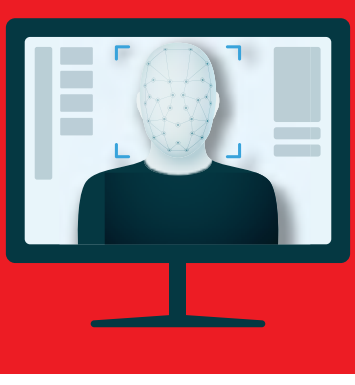
The Perfect Storm

AI, ChatGPT, and Deepfake Threats on Government Agencies

Fraudsters are turning to generative artificial intelligence (AI) for swindling millions of dollars from unwitting victims and government agencies. It's now easier than ever to bypass legacy document authentication and "liveness checks" to fraudulently claim benefits with readily available AI tools.

The advent of AI has given rise to a new form of deception called "deepfakes" – digital manipulations of photos, audio, or videos that convincingly replace one person's likeness with another. With the exposed data vulnerabilities, the issue is critical when it comes to preventing nearly perfect identity imposter fraud.



No Government Program is Safe

Fraudsters now employ AI tools with minimal technical expertise to download someone's pictures from various online sources and generate realistic images, imitate their voice, or even create videos of them engaging in events that never actually occurred. AI generated images create a world where humans often can't tell what images are fake. **Government agencies are incredibly vulnerable.**

Verification based on static identity attribute assessment and vulnerable physical documents alone is outdated, bringing unnecessary, avoidable risk to both the agency and the individual.

The breaches of state and federal databases indicate fraudsters are targeting government data sources to beat National Institute of Standards and Technology (NIST) Identity Assurance Level (IAL) standards. It is critical that, as an identity community, we act swiftly and collectively to stay ahead of these emerging threats.

Numerous static data points that generative AI needed are now available at scale due to recent DMV data breaches. This combination of data and AI technology will materialize as "guaranteed" fake drivers licenses, real driver's licenses for imposters, and real-time deepfake (a.k.a. identity not present) impersonation.

The challenge of outsmarting generative AI attacks is made worse when trusted "referees" are tasked with making picture-to-person comparisons on their own – using humans to make risk-based decisions.

AI and deepfakes can bypass the IAL2 facial recognition and liveness checks employed by many agencies with astonishing ease – seamlessly deceiving systems designed to authenticate individuals based on their facial features and real-time interactions.

Government agencies – and the U.S. taxpayer – stand to lose billions, if not trillions of dollars due to fraudsters deploying AI-enabled fraud

Hundreds of billions of dollars were plundered from the coffers of vital government programs — rent relief, unemployment benefits, SNAP benefits, and PPP loans became piggy banks for thousands of domestic and transnational cybercriminals.[1]

Social Security benefits are a lifeline for millions of Americans. AI could generate synthetic identities matching the profile of legitimate beneficiaries, **directing millions of dollars away from deserving recipients**.[1]

Medicare and Medicaid: AI could fabricate seemingly legitimate medical claims, leading to the loss of billions of dollars — funds intended to ensure that low-income families and seniors can access vital healthcare services.[1]

Tax collection, the backbone of our government funding, could be compromised. Advanced AI algorithms could create complex tax returns designed to **exploit loopholes and maximize fraudulent refunds**.[1]

In North America, the proportion of deepfakes more than doubled from 2022 to Q1 2023. This proportion jumped from 0.2% to 2.6% in the U.S.[2]

At the current rate of growth, damage from cyberattacks will amount to about $10.5 trillion annually by 2025—a 300% increase from 2015 levels.[3]

Solutions that Work – The Power of Dynamic Intelligence

What can government agencies that oversee critical data do? A potential solution lies in turning AI systems on themselves to keep AI fraud in check by detecting patterns and anomalies that are often overlooked by humans.

AI technology relies on static data points (i.e., PII, voice, and facial biometrics) that are readily available. While static data remains the same after collection, dynamic data continually changes after it is recorded in order to maintain its integrity. Invoking dynamic identity intelligence can provide the strong and reliable evidence necessary to verify identities to help meet the requirements of government agencies and the people they serve.

Our solutions can help.

LexisNexis® ThreatMetrix® for Government: Provides the fast, digital identity assessment agencies need. It harnesses data intelligence across one of the world's largest, global digital networks.

LexisNexis® BehavioSec®: Leverages superior behavioral biometrics insights to accurately trust genuine users, actively detect threats, provide a seamless experience, and confidently protect agencies and participants.

LexisNexis® RISK SOLUTIONS

For more information visit, scan QR code or call 800.458.9197.

1 https://www.foxnews.com/opinion/government-wildly-unprepared-ai-abused-criminals

2 https://www.businesswire.com/news/home/20230530005194/en/New-North-America-Fraud-Statistics-Forced-Verification-and-AIDeepfake-Cases-Multiply-at-Alarming-Rates

3 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers