No Government Program is Safe

Fraudsters are turning to synthetic and artificial intelligence (AI) for swindling millions of dollars from unsuspecting victims and government agencies. It's never been easier to bypass legacy document authentication and "liveness checks." In fact, it's backfiring 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 extra critical when it comes to preventing nearly perfect identity imposter fraud.

In North America, the proportion of deepfakes more than doubled from 2022 to Q3 2023. The proportion jumped from 0.2% to 2.4% in the U.S.

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.

Government agencies – and the U.S. taxpayer – stand to lose billions, if not trillions of dollars due to fraudsters deploying AI-enabled fraud. Government agencies – and participants – need a way to stay ahead of these new and emerging threats.

The Perfect Storm

Government agencies are incredibly vulnerable. They're tasked with making picture-to-person comparisons on their own – using humans to make risk-based decisions. Many agencies with astonishing ease – seamlessly deceiving systems designed to authenticate connections, identities, and vulnerable physical documents.

A technology ripple in static data points (i.e., files, voices, and social positioning) that are readily available. While static data remains the same after an identity authentication, facial information is the most difficult to maintain its integrity. Involving dynamic-customer intelligence can provide the strong and reliable evidence needed to meet the demands of government agencies and the world at large.

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 or flag a user, provide a more secure and confident experience, and protect agencies and participants.

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

Solutions that Work – The Power of Dynamic Intelligence

What can government agencies do about this critical data? A potential solution lies in leveraging systems of themselves to keep up with fraud by detecting patterns and anomalies that are otherwise overlooked by humans.

It is critical that, as an identity community, we act swiftly and collaboratively to stay ahead of these emerging threats.

Numerous static data points that generate AI-enabled fraud are now available at scale due to recent DMY data breaches. This combination of data and AI technology will materialize as “guaranteed” fake human voices, real driver’s licenses for imposters, and real-time deepfake (a.k.a. identity not present) imposters.

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

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

Fraudsters are turning to synthetic and artificial intelligence (AI) for swindling millions of dollars from unsuspecting victims and government agencies. It's never been easier to bypass legacy document authentication and "liveness checks." In fact, it's backfiring 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 extra critical when it comes to preventing nearly perfect identity imposter fraud.

In North America, the proportion of deepfakes more than doubled from 2022 to Q3 2023. The proportion jumped from 0.2% to 2.4% in the U.S.

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.

Government agencies – and the U.S. taxpayer – stand to lose billions, if not trillions of dollars due to fraudsters deploying AI-enabled fraud. Government agencies – and participants – need a way to stay ahead of these new and emerging threats.

The Perfect Storm

Government agencies are incredibly vulnerable. They're tasked with making picture-to-person comparisons on their own – using humans to make risk-based decisions. Many agencies with astonishing ease – seamlessly deceiving systems designed to authenticate connections, identities, and vulnerable physical documents.

A technology ripple in static data points (i.e., files, voices, and social positioning) that are readily available. While static data remains the same after an identity authentication, facial information is the most difficult to maintain its integrity. Involving dynamic-customer intelligence can provide the strong and reliable evidence needed to meet the demands of government agencies and the world at large.

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 or flag a user, provide a more secure and confident experience, and protect agencies and participants.

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