defenses must operate at the speed and scale of the attacks they are designed to stop.

Automation should not replace experienced government professionals.

It should focus their expertise where judgment and intervention matter most.

Transparent and Accountable AI

AI Is Your Defense

AI-powered defense introduces another critical trust decision:

Can the agency trust and defend the intelligence informing its decisions?

Government cannot respond to increasingly sophisticated fraud by introducing systems it cannot understand, govern or explain.

When AI contributes to decisions involving benefits, healthcare, payments, credentials or other essential services, agencies need confidence not only in the outcome, but also in the intelligence, controls and reasoning behind it.

That makes transparency more than a technology requirement.

It is a government accountability requirement.

For CIOs, **transparent and accountable AI** should support four foundational capabilities:



Explainability and Auditability

Agencies should be able to understand why an interaction was flagged or escalated, trace the relevant signals contributing to the outcome and retain sufficient evidence for appropriate review.



Human Oversight

Experienced professionals should remain appropriately involved when decisions require judgment, intervention or escalation.



Privacy, Fairness and Accessibility

Fraud controls should protect public resources without creating unnecessary or inequitable barriers for legitimate residents.



Governance

Clear policies, controls, ownership and accountability should guide how AI models and automated decisioning are deployed, monitored and changed over time.

The objective is not AI making consequential decisions in isolation.

Transparent intelligence helps experienced people make more confident, explainable and defensible decisions.

From Detection to Confident Decision-Making

AI-powered fraud requires more than detecting suspicious activity. It requires intelligence that can reveal risk early enough to inform the decision itself.

The Shift

Isolated identity checks → Continuous identity assurance

Individual data points → Connected intelligence

Hidden relationships → Full-picture understanding

After-the-fact detection → Earlier risk identification

Review everything → Risk-based intervention

Black-box outcomes → Explainable, traceable intelligence

This is more than technology modernization.

It is a shift toward government decisions that are faster, smarter and more defensible.

What Comes Next

Today's threats are only part of the story.



AI Agents Acting as Citizens

Autonomous agents capable of executing government transactions and creating, modifying and/or maintaining fraudulent identities.



Synthetic Households and Fraud Networks

Coordinated identities, households, providers and beneficiaries operating across programs.



Credential and Digital Wallet Manipulation

Attacks targeting trusted digital identity ecosystems and credential-issuance processes.



Cross-Channel Fraud Orchestration

AI coordinating attacks across web, mobile, call center and in-person channels.



Self-Learning Fraud Operations

Fraud systems that continually adapt tactics based on agency responses and controls.

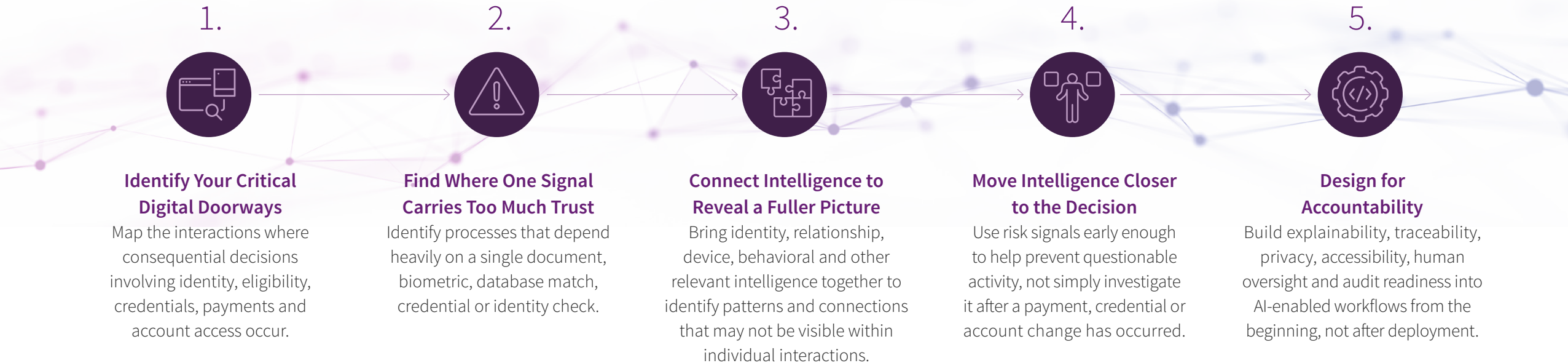
The future of fraud is not simply better deception.

It is fraud that can become autonomous, adaptive and increasingly capable of operating at scale.

Five Actions Government Leaders Can Take Now

Preparing for AI-powered fraud does not necessarily require a multi-year transformation.

Agencies can begin by strengthening the trust decisions that matter most.



Start where risk and mission impact are highest. Demonstrate value. Then expand.

From Strategy to Defense

Building a more complete view of identity and risk.

As AI-powered fraud becomes more sophisticated, agencies need the ability to evaluate risk across the entire interaction, not through disconnected checks or a single point of verification.

That requires bringing multiple dimensions of intelligence together.



Trusted Identity Intelligence

Establish confidence in identities and determine whether attributes belong to the right person.



Relationship Intelligence

Reveal connections across identities, entities, households, associates and interactions that isolated records may miss.



Digital Intelligence

Understand device characteristics, location, bot activity and the digital environment behind an interaction.



Behavioral Intelligence

Identify anomalous patterns that may indicate automated, compromised or fraudulent activity.



Document and Biometric Intelligence

Authenticate evidence and introduce stronger identity assurance when risk warrants it.



Risk Intelligence

Connect signals to identify patterns, anomalies and emerging threats earlier.



Transparent AI and Intelligent Orchestration

Bring intelligence together within dynamic workflows to determine the appropriate next action, with explainability and human oversight where needed.

Multiple signals.
One confident decision.

The result is not simply another identity check or another fraud score.

It is a more complete view of identity and risk, designed to help agencies understand:

Who are we interacting with?

What relationships, behaviors and risks surround the interaction?

What level of assurance is appropriate?

Why was that action taken?

For a CIO, that last question matters as much as the first three.

This creates a more adaptive model of digital trust:

More risk → More assurance

Less risk → Less friction

And it supports something bigger than fraud prevention:

- ✓ **Faster service.**
- ✓ **More efficient operations.**
- ✓ **Stronger accountability.**
- ✓ **More confident government decisions.**

Turning Intelligence Into Trusted Outcomes

LexisNexis® Risk Solutions brings together trusted identity intelligence, authoritative data, relationship intelligence, advanced analytics and transparent AI to help government agencies reveal risk, secure transparency and make more confident, defensible decisions.

LexisNexis EssentialID® extends that intelligence through an adaptive identity assurance and orchestration approach, bringing together identity, digital, behavioral, document, biometric and other risk signals within dynamic workflows.

The objective is not more verification for everyone.

It is greater confidence where it matters.

More risk → More assurance.

Less risk → Less friction.

This helps agencies strengthen fraud defenses, maximize resources and deliver secure, seamless services while supporting decisions that can be understood, explained and defended.

Independently Recognized Innovation

AI-Driven Deepfake Detection

Award winner, Chartis RiskTechAI50, 2025.

Advanced Fraud Prevention and Behavioral Analytics

Recognized technology provider, Everest Group Top 50™ Financial Crime and Compliance Technology Providers, 2026.

Orchestration Platform

Platforms category award winner, Chartis Financial Crime & Compliance50, 2026.

AI vs. AI

Today's AI has changed what government can trust.

An identity that looks established may be synthetic.

A face or voice may be generated.

A convincing document may be fabricated.

An authenticated account may be compromised.

And an interaction that appears to come from a person may increasingly be driven by a machine.

Government cannot respond by making every interaction harder.

Nor can agencies expect human teams to manually identify every increasingly sophisticated attack.

The opportunity is a smarter model of digital trust, one built on trusted identity intelligence, authoritative data, relationship intelligence, multiple risk signals, transparent AI and human expertise.

When governed transparently and paired with human oversight, today's AI can help reveal relationships, identify emerging risk, prioritize intervention and give experienced professionals stronger identity intelligence the moment decisions are made.

The objective is not to automate trust.

It is to power more confident decisions.

Decisions government can act on.

Decisions government can explain.

Decisions government can defend.

It takes AI to fight AI.

Find Out More

[IDVerse – Unmasking Deepfakes](#)

[Global State of Fraud Report](#)

[Explore LexisNexis EssentialID®](#)





Find Out More
Scan or call 1-888-216-3544



This material is provided for informational purposes only and does not constitute legal, regulatory, compliance, cybersecurity, or professional advice. LexisNexis® Risk Solutions products and services assist organizations in evaluating identity, fraud, and risk indicators but do not guarantee detection or prevention of all fraudulent, unauthorized, or improper activity. AI-enabled tools and analytics provide risk insights and recommendations that should be considered with human judgment and organizational policies. References to future trends, emerging threats, awards, or recognitions are provided for informational purposes only and are not guarantees of future results. Organizations remain responsible for compliance with applicable laws, regulations, policies, and operational requirements.

LexisNexis, LexisNexis EssentialID and the Knowledge Burst logo are registered trademarks of RELX Inc., registered in the U.S. or other countries. Other products or services may be trademarks or registered trademarks of their respective companies. Copyright © 2026 LexisNexis Risk Solutions.

NXR17178-00-0926-EN-US

