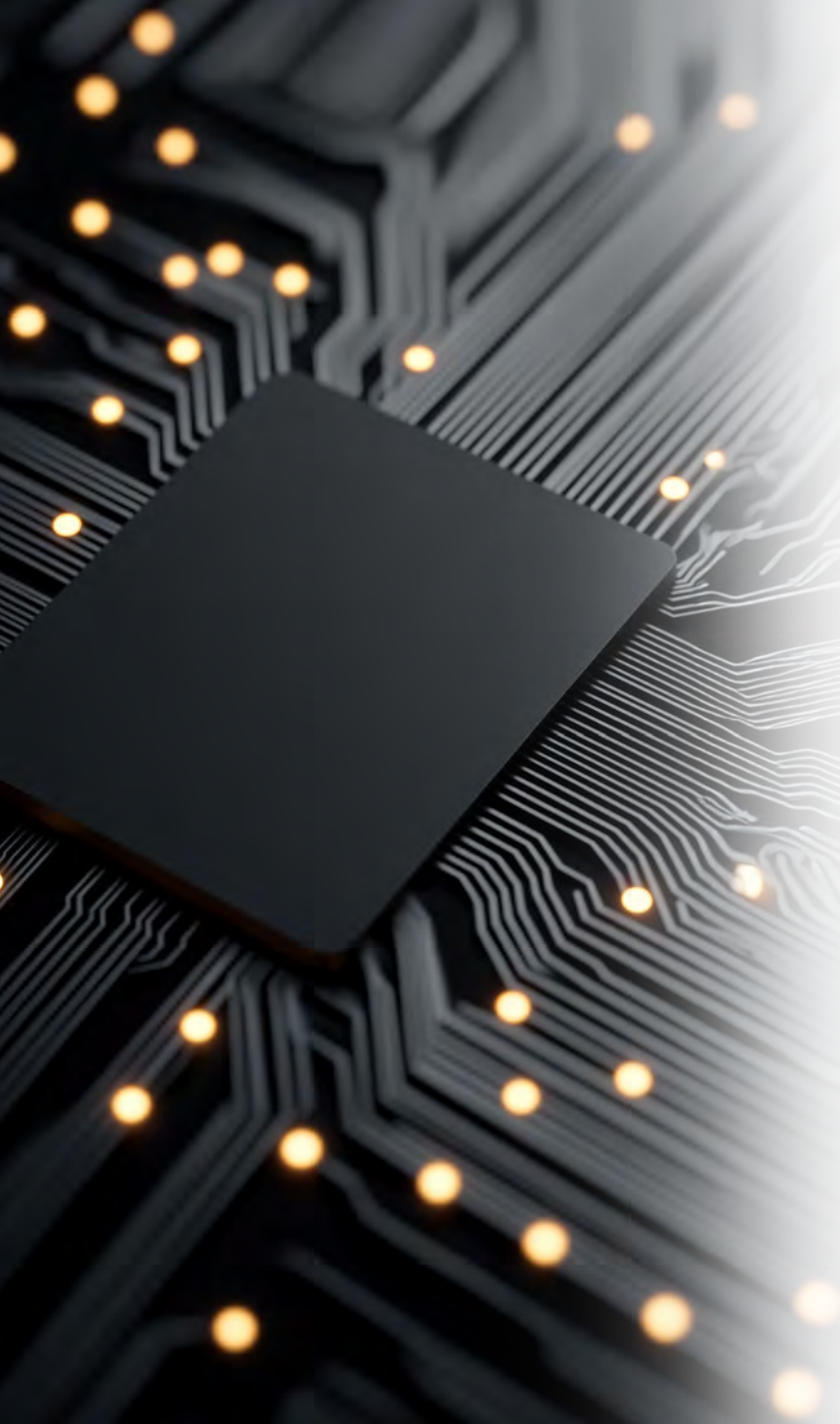
Unmask Deepfakes and Forged Documents with the Power of AI

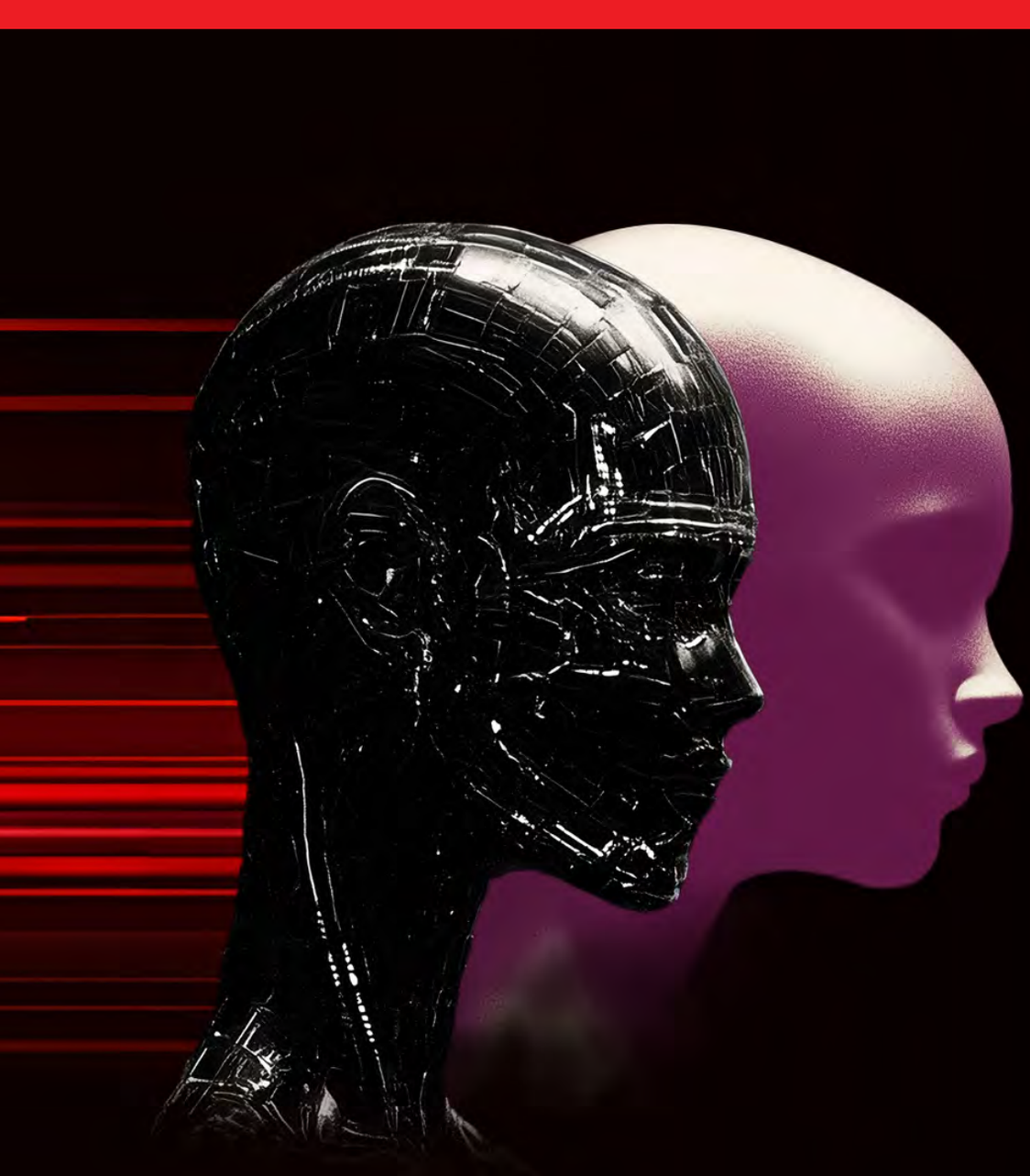
Threat actors are scaling their attacks with generative AI.
Learn how to stay ahead with AI-powered solutions,
while providing a smooth user experience built on digital trust.

Get Started

LexisNexis®
RISK SOLUTIONS



Contents



The Rising Complexity of AI-Generated Fraud

As Generative AI Threats Escalate, Businesses Struggle to Stay Ahead

Fraudsters are leveraging generative AI to forge identities at scale—using deepfake images, video, audio and falsified documents to bypass traditional security protocols. These sophisticated schemes can strike at every stage: from account opening to high-value transactions and re-authentication—posing a growing threat to businesses around the world.

When combined with emulators and tools that manipulate device and session metadata, bad actors can infiltrate systems, steal sensitive data and drain assets across the global economy.

To make it more severe, the rise of low-cost, easily accessible generative AI tooling accelerates this trend—enabling criminals to launch **faster, more convincing attacks with unprecedented reach and scale.**

AI-Generated Fraud Is Hitting its Stride

$40 billion

in generative AI–enabled fraud losses are projected in the U.S. by 2027—**more than tripling from $12.3 billion in 2023.**[1]

More than 1 in 3

fraudulent attacks in 2024 involved generative AI—up from fewer than 1 in 5 in 2023.[2]

85%

of identity fraud cases now involve generative AI tools.[3]

Deepfakes Lead to Swarms of Fake Identities

As generative AI tools become more accessible, the barrier to entry has dropped. Almost anyone can find low-cost, low-risk tools through a simple search—no need for dark web access or expensive fake IDs.

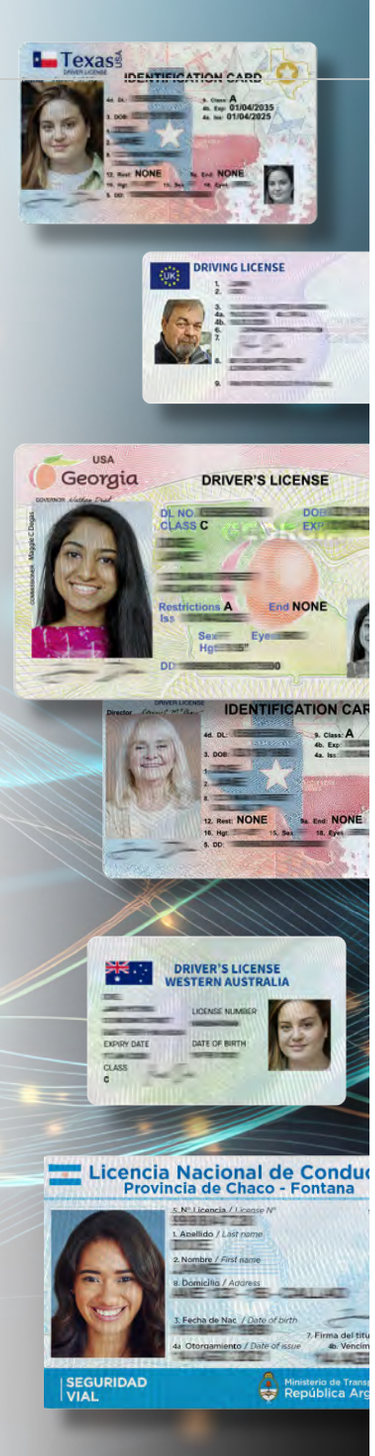
But it's not just opportunistic individuals taking advantage. Fraud today is also a coordinated effort—carried out by well-funded, highly sophisticated networks that actively collaborate and share information to increase their success rates.

Stolen personally identifiable information (PII) from large-scale data breaches is being fed into generative AI tools to create highly convincing fake identity documents at scale. Armed with this data, bad actors can easily create synthetic identities or forge realistic counterfeit documents—making it increasingly difficult for businesses to detect fraud and verify consumers using traditional methods.

To stay ahead, businesses need advanced tools that can verify the authenticity of identities at scale—faster and more accurately than fraudsters can manipulate them.

The answer?

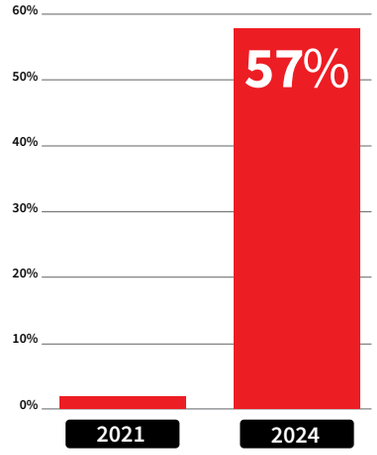
Outsmarting AI with AI.



Forged Documents Are Increasingly AI-Generated[4]

In 2021, virtually no forged documents were generated by AI.

In 2024, AI-generated forgeries were involved in 57% of attacks



It Takes Advanced AI to Fight 'Bad' AI

To combat AI-generated deepfakes and forged documents, businesses must meet the challenge head-on—by utilizing the power of AI 'for the good'. This means adopting scalable, adaptable solutions that leverage the latest AI innovations to defend against emerging fraud tactics.

AI-powered detection models can process massive volumes of data at high speed, continuously learning and evolving to identify new forgery techniques. These specialized systems are trained to spot subtle, often imperceptible, signs of manipulation that humans cannot spot—making them essential in the fight against generative AI-driven fraud.

A recent study revealed that people correctly spot deepfakes **only 20%** of the time, highlighting the technology's rapid advancement.[5]

Can You Spot The Fakes?

Some of these images are real people, but others are AI-generated deepfakes. Without AI, detection by the human eye is near impossible.

Can you tell the difference? **Click each one to see if you're right.**

Real photos are licensed from the iStock stock photo agency. Deepfake photos were created by feeding descriptive prompts into the generative AI service Midjourney.

AI-Driven Defense Against Deepfakes to Fuel Trust in Identities

Meet the Future of Document Authentication and Biometric Verification through the Power of AI

IDVerse®, part of LexisNexis® Risk Solutions, harnesses the power of AI to help businesses seamlessly authenticate end users while disrupting deepfakes and forged documents from infiltrating their systems—quickly, more accurately and at scale.

Whether a user is opening a new account, re-authenticating after periods of inactivity or making high-value transactions, the solution combines proprietary AI models with advanced face-matching technology to automate ID document authentication and verify identities with precision—helping ensure businesses can keep bad actors out with high confidence.

An AI-first approach

At the core of IDVerse® are proprietary AI models and a deep neural network that have surpassed human capabilities in fraud detection. Unlike rule-based systems, the IDVerse solution's self-learning technology trains on new ID documents within hours—eliminating the need for endless templates—helping businesses stay ahead of new threats as they surface.

A Deep Neural Network

The IDVerse solution's deep learning models and anomaly detection algorithms instantly differentiate between real and AI-generated images or videos by finding inconsistencies or artifacts left behind by AI-generated fraud.

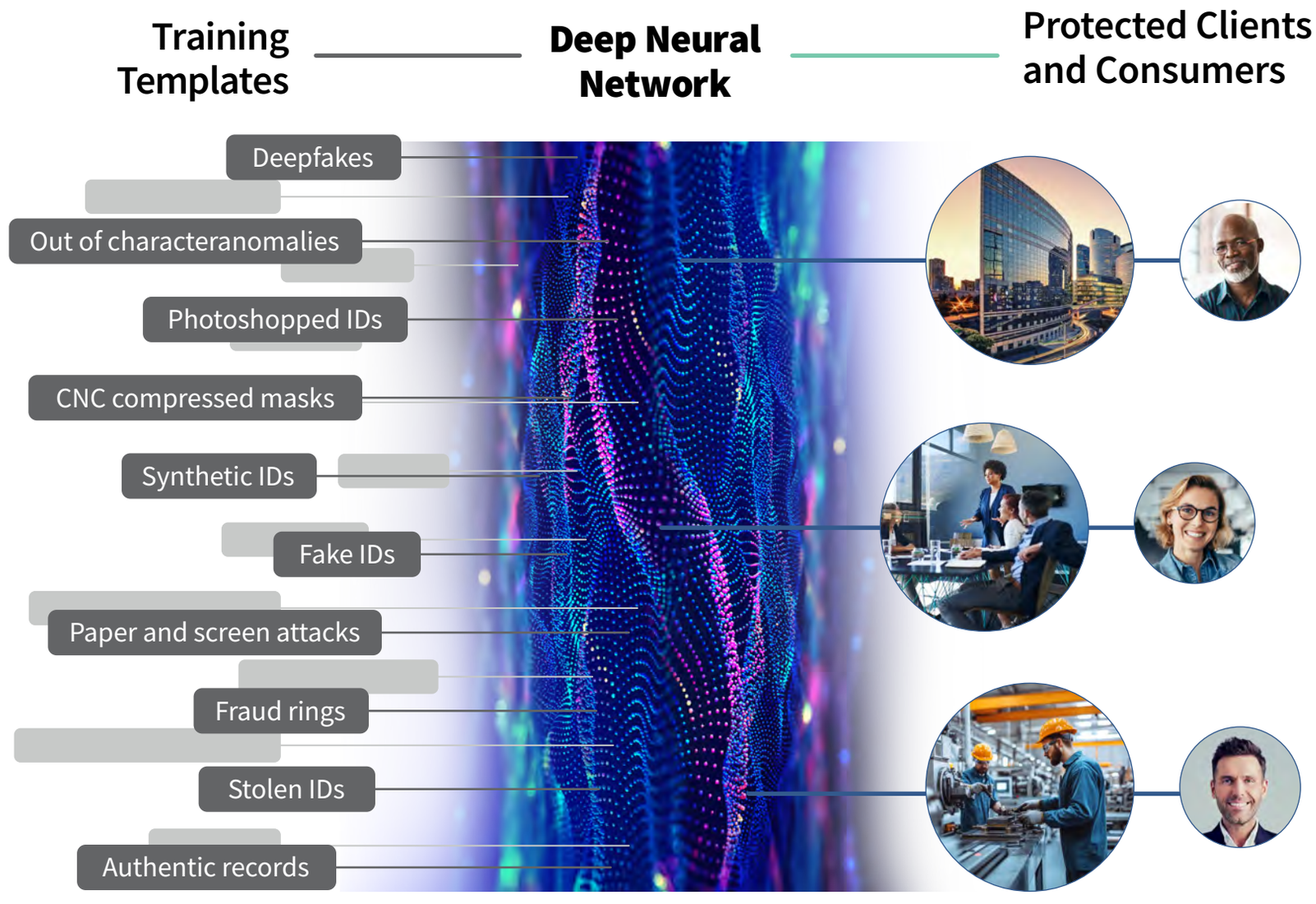
The deep neural network has been trained to replicate the intelligence of countless fraud experts, learning how to analyze the metadata of images and videos, such as the format, compression and noise distribution, with digital forensic techniques that lead to greater depth and accuracy.

The network is trained daily on new fraud types, ensuring the utmost protection for clients and customers.

Adversarial training: Models learn to flag AI-generated fraud by being exposed to the latest examples.

Model combinations: Combining visual and temporal models improves detection by identifying mismatched event timings.

Cross-referencing databases: Checking against authentic records helps spot discrepancies, especially in document authentication.



The Four Engines

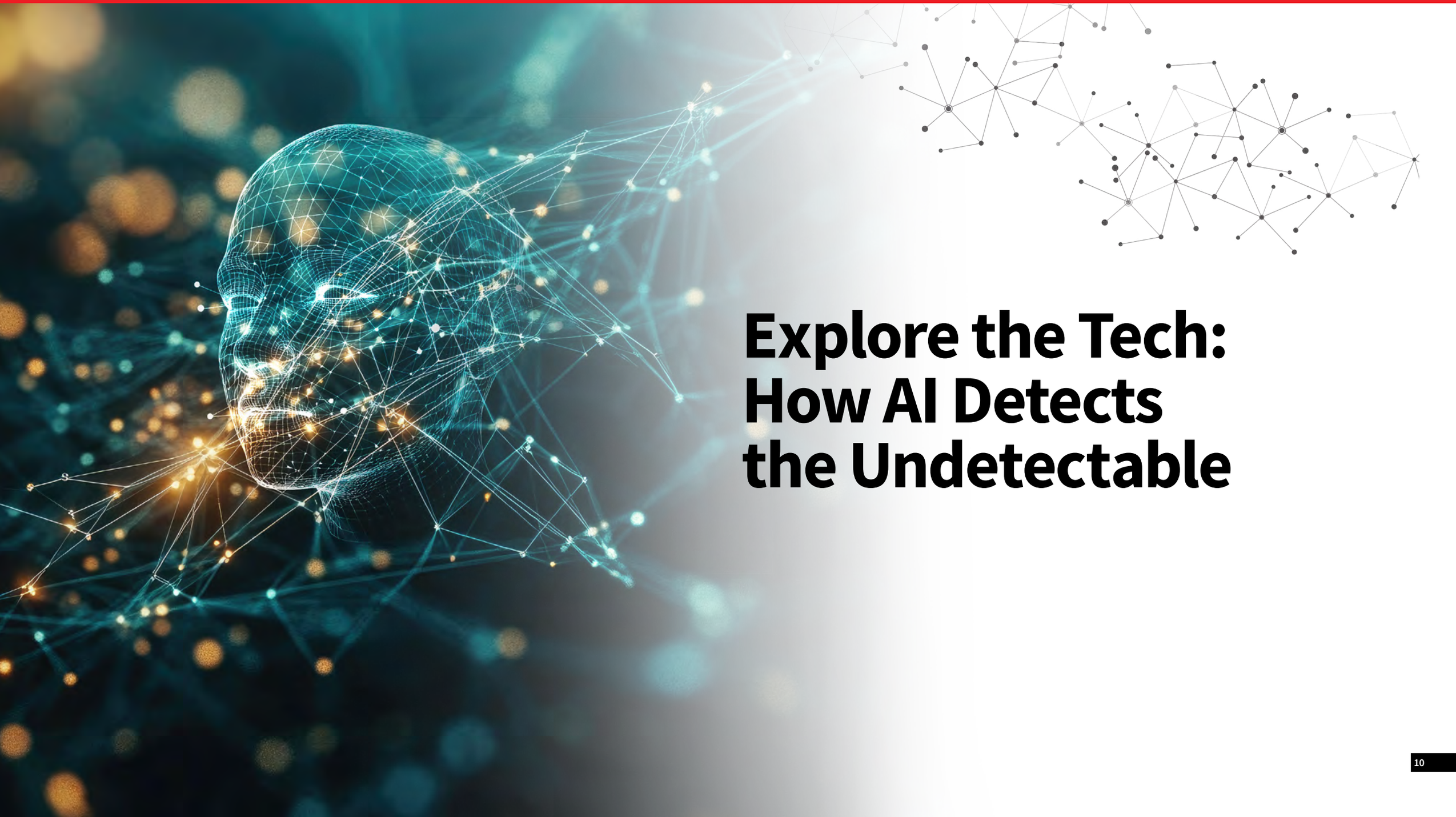
Through four core engines, IDVerse performs hundreds of real-time checks in a matter of seconds, analyzing security features, document structure and image integrity to detect authenticity. Advanced biometric verification helps ensure liveness and matches faces to document photos, preventing deepfakes and forgeries at scale. All these engines work together to prove a person is who they say they are with unprecedented accuracy.

Click on each engine to learn more about how it works:

Continuously trained to keep up to date with the latest technologies and document types

- Optical Character Recognition (OCR)
- Document Fraud Analysis
- Liveness Detection
- Face Matching

Advanced OCR technology and natural language processing automatically extract personal data from government-issued IDs, **capable of covering up to 16,000 document types across 220+ countries and territories and 140+ languages and typesets.** It achieves 98.5% accuracy for **human-readable data and 99.98% accuracy for machine-readable text.**



Explore the Tech: How AI Detects the Undetectable

Discrepancies that AI Helps Uncover

These advanced AI models analyze signs of fraud and ID tampering, helping to answer questions like:

1. Is the ID real or manipulated?
2. Are there signs of ID tampering?
3. Does the photo make sense from a real space and time perspective?
4. Is it a human or a deepfake?
5. Is it a live selfie, or a photo of a photo/video?
6. Are there signs of a spoof attack or mask?
7. Are there micro muscle movements and blood flow?
8. Is this interaction happening in real time?
9. Does it match the face on the ID?

Hover over each image to learn how it works.

A Deeper Look at ID Document Analysis

IDVerse is capable of verifying up to 16,000 documents across 220+ countries and territories in 140+ languages and typesets. The most impressive part, though, is that through natural language processing (NLP) and directional analysis, hundreds of data fields and security aspects are checked to help detect tampering in the ID and validate its authenticity. This automated process happens more reliably, more efficiently and much faster than human teams can accomplish.

Click on any of the magnifying glasses to see a few of the things IDVerse checks for.

IDVERSE LOOKS FOR:

Subtle changes in shapes, symbols, alignments, typography and context

Step Into the Consumer's Shoes

With IDVerse, authentication and verification are quick and intuitive for end users, giving them a yes or no answer within seconds, not minutes. The user interface is fully branded to your organization, so end users won't know they're accessing a third-party environment.

Legitimate Users Experience a Quick and Secure Interaction…

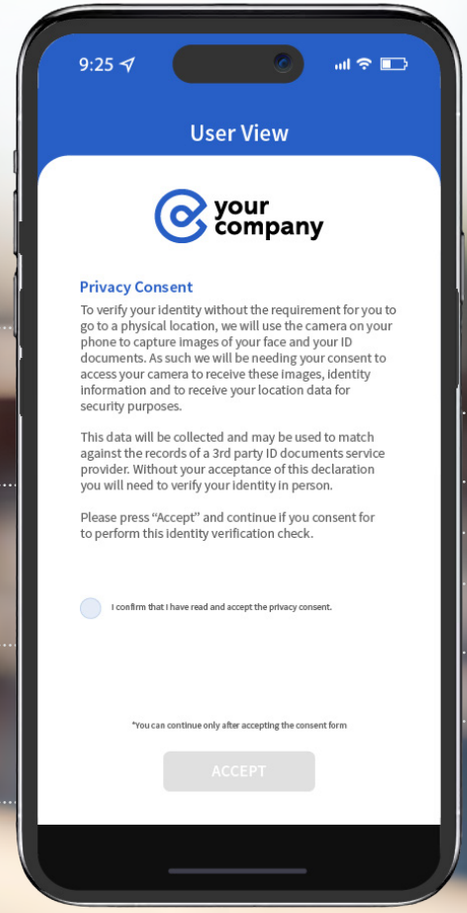
Click on each to learn how it works

STEP 1 — A user interaction triggers the verification process

STEP 2 — User captures an image of their photo ID

STEP 3 — User takes a selfie

STEP 4 — Verification is complete



…While IDVerse Automatically Defends Against Deepfakes and Identity Fraud

This can happen through SMS, QR code, API, in-app or call center. After giving consent, the process begins.

Conclusion: The Powerful, Responsible, Self-Learning Solution Modern Businesses Need

Disrupt Large-Scale Identity Fraud

Powered by propriety AI and a deep neural network, the IDVerse solution learns and adapts to emerging fraud tactics, ensuring businesses stay ahead in an evolving landscape. The advanced technology helps organizations verify legitimate users wherever they are, using just a smartphone.

Businesses can onboard and authenticate consumers securely and quickly, enabling them to scale and grow efficiently. Consumers benefit from a smooth, seamless, and fully branded interaction with quick access to products and services.

With a user-friendly approach, businesses can decrease application times, catch fraud attempts early, save money, remain compliant with regulations and reduce the potential for reputational damage.

What Sets IDVerse Apart?

- **Proprietary End-to-End Technology**
- **Global Coverage and Language Support**
- **Industry-Leading Accuracy and Fraud Detection**
- **Fully Automated**
- **Fast, Seamless Onboarding**
- **Advanced Liveness Detection with Managed Capture**
- **Customizable and Flexible Integration**
- **Contextual Learning with AI**
- **Regulatory Compliance and Security**
- **Scalability**

Fully in-house, 100% proprietary tech stack with quality control at every step, ensuring reliability and security.

Securing Today, Innovating for Tomorrow with Responsible AI

Our AI models are explainable, transparent and deliver results with full reasoning, so businesses can reliably understand why a user is flagged for further review or automatically accepted. We strive to be as straightforward as possible, so there's no room left for guesswork.

Our Commitment to Responsible AI

- Understand the real-world impact
- Respect privacy & champion data governance
- Avoid exclusion and bias
- Make everything explainable and accountable

Download the Responsible AI whitepaper