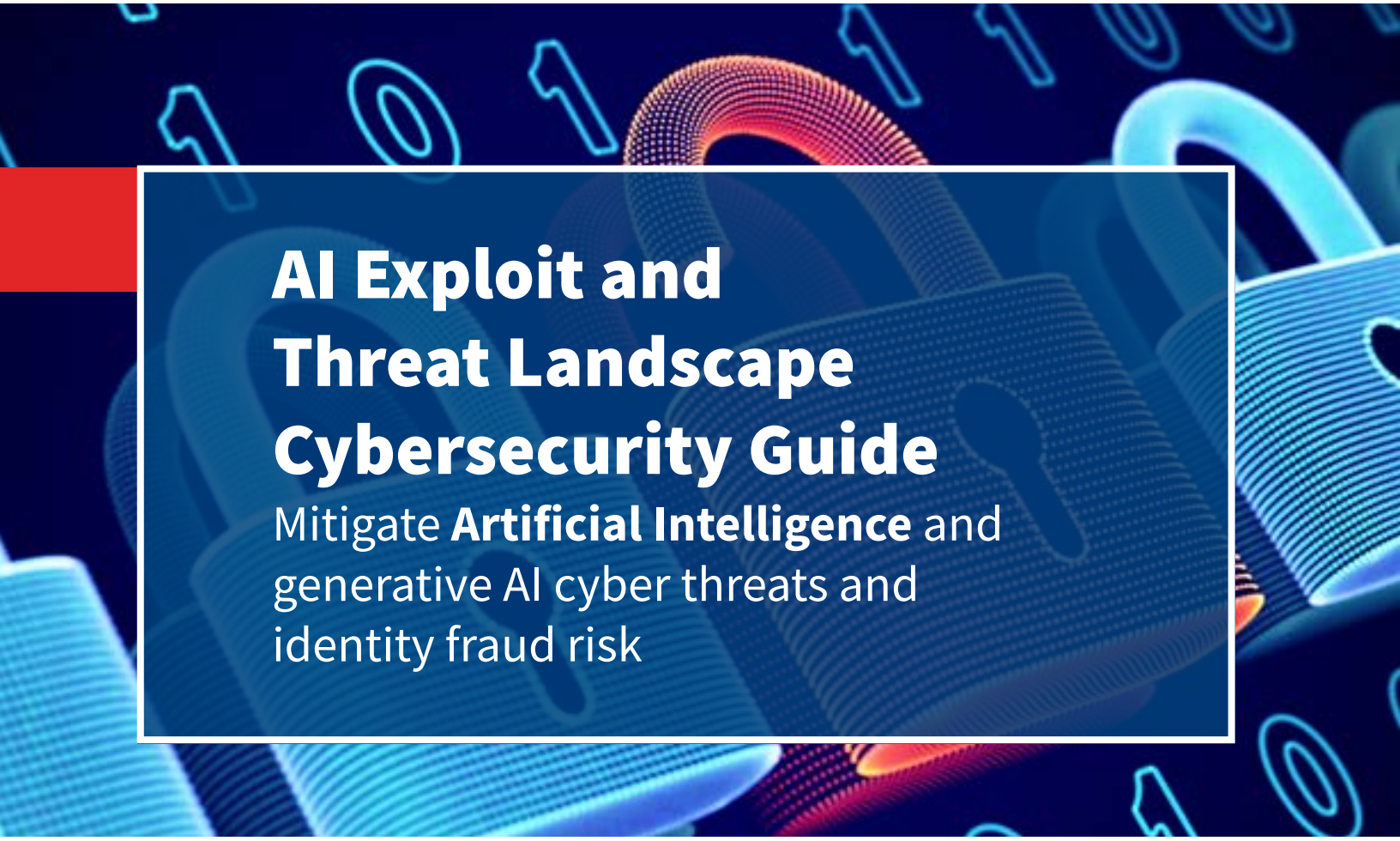
LexisNexis®
RISK SOLUTIONS



AI Exploit and Threat Landscape Cybersecurity Guide

Mitigate **Artificial Intelligence** and generative AI cyber threats and identity fraud risk

Contents

Don’t be fooled — cyber attacks and identity fraud come in many forms

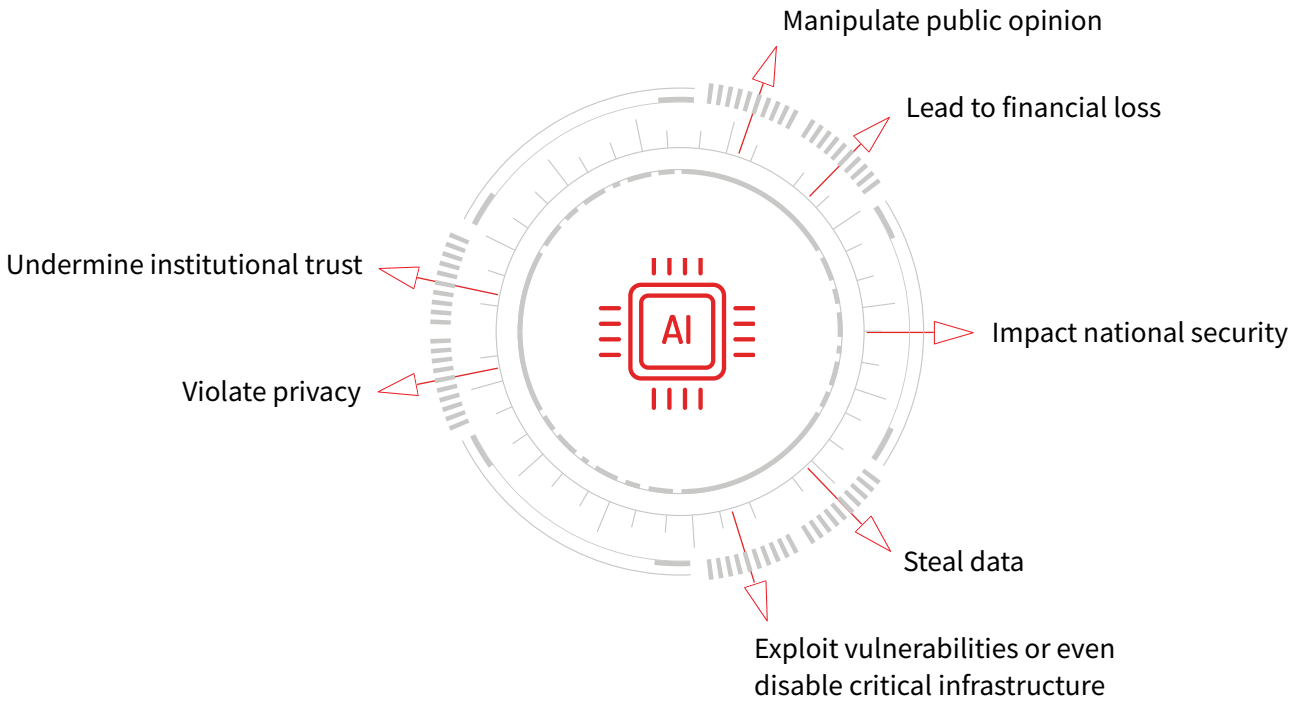
In a world of Deepfakes and voice cloning, how can your agency be sure people are who they say they are? If you are not up to speed with the latest exploits and threats enabled by Artificial Intelligence (AI) and generative AI (Gen AI), your organization could be vulnerable to identity fraud and at risk of a major cyber breach.

In this guide, we explore the latest AI and Gen AI exploits and threats. We also reveal the methods your agency can use to expose various types of fraud and the tools you can use to mitigate the risk.

AI exploits and new threats

Variants of AI models are designed for malicious purposes and facilitate cybercriminal activities. These tools can create highly convincing phishing emails, generate malicious code, and conduct other illegal activities that put your agency at risk.

For example, they can:



Malicious AI models

WormGPT

- Born in March 2021, WormGPT went live in June 2021
- Based on the older GPT-J language model, this tool was allegedly trained with sources that included malware-related data
- It was tested to create well-crafted phishing emails
- As a tool for writing malware, it was initially not very successful

FraudGPT

- Appearing in July 2023, FraudGPT is considered “WormGPT 2.0”
- The tool has been used to craft highly targeted spear-phishing emails, create cracking tools, and develop undetectable malware
- It identifies leaks and vulnerabilities
- A variant, LoveGPT, has been used in romance scams

Types of attacks

AI-generated spear-phishing emails

- These emails are highly personalized to specific individuals within an organization
- Senders may pose as a member of your IT team or another authority figure
- They can be created in seconds and scaled rapidly

AI-generated cyber attacks

- Automated attacks can identify and exploit system vulnerabilities at high speed and with a lower barrier to entry for non-expert attackers
- Detecting these attacks and responding to them is challenging
- They can be created in less than 24 hours and scaled rapidly

Generative Artificial Intelligence (Gen AI) and identity threats

Malicious AI can also be used for sophisticated forms of identity fraud using Deepfake videos, voice-cloned audio clips, high-precision fake IDs, and other documents. For agencies, identity fraud brings risk of financial losses, misinformation spread, and undermining of public trust and legal issues.

Generated Deepfake video and audio files

Deepfake AI is a type of artificial intelligence used to create convincing audio and video clips that can be used to:

- Spread false information that appears to come from a trusted source
- Generate political propaganda and meddle in elections
- Conduct video meeting business fraud

Generated images

Automated image generation tools can create human face images or alter existing photos that can be used to:

- Accelerate the creation of fake ID documents
- Develop fake news or propaganda images
- Build fraudulent advertising
- Execute scams

Generated text

AI text generation tools like DarkBARD can produce written content, imitating human language patterns and styles, that can be used to:

- Create exceptionally convincing phishing and smishing email content
- Develop sophisticated chatbots on social networks
- Formulate false legal citations

Generated audio

AI text-to-speech (AI TTS) converts written text into lifelike spoken words using AI algorithms and voice synthesis technology. Trained on recordings of someone's voice, it can be used for:

- Voice cloning as-a-service (VCaaS)
- Voice authentication compromise
- Voice scams, especially with seniors
- Business fraud, such as wire transfer calls

Synthesized identity data

Gen AI can be used to create synthetic identity data for fictitious identities. By combining fake and real data, or using real data from a range of different sources, a synthetic identity can be used to:

- Open bank accounts, obtain loans, or apply for credit cards with fake and inflated credit scores, harming financial institutions and increasing loan defaults

AI automated fraud

AI can be used to enhance various hacking activities, including:

- Automated vulnerability scanning
- Intelligent detection and exploitation of system weaknesses
- Development of adaptive malware
- Identity and credential theft, or account takeover

How to mitigate the risk of cyber attacks and identity fraud

Fortunately, there are things your agency can do to mitigate the risk. By exposing various types of fraud, you can identify vulnerabilities and implement solutions.

Expose Deepfakes and generated image fraud

Use analysis

- Analyze the temporal sequence between frames to discriminate between real and fake videos

Recognize device risk

- Uncover evidence of device risk and compromise
- Perform velocity checks for local and global customers and constituents
- Conduct anomaly checks for multiple identities per device
- Use behavioral biometrics to expose idle device/no sensor data and sophisticated bot activity
- Test emerging threats using machine learning and learning policies

Expose text generation and audio generation fraud

Mitigate suspicious text message scams

- Messages often trick users into exposing login credentials
- Identity assurance workflows will expose this credential theft
- Text message scams can socially engineer users into money transfers to online criminals
- Behavioral Biometrics can expose user influence behavior and flag or block as a 'fraud detected'

Mitigate voice cloning scams

- Users fall victim to authorizing account access for online criminals who sound like someone they trust
- Identity assurance workflows expose credential theft/misuse
- Voice cloning scams can socially engineer users into sending money to "friends/family" who are imposters
- Behavioral Biometrics can expose user influence behavior and flag or block as a 'fraud detected'

Expose synthetic data

- Search for the person online using people search services
- Look for the following red flags:
  - Brief existence of identity, often less than one year
  - Lack of any family connections
  - Fake ID's, including scans, optical character recognition (OCR), and identity-proof lookup
- Combine behavioral risk assessment during the online session to further expose risk associated with Synthetic Identity

What does your future hold?

In the volatile cybercrime landscape, AI and Gen AI are enabling threat actors to scale exploits and threats at an unprecedented pace. To thwart these threats, existing tools are available, with more being released and upgraded to help organizations identify fraudulent activity, resolve vulnerabilities, and verify people's identities.

Outsmart AI and Generative AI threats with confidence

LexisNexis® Risk Solutions can help agencies face these evolving threats. Our fraud detection, prevention, and analytics solutions are specifically designed for government.

Detection: Rely on broad, diverse data sets — aggregated and resolved down to the individual or entity with our proprietary LexID® linking technology — to see beyond limited encounters and isolated data.

Prevention: Defend your agency against the full range of fraud threats and gain actionable insights that enable you to more quickly spot and prevent outliers or emerging patterns.

Analytics: Leverage automation to score risks and prioritize investigative efforts, so you can focus on the largest incidents or those where you're most likely to successfully recoup improper payments.

Experience the Power of LexisNexis EssentialID™

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 EssentialID™ can help your agency deploy multi-dimensional intelligence and risk frameworks proactively so you can outsmart threats before they start.

LexisNexis EssentialID™ Solves Real AI and Cyber Threat Challenges

Login Account Takeover (ATO) Risks:

- Stolen/breached credentials.
- Compromised devices (malware, Remote Access Trojans (RATs)) used for Short Meddage 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.

LexisNexis EssentialID™

- Complete fast, precise, and timely digital identity assessments by harnessing data intelligence across one of the largest, most secure global digital networks.
- Uncover risk during new account opening by leveraging our industry wide knowledge of prior fraud or fraud-related risk.
- Fortify your identity management workflow with superior behavioral biometric insights to identify and trust genuine users while providing a seamless friction-appropriate experience for your constituents.

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

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

- Reduce identity fraud by authenticating constituents in real-time with knowledge-based authentication.
- Gain strengthened authentication for high-risk transactions leveraging award-winning device and behavioral technology and intelligence.
- Instantly authenticate identity documents in face-to-face transactions, fight fraud, and improve the constituent experience.

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.

- Combined phone content and one of the industry's largest repository of identity information delivers connections between phones and identities.

Let's talk

LexisNexis® RISK SOLUTIONS

For more information about fraud detection and prevention contact us at 1-888-216-3544

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.