The Perfect Storm of Escalating Artificial Intelligence (AI), ChatGPT, Deepfake Threats Facing Government Agencies

How to Navigate Threats Successfully

Fraudsters are turning to generative 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.**

Increasingly sophisticated and targeted exploits are exposing exponential amounts of personal identity information to the dark web marketplace. The result is a nearly perfect identity imposter fraud. Verification based on static identity attribute assessment and vulnerable physical documents is no longer effective in exposing identity fraud. This is exposing **both the agencies and individuals to identity theft as well as benefits and services compromise.**

- Valuable identity attributes that fraudster use for generative AI **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 drivers licenses for imposters, and real-time deepfake (a.k.a. identity not present) impersonation.**
- AI and deepfakes can bypass Identity Assurance Level 2 (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 in video-based authentication sessions.**
- Generative AI created identities is challenging **trusted "referees" who are tasked with making picture-to-person comparisons on their own – using humans to make risk-based decisions.**

Means, Motive, Opportunity = Crime 3.0

Means
Generative AI, Deepfakes

- Synthetic identities identical to the profiles of legitimate beneficiaries
- AI-fabricated medical claims
- AI-generated tax returns designed to exploit loopholes and maximize refunds
- Fabricated businesses with complete identities

Motive
Government benefits

Opportunity
Online, easy-to-access benefit programs

The Real Impact of Escalating Threat Vectors

Deepfakes Now Real-Time: Deepfake video will pass live video identity proofing.[1]

VCaaS: (Voice Cloning-as-a-Service): can now pass voice-print authentication.[2]

Generative AI Cyberthreats: Phishing emails are "cleaned up" and becoming more convincing to recipient/victim.[3]

'WormGPT' now writing malicious code, speeding up release of malware/hostile scripts to steal credentials.[4]

1.4 billion records exposed in the U.S. between 2010 and 2020.[5]

68% increase in data compromises in 2021.[6]

40% more supply chain attacks than malware attacks in 2022.[7]

$90M stolen using a silicone face mask on Skype.[8]

AI could generate synthetic identities matching the profile of legitimate Social Security benefit beneficiaries, directing millions of dollars away from deserving recipients.[9]

Medicare and Medicaid: AI could fabricate seemingly legitimate medical claims, leading to the loss of billions of dollars.[10]

Advanced AI algorithms could create complex tax returns designed to exploit loopholes and maximize fraudulent refunds.[11]

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.[12]

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.[13]

With the introduction of **each new security technology,** fraudsters have **quickly established work arounds.**

Implementing a **multi-pronged approach** to identity proofing is key:

- Bot detection and mitigation
- Behavioral biometrics
- Identity verification
- Multi-factor authentication
- Support for document authentication and liveness checks

Remedy Risk, Optimize Effectiveness

Establish a smart, secure perimeter around your benefits.

Recommendations:

- **Always monitor existing recipient population for changes and evaluate new risk.**
- **Ensure identity workflow is configurable and adaptive to identify and stop emerging fraud tactics.**

Invest in identity solutions that are:

- Nimble
- Scalable
- Adaptable

Invest in Tomorrow – Today

Work with vendors that actively utilize data science to inform decisions.

Prepare and Plan for the Unknown

Stop AI-Enabled Fraud with Dynamic Intelligence

Expose Login Account Takeover (ATO) Risks:

- Stolen/breached credentials
- Compromised device (malware, RATs) used for Short Message Service (SMS) interception
- Social engineering (user being influenced, soon to be deepfake)
- Session hijack or transaction insertion
- Device location, manipulation, other high risks common to VCaaS AI threat

Solutions:

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® Emailage®: Exposes risk at new account opening by identifying prior fraud or fraud-related risk.

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

Expose Phone/Mobile Device ATO Risks:

- Forwarded phone
- Subscriber Identity Module (SIM) swap for SMS interception
- Stolen device or device being used by different identity
- Carrier reported identity associated with phone number exposes stolen/compromised device

Solution:

LexisNexis® Phone Finder: Combines phone content with the industry's largest repository of identity information to deliver connaections between phones and identities.

Expose Fake ID, Deepfake ID Image, or Deepfake Live Video:

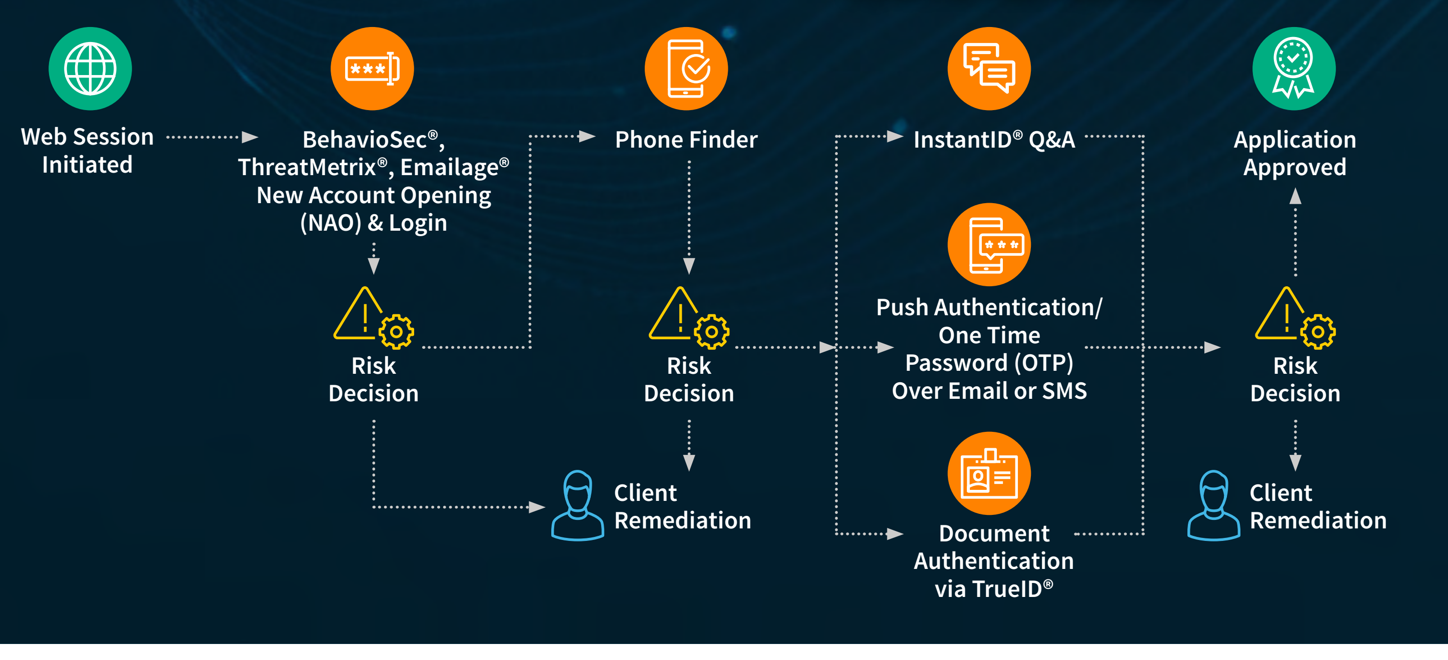
- Image manipulation or insertion detection during ID scan
- Video insertion detection during liveness check
- Generative AI created Fake ID

Solutions:

LexisNexis® InstantID® Q&A: Reduce identity fraud by authenticating citizen identities in real-time with knowledge-based authentication.

LexisNexis® One Time Password: An authentication method that strengthens authentication during high-risk transactions.

LexisNexis® TrueID®: Instantly authenticate identity documents in face-to-face transactions, fight fraud and improve the citizen experience.



It takes a network to break a network. Establishing a centralized risk responsive defense strategy catches emerging threats before they drive significant loss and break privacy protections. Thinking outside the box drives agility and understanding of identity across channels. LexisNexis® Risk Solutions can help your agency deploy multi-dimensional intelligence and risk frameworks proactively so you can outsmart threats before they start.

LexisNexis® RISK SOLUTIONS

For more information visit, scan QR code or call 1-888-216-3544.

1. https://blogs.gartner.com/akif-khan/will-deepfakes-kill-identity-verification/
2. https://www.infosecurity-magazine.com/news/experts-warn-of-voice/
3. https://www.egress.com/blog/phishing/will-hackers-use-ai-chatbots-to-craft-better-phishing-emails
4. https://decrypt.co/148963/wormgpt-chatgpt-phishing-attack-malicious-malware
5. https://www.idtheftcenter.org/publication/2022-trends-in-identity-report/
6. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/
7. https://quanexus.com/supply-chain-compromise/#:~:text=In%202022%20there%20were%2040,used%20in%20manufacturing%20and%20distribution.
8. https://www.bbc.com/news/world-europe-48510027
9. https://www.foxnews.com/opinion/government-wildly-unprepared-ai-abused-criminals
10. https://www.foxnews.com/opinion/government-wildly-unprepared-ai-abused-criminals
11. https://www.foxnews.com/opinion/government-wildly-unprepared-ai-abused-criminals
12. https://www.businesswire.com/news/home/20230530005194/en/New-North-America-Fraud-Statistics-Forced-Verification-and-AIDeepfake-Cases-Multiply-at-Alarming-Rates
13. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers | McKinsey

About LexisNexis Risk Solutions
LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

The LexisNexis ThreatMetrix for Government, BehavioSec, Emailage, Phone Finder, InstantID Q&A, One Time Password, and TrueID services are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and do not constitute "consumer reports," as that term is defined in the FCRA. Accordingly, the LexisNexis ThreatMetrix for Government, BehavioSec, Emailage, Phone Finder, InstantID Q&A, One Time Password, and TrueID services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment, or another purpose in connection with which a consumer report may be used under the FCRA. Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified.