2025 Deepfake Detection Market Report & Buyer's Guide

by Biometric Update and Goode Intelligence

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

© 2025 Biometrics Research Group, Inc.

2025 Deepfake Detection Market Report & Buyer's Guide

Deepfakes were thrust into the popular awareness over the past couple of years through a combination of celebrity victims, attempted elections fraud and brazen high-tech heists of eye-popping sums. The cost of falling prey to deepfakes depends on the scenario, but for businesses in general it is high and rising. Lawmakers are taking note, and the public is worried.

Deepfake detection technology has proven capable of detecting and thwarting many different kinds of fraud attacks carried out with AI-generated images or voices impersonating real people, or in some cases completely invented ones. In some cases, it uses biometrics and other types of content analysis to identify synthetic content. In other cases, it utilizes metadata analysis or device signals to detect signs of the delivery of spoofed faces or voices. Businesses have discovered active financial accounts opened with deepfakes through investigations with these technologies in some cases, and in others prevented account opening fraud by catching injection attacks intended to deliver deepfakes.

The market report explains what deepfakes and deepfake detection are and how they work, and the types of fraud attacks deepfake are used for. It explores the state of the art, including the developing standards landscape, the testing that is possible, and the competitions that have helped fuel innovations in deepfake protection. The different drivers, sectors and applications that make up the market are described, and forecasts are provided for transactions involving voice and face deepfake detection and the revenues they generate.

The buyer's guide section defines common terms and shares advice on what to look for in a technology supplier. It provides case studies of real-world applications of deepfake detection technology, profiles prominent vendors, and presents a directory of dozens of options for businesses that need to protect themselves from deepfake fraud.

About Biometric Update and Goode Intelligence

This study has been created by a partnership bringing together Biometric Update and Goode Intelligence to produce analytical market reports stakeholders can use to make informed strategy, product and technology procurement choices.

Reports produced by the partnership are based on analysis of recent transactions and trends in the biometrics market, reviews of the regulatory, standards-development and competitive landscapes, and feedback from key insiders in each given area of focus.

Biometric Update is the world's leading source for daily news, opinion and insight into biometrics and digital identity.

Goode Intelligence is the world's leading independent biometrics market analyst and consulting firm, providing quality advice to global decision makers in business and technology.

Executive Summary

The 2025 Deepfake Detection Market Report from *Biometric Update* and Goode Intelligence addresses one of the most disruptive and impactful changes happening in the digital world.

Deepfakes have dramatically undermined trust in digital media and digital identity verification, with profound implications for fraud and other social ills. Empowered by deepfakes, cybercriminals are inventing new kinds of attacks and deploying traditional ones at previously-unseen scale.

The report begins by explaining what deepfakes and deepfake detection mean. It goes on to outline the cause and extent of the problem, the types of deepfake attacks observed so far and how to defend against them.

Deepfakes are enabling sophisticated fraud attacks of various types, and both the technology to carry out these attacks and to defend against them are evolving at a remarkably rapid rate, even relative to the generally fast-moving field of biometrics.

Early efforts to formulate international standards around the technology are reviewed, and research efforts to better understand the problem and what kinds of defenses are effective against it are explained to help organizations determine how to protect themselves.

The market analysis section breaks down the most important market drivers, the sectors where deepfake detection is already important, and how deepfakes can impact different parts of the identity life cycle.

The report concludes with forecasts for deepfake detection transactions and revenues over the next three years, divided between voice and face deepfakes. In total, there are expected to be 9.9 billion deepfake checks by 2027, generating nearly $4.95 billion in revenue.

Introduction to Deepfake Detection

Deepfakes are pieces of fake or altered digital media, typically used to impersonate an individual, created using artificial neural networks, deep learning algorithms and other generative AI technologies. What distinguishes them from fake IDs and other existing forms of image manipulation is the ease with which they can be generated digitally, and the resulting ability of bad actors to scale operations.

Deepfakes are the bane of traditional methods for KYC and identity verification. The ability to generate deepfakes in bulk and launch large-scale attacks has transformed the fraud landscape. Realism in deepfakes has improved dramatically; according to UK regulator Ofcom, fewer than one in ten people aged 16 or older say they are confident in their ability to identify a deepfake.

On the financial side, deepfakes have resulted in losses in the millions; in a notorious deepfake attack on a Hong Kong firm, deepfake executives injected into a video feed successfully prompted an employee to transfer $25 million to fraudulent bank accounts.

The story also illustrates the more existential threat that deepfakes present: they are eroding our ability to be certain of what is real, and what has been generated by a deep learning algorithm. To that end, the ability to recognize them has become crucial to the very notion of "Know Your Customer" – in that, first and foremost, you must know your customer is real.

Since the term "deepfake" refers to a category rather than a specific use or technique, deepfake detection likewise refers to a category of tactics, safeguards and technologies designed to identify deepfake media. What unifies the deepfake detection ecosystem is intention: find the fake content to block fraud, child sexual abuse and exploitation, extortion, and other malicious attacks.

Broadly, deepfake detection can be divided into three major streams: video deepfake detection, document or image deepfake detection, and audio deepfake detection. Most visual deepfakes are faces – meaning that deepfake detection is often the art and forensic science of recognizing fake faces. Audio deepfake detection likewise recognizes cloned or synthetic voices.

Since the quality of face deepfakes has advanced to the point that most are unrecognizable to the human eye, firms offering deepfake detection typically use algorithmic software, or deep learning AI, as a basis for their product. As such, for the purposes of this report, we can define deepfake detection as using AI tools to identify synthetic media, particularly faces, created with AI.

The deepfake crisis

As deepfakes have become easier and cheaper to make, freely available through sites such as thispersondoesnotexist.com, the problem has reached crisis levels. The UK government says a projected eight million deepfakes will be shared in 2025, up from 500,000 in 2023. It has declared efforts to mitigate the growing threat from AI-generated deepfakes as an "urgent national priority" and "arguably the greatest challenge of the online age." The potential for misuse and attendant harms continues to grow, resulting in an ongoing erosion of public trust in digital images. According to the 2024 Sensity State of Deepfakes report, the number of available tools for deepfake generation rose to more than 10,000 in 2024.

As the Alan Turing Institute sums up, "it is becoming harder to tell what is real and what is fake." Consequently, in the words of actor Scarlett Johansson – whose voice was faked without her consent after she turned down an offer to provide it to OpenAI's ChatGPT product – "we risk losing a hold on reality."

In response to the surge of deepfakes, the market for deepfake detection has exploded, and governments' calls for innovation are becoming urgent. There are dozens of deepfake detection providers in the market, which are profiled in the buyer's guide accompanying this report, and their ranks are expected to grow over the next five years. According to Deloitte, as deepfakes proliferate and organizations look to verify their digitized assets, "credible content is expected to come at an increased cost for consumers, advertisers, and even creators;" Deloitte's Center for Financial Services projects that generative AI could cause fraud losses of $40 billion in the U.S. by 2027.

How are deepfakes made?

Deepfakes are made using online tools that leverage neural networks, deep learning and other generative AI technologies.

Early deepfakes relied on **Generative Adversarial Networks (GANs)**, a system of competing neural networks that analyze data and train each other to make their outputs more realistic.

The generator model produces a piece of media that it has either sourced from a library of real images

or videos, or generated synthetically. The discriminator model then decides whether the image or video is real or fake. Repeating this exercise trains the generator to produce more realistic content, and improves the discriminator's accuracy.

In deep learning encoding-decoding pairs, or **variational autoencoders (VAEs)**, an encoder trained on face data creates a latent image – something like an abstract object in Plato's Theory of Forms – that can be used to generate a deepfake by a decoder that has also been trained on face data to understand the idea of "face," and can thus translate the latent data into a representation of one. Both encoder and the decoder are recurrent neural networks that train themselves on source data to improve exponentially.

First-order motion models use AI to superimpose fake features onto video (the same tech used in Snapchat filters). They train to learn key features (eyes, lips, teeth, eyebrows) and map biometric data onto a target face to mimic and match movement.

Diffusion models, such as Stable Diffusion, DALL-E 2 and Midjourney, are neural networks trained to progressively "diffuse" samples with random gaussian noise, then reverse that process; imagine a computer that learns how to slowly make a screen turn to white noise, and then turn it back. As such, diffusion models can 'inpaint' missing patches or replace noise in an image with plausible content. Some take text prompts as part of their input. Latent diffusion models use the same concept of latency that occurs in VAEs; they translate images rendered in pixel space to latent space, then perform diffusion at that level.

However, a comprehensive understanding of deep learning is not necessary to create deepfakes. A simple online search will yield dozens of free AI face generator sites, and even major platforms like Canva offer the service. Audio spoofing tools are just as readily available. Moreover, fraud-as-a-service (FaaS) networks enable the outsourcing of deepfake fraud to professional fraudsters for a fee. Deepfakes are literally accessible with a few clicks; according to a research paper from the IEEE, "the accessibility and scalability of deepfake technology allow nearly anyone with device access to create compelling fake videos closely resembling authentic media."

Types of deepfake attacks

Deepfake attacks hijack real identities or create fake ones, to work around traditional methods for identity verification. They leverage a variety of attack vectors and surfaces.

Presentation attacks try to fool a biometric facial authentication system by using fake or manipulated facial images or video. They can be attempted physically (for instance, using a silicon 3D mask) but increasingly rely on synthetic or altered digital imagery. The ability to detect them has historically been called Presentation Attack Detection (PAD), but it has evolved into what is now typically called liveness detection.

Digital injection attacks occur when someone injects malicious code or malware into a computer in order to control output, or when an attacker injects fake biometric data directly into a system's data stream to override it. The most highly publicized deepfake attack thus far – in which fraudsters hijacked a video call with deepfaked executives, resulting in the fraudulent transfer of $25 million dollars – was a video injection attack.

Deepfake face manipulations can be divided into distinct subcategories:

- **Full-face synthesis** involves generating entirely new facial images.
- **Face swaps** use algorithms to replace or superimpose one person's face over another in an image or video.
- **Attribute manipulation** alters features like eye color, hair color or age.
- **Expression swaps**, or re-enactment, transfers one person's facial expressions onto the face of another.
- **Face morphing** is a non-algorithmic technology in which facial images from more than one identity are combined into a hybrid, typically for the purpose of attaining a passport that can be used by multiple people.

Despite the proliferation of face deepfakes, voice is the modality most often spoofed with generative AI. Audio deepfakes can be created with text-to-speech engines that convert text input into a voice based on a reference sample, or speech-to-speech tools that do the same, but with spoken input instead of text so that intonation and cadence can be replicated.

How can deepfakes be detected?

The increasing sophistication of deepfake technology has led to a point at which deepfakes are often undetectable to the human eye (or ear) alone. Detecting deepfakes in images and videos requires analyzing the content to determine if it has been altered or synthesized by AI, by searching for telltale elements, artifacts and inconsistencies in the image, media feed or metadata, and by determining if a video is of a living person through the use of liveness detection. It is fundamentally a binary classification problem, which categorizes an input that is actually real or actually fake as predicted real or predicted fake.

This task typically requires "using AI to fight AI" by deploying neural networks and deep learning algorithms to isolate and analyze individual frames, features and patterns in the biometric data. According to the IEEE, the majority of frame-based deepfake detection techniques rely on identifying the artifacts left by the Generative Adversarial GANs during the generation of the deepfake. But as video deepfakes have evolved, temporal approaches are needed. Effective AI tools can detect visual artifacts, facial expressions or movements, and – in the case of liveness detection – biological and biometric artifacts such as irregularities in heart rate, blood flow or how skin reacts to changes in light.

Some other approaches analyze the color and intensity of individual pixels in an image, complex statistical data from faces (what the IEEE calls the "Pixel and Statistical Feature Approach") or the source characteristics of certain segments of data. Yet another avenue is to use cryptographic metadata – AKA a digital watermark – when creating content.

The development of deepfake detection technology aims to match the rapid pace at which fraudsters and bad actors refine existing tools and develop new ones. As such, new approaches and techniques are being tested constantly as the proliferation of deepfakes accelerates. Challenges and contests drive innovation. However, at present, there are few formal standards or certifications for deepfake detection products.

Standards and testing

In keeping with the dynamic nature of deepfake technology, standards and testing are evolving, but for the moment have not yet been designed to specifically address deep learning-based binary classifier deepfake detection systems.

In 2017, the ISO and IEC jointly set up the ISO/IEC JTC 1/SC 42, a standardisation subcommittee (SC) focusing on AI under ISO/IEC JTC 1, the joint technical committee for standardizing "information technology."

The subcommittee produced the technical report, ISO/IEC TR 24029-1:2021 "Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview," which systematically covers commonly used performance assessment methods and metrics. However, it does not necessarily address deep learning networks, which comprise at least three layers of neural networks.

Most recently, it published ISO/IEC DTS (Draft Technical Specification) 4213 "Information technology – Artificial Intelligence – Assessment of machine learning classification performance" and ISO/IEC TS 25058:2024 "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guidance for quality evaluation of artificial intelligence (AI) systems."

ISO/IEC JTC 1/SC 3714 is a subcommittee that focuses on biometrics-related technology, and as such three of its standards in particular also apply to deepfakes. ISO/IEC 19795-1:2021 "Information technology – Biometric performance testing and reporting – Part 1: Principles and framework" covers general metrics about evaluating biometric systems, including false accept rate (FAR) and false reject rate (FRR).

ISO/IEC 30107-1:2016 "Information technology – Biometric presentation attack detection – Part 1: Framework" defines a general framework for presentation attack detection (PAD) mechanisms. And ISO/IEC 30107-3:2017 "Information technology – Biometric presentation attack detection – Part 3: Testing and reporting" defines several special performance metrics for evaluating PAD mechanisms standardized in the ISO/IEC 30107-1:2016.

The ISO is currently developing an international standard for biometric injection attack detection, ISO/IEC WD 25456, "Information technology – Biometrics – Biometric data injection attack detection." A joint working group (JWG) working on the standard, which is expected to reach a stable draft stage by January 2026, is scheduled to hold four meetings in 2026, with additional online meetings to be held on an as-needed basis.

The ISO/IEC standard-in-progress is based on the CEN/TS 18099:2024 standard and technical specification, published in November 2024 by the European Committee for Standardization (CEN); it provides an overview and guidance on biometric data injection attacks and systems for the detection of injection attack instruments.

Labs have begun issuing certificates of conformity with the CEN/TS 18099 standard for biometric data injection attack detection. In March 2025, CLR Labs' CLR Cert evaluated InfoCert and made it the first company to be confirmed for compliance to both CEN/TS 18099 and the ISO/IEC 19989-3:2020 standard on presentation attack detection, "Information security – Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection."

Deepfake detection challenges

In the absence of formal testing labs for deepfakes, challenge competition datasets and workshops remain one of the data sources that can gauge the effectiveness of platforms that detect deepfake fraud. Several iterations have emerged globally to address the need for standardized evaluation mechanisms.

The DeepFake Detection Challenge (DFDC) dataset launched in 2019, spearheaded by Meta in partnership with industry leaders and academic experts. The DFDC dataset is "the largest currently and publicly available face swap video dataset, with over 120,000 total clips sourced from 3,426 paid actors, featuring eight facial modification algorithms." The full dataset was used in a 2019 Kaggle competition to create new ways of detecting deepfake video. However, the challenge itself resulted in few actionable insights.

The Global Multimedia Deepfake Detection Challenge 2024 is a contest sponsored by the Inclusion Conference on the Bund and digital conglomerate Ant Group. It offers a total prize pool of 1,000,000 Chinese yuan (around US$137,000) to entrants that can innovate, develop and test deepfake detection models that prove effective in a series of real-world scenarios.

DARPA runs the AI Forensics Open Research Challenge Evaluation, an open community research initiative designed to accelerate the development of machine learning models capable of distinguishing synthetic media from authentic content.

The 1M-Deepfakes Detection Challenge 2024 is led by a team of seven researchers from five universities in Australia, the UK and UAE, plus Qualcomm. It aims to advance the development of "next-generation deepfake detection and localization systems." Challenge participants use the AV-Deepfake1M dataset, which is made up of 1 million manipulated videos of more than 2,000 subjects.

Germany's Federal Agency for Jump Innovations (Sprind) is hosting a year-long deepfake Funke, which translates as "spark," to prototype deepfake detection and prevention tools. The twelve selected teams each received up to 350,000 euros for the first stage of the Funke. An evaluation then determines which teams show "the greatest potential for innovation."

The Biometrics Security and Privacy team at Idiap Research Institute and PXL Vision are hosting "the first competition that challenges participants to detect synthetic manipulations" – i.e. injection attacks – in identity documents.

The U.S.-Japan Global Innovation Challenge, sponsored by the Defense Innovation Unit (DIU) and Japan's Ministry of Defense Acquisition, Technology, and Logistics Agency (ATLA), has also recognized deepfake detection firm Reality Defender in its contest for ventures that "advance AI-driven command and control decision-making to strengthen resilience against information warfare."

The UK government has its own Deepfake Detection Challenge, a joint effort between the Home Office, the Department for Science, Innovation and Technology (DSIT), the Alan Turing Institute and the Accelerated Capability Environment (ACE).

Advancing the state of the art

The term "deepfake" was coined in 2017 by a Reddit moderator, who created a forum for users to post deepfake pornography created using photos of celebrities and open source face swap tools. But the deepfake era can realistically be said to have begun in 2014, with the development of Generative Adversarial Networks (GAN), which enabled machines to refine their own learning and output capabilities.

Reality Defender, a firm that focuses exclusively on deepfake detection, notes how deepfake technology has evolved in part due to the contributions and experiments of everyday users. "The open-source deepfake creation tools have been tested and refined by legions of hobbyists, who have utilized these tools for purposes of benign entertainment (memes, swapping out actors' faces in classic movies) and more sinister, appalling goals, like the creation of deepfake pornography."

The firm locates the major surge in this kind of activity in 2017. By the following year, deepfakes were cause for concern among major tech platforms, efforts to regulate deepfakes had begun, and the deepfake detection sector had started to emerge; Reality Defender was founded in 2018, among the first firms to distinctly target deepfakes.

Scale, speed and the narrowing threshold for detection

In many ways, the history of deepfake detection can be mapped against the quality of deepfake images, as improvements in realism and accuracy have driven the need for more sophisticated tools and approaches.

For some, face morphs, created by blending faces, do not qualify as deepfakes. Nonetheless, they were likely among the first digital facial manipulations many people saw, when a then-advanced digital morphing technique was used in the 1991 music video for Michael Jackson's song, "Black or White." The iMARS Project, funded by the European Commission through the Horizon 2020 program, does work focused specifically on "image manipulation attack resolving solutions" for morphing attacks – i.e., algorithms for morphing attack detection (MAD).

Early "true" deepfakes often included artifacts at the pixel level or above – spatial or visual inconsistencies such as differences in noise patterns, or colour contrasts, which are indications of synthetically generated media. Deepfakes produced by GANs leave such digital fingerprints. And, by now, most of us have seen a diffusion-generated image of a person that features telltale hallucinations in the form of extra hands or fingers.

However, refinements in a technology that is always learning mean that the visual hallmarks of generative AI are being eliminated, as the tech enables ever-greater veracity. Several firms have developed GenAI tools they claim are too effective for public release: Microsoft, citing fears about misuse, promised not to unleash VASA-1, which can reportedly generate "hyper-realistic talking face video" from nothing but a single static image, an audio clip and a text script, paving the way for "real-time engagements with lifelike avatars that emulate human conversational behaviors." Many industry experts emphasize that the most sophisticated deepfakes are no longer obvious to the human eye and are good enough to fool some authentication systems. As such, the threshold for effective detection is narrowing.

Data sets

Effective machine learning approaches require training on large, diverse data sets of both real and synthetic facial data.

Researchers from China's Peking University and Tencent's AI research department Youtu Lab have proposed a new benchmark for deepfake detection: the DF40 deepfake detection dataset, comprising 40 distinct deepfake techniques. The dataset includes realistic deepfake data created by popular generation software and methods such as HeyGen, MidJourney, and DeepFaceLab and offers a million-level deepfake data scale for both images and videos.

The Fake Media Forensics Challenge of China Society of Image and Graphics (FMFCC-V) dataset is the first and largest publicly available Asian dataset, containing 38102 deepfake videos and 44290 pristine videos, corresponding to more than 23 million frames.

A 2025 article by researchers out of the University of Bucharest, MBZ University of Artificial Intelligence, Linköping University and University of Central Florida presents "the first large-scale open-set benchmark for multilingual audio-video deepfake detection." The dataset comprises over 250 hours of real and fake videos across eight languages, 60 percent of which is generated. For each language, fake videos are generated with seven distinct deepfake generation models.

Data sets continue to develop, and access will become less of a problem as volume increases.

The rapid pace of deepfake development and evolution

However, pace presents another major challenge. The deepfake detection effort is operating against tech that evolves so fast, keeping up requires constant adaptation and innovation.

According to research from the IEEE, "with new deepfake generation methods emerging, detecting deepfakes will become increasingly challenging,

and the accuracy and efficiency of current deepfake detection approaches will decline."

Technically, potential solutions are to be found in protections such as watermarking and biometric hashing. However, per Mateusz Łabuz of the Chemnitz University of Technology, "technology must be matched with awareness, regulations, resilience and ways to dampen amplification."

Peter Eisert, head of Vision & Imaging Technologies and department chair of Visual Computing at Humboldt University, has noted that many current deepfake detectors are frame-by-frame based, whereas they should be attuned to temporal effects and "inconsistency over time" – semantic and temporal information in the content, such as heart rate or temporal flow of blood in the face – as potential indicators.

Training strategies such as AltFreezing or Real Forensics offer potential ways to train detectors to pay attention to temporal features. There are further possibilities: facial expression parameters and avatar fingerprinting – a user ID technology developed by NVIDIA – which uses facial dynamics for identity verification.

Deep learning and convolutional neural networks are another option to amplify detection. Gian Luca Marcialis of sAIfer Lab's Biometric Unit is working on approaches to passive deepfake detection, and on a deepfake detection taxonomy which classes a number of detection approaches: general network/undirected detection, visual-artifacts-based, temporal-consistency based, biological signals and camera/GAN fingerprints. (In other words, extra fingers, trouble blinking, heart rate, and digital noise.)

Deepening layers of threat

Yet another major hurdle to deepfake detection is the scale of the problem, and its primary driver. A 2019 report estimated that 96 percent of all deepfakes online are pornographic, and 99 percent involve women who did not consent to their likeness being used. As such, while financial fraud and executive deepfakes are significant concerns with major financial implications, deepfakes also present risks to reputation, likeness, mental health and online safety, especially for women. (Mateusz Łabuz has asserted that the problem of deepfakes can primarily be seen as an issue of women's safety.)

Deepfake-enabled blackmail, revenge porn and child sexual abuse material can cause long-term psychological

damage to victims. Given the growing risk, the issue of "deepfakes" is likely to eventually come to encompass the concept of "likeness" – i.e., who or what is allowed to do what with an individual's likeness.

The cutting edge of deepfake detection

Among the few dozen firms offering deepfake detection, several have demonstrated leadership, won recognition or contributed notable developments to the effort.

One of the most recognizable is Pindrop, which specializes in audio deepfake detection, and gained mainstream attention for being the firm to identify the text-to-speech engine used to generate deepfake audio of U.S. President Joe Biden in January 2024.

Other noteworthy audio deepfake detection firms include Polyguard, which claims an industry-first in its real-time inbound and outbound number blocking, and Daon, which in 2024 won a U.S. patent for a way to build better deepfake voice watch lists.

In November 2024, BioID's real-time deepfake detection technology for photos and videos picked up the 9th Munich Digital Innovation Award in November. In December 2024, the U.S. Department of Defense awarded a US$2.4 million contract for deepfake detection of video, image, and audio content to the San Francisco company Hive.

This year, Au10tix identified and named a new deepfake fraud technique in "repeaters," which it defines as "minor variations of a single digital asset (face picture, image background, document number, etc.) that bad actors deploy in small numbers to test detection systems before launching cross-industry mega-attacks."

Some firms have emerged to offer specialization or expertise in certain areas or services. In May 2025, GetReal Security, a New York based firm focused on deepfake detection for governments and enterprises, closed $17.5 million in series A funding. It is notable for having as its chief science officer Dr. Hany Farid, a pioneering researcher in deepfakes.

Loti AI concentrates on the market for likeness protection, mainly centered on celebrities and public figures whose likeness represents valuable IP. Reality Defender, whose CEO Ben Colman is a regular commentator on deepfake technology, has looked at the issue of "whaling attacks" that target high-powered executives.

Idemia Group formed a consortium in 2022 to contribute to a project run by the French National Research Agency (ANR) on the development of A Prototype Assessment Toolbox for Forensic Experts (APATE). The consortium is developing forensic tools resistant to spoofing with deepfakes for the national police and forensic experts to use in prosecutions.

Market Analysis & Forecasts

This section covers market analysis and forecasts for deepfake detection for fraud prevention. As such, it includes technologies for the identification of deepfake content intended to defraud an online service, but not deepfakes of pornography or misinformation.

It investigates key drivers, adoption, key applications and sectors for deepfake detection.

There are three-year forecasts, 2025-2027, covering:

1. Checks
2. Revenue

Deepfake Detection Market Analysis

This section investigates key drivers for adoption, important sectors, and applications for the adoption of deepfake detection, and adoption examples around the world.

Key Drivers

The four key drivers for deepfake detection are:

1. Fraud Prevention
2. Enhancing Security
3. Enabling Remote Identity Verification & Authentication
4. Ensuring compliance with potential regulation

Fraud Prevention

With growing levels of fraud, especially AI-Driven fraud, deepfake detection prevents fraud by ensuring that the person is real, physically present, and not a deepfake.

Enhancing Security

Deepfake detection enhances security of digital interactions and transactions by detecting deepfake attacks. It adds an extra layer of protection against advanced AI-generated deepfake techniques.

Enabling Remote Identity Verification & Authentication

With increasing levels of deepfake attacks on identity verification and biometric-based authentication systems, the ability to withstand the latest AI-generated deepfakes is paramount.

Ensuring Compliance with Potential Regulation

With the level of deepfake attacks against critical systems, it will be probable that legislation will be introduced to mandate that companies deploy deepfake detection solutions. The EU AI Act includes provisions for identifying and labelling AI-generated content, including deepfakes.

Deepfake Detection Adoption

This section investigates adoption of deepfake detection on a regional basis, identifying key suppliers and sector focus.

It is a guide to adoption levels and reflects the health of a technology product or service.

Past and current adoption examples and levels are a key indicator for forecasting and form part of the quantitative data for forecasts.

This report includes four examples of liveness detection adoption from around the world. There are many more examples indicating an extremely healthy, and growing, technology sector.

Key Sectors

As deepfake detection is a key component of biometric-driven identity verification, authentication, and assurance, then the key sectors that are adopting the technology are predominantly those that are high-assurance sectors, often highly regulated.

GI has identified seven key sectors that are leading the way with adoption of face liveness detection:

1. Financial Services
2. Government
3. Enterprise
4. Gaming / Gambling
5. eCommerce / Retail
6. Healthcare
7. Travel (includes border control)

Financial Services

AML / KYC regulation is an important driver for the use of deepfake detection in financial services.

Identity related fraud is a growing concern for the financial services sector, driven by AI-Driven fraud including deepfake attacks on biometric systems, both face and voice. This includes all types of financial fraud including new account opening fraud where criminals use deepfake fraud using synthetic videos, audio, or images that appear to be a legitimate person and open a new bank account.

A September 2024 Medius study found that 87 percent of finance professionals admit they would make a payment if 'called' by their CEO/CFO, and 53 percent have already experienced attempted deepfake scamming attacks.

Regula has found that banks and other organizations are losing an average of $600,000 per voice deepfake incident, with 23 percent losing over $1 million.

In 2025, fraudsters cloned the voice of a Hong Kong-based financial manager, facilitating a cryptocurrency scam worth $18.5 million.

As a result of increasing levels of financial fraud, deepfake detection is becoming a critical component to detect and deter identity and financial fraud.

Government

Governments are increasingly rolling out digital services to their citizens across the globe, but this comes with risks.

The need to accurately identify citizens accessing digital government services is a vital part of delivering secure digital government services with the need to know that it is a real person accessing them becoming increasingly important.

There are also the risks associated with deepfake generated content that purports to be from legitimate politicians which is a serious threat to the rule of law and democracy.

In May 2025, the FBI issued a warning to the public after investigating a malicious campaign targeting former senior U.S. federal or state government officials with deepfakes. The campaign uses AI-generated voice messages impersonating senior US officials.

This is especially important for tax and welfare services and when applying for / renewing government-issued identity documents including Driver's Licenses, National ID, and Passports.

Enterprise

The ability to prove identity is now an integral part of a modern digital workplace supporting a range of enterprise applications including:

1. Onboarding employees: especially important for remote working scenarios.

2. Privileged access control: linked to privileged identity and access management PIM/ PAM).

3. Fraud detection in web conferences: detecting deepfake attacks in business web calls.

4. Remote worker authentication: reducing home and remote working fraud where an imposter or alternative worker attempts to gain access to business digital services.

There have been examples of deepfake attacks on employers. In April 2025, a news story ran that detailed the risks of not doing adequate identity verification for new hires. It was discovered that North Korean IT workers are using deepfake technology to create synthetic identities for online job interviews aimed at securing remote work.

This identity manipulation is part of ongoing state-sponsored employment scams aimed at infiltrating US and other organisations globally for malicious intent. The story was discovered by researchers at

Palo Alto Networks' Unit 42[1] who documented a case study involving a Polish AI company that encountered two separate deepfake candidates. Interviewers suspected the same individual operated both personas, particularly when the operator showed notably increased confidence during the second technical interview after previously experiencing the interview format and questions.

With the easy availability of deepfake creation tools, organisations must ensure that they employ robust and secure technology that can detect and prevent these kinds of AI-driven fraud attacks.

Gaming / Gambling

To counteract fraud and to support proof of age (age assurance) requirements, the gaming and gambling communities are beginning to adopt deepfake detection measures.

To support secure onboarding and to reduce money laundering liabilities, the ability to prove identity and appropriate age is an important countermeasure to fraud in a sector that has historical problems with organized crime.

eCommerce / Retail

Popular applications that are applying deepfake detection include digital onboarding, payment security, and are used in combination with face age assurance (estimation).

Governments are increasingly using legislation to prevent young people from accessing restricted goods and services, including alcohol, medication, and dangerous weapons including knives and drugs. Deepfakes are being used in an attempt to get around these checks.

Healthcare

Healthcare providers around the world lose billions of dollars in fraud. The UK's NHS lost £7.5 billion (roughly US$9.3 billion) to fraud in the six-years to 2023.

The FBI[2] lists the following fraud types in relation to common types of health care fraud that are identity related.

1. **Identity theft/identity swapping:** Using another person's health insurance or allowing another person to use your insurance.
2. **Impersonating a health care professional:** Providing or billing for health services or equipment without a license.

Combining identity proofing and verification with face liveness and deepfake detection can be a crucial tool in preventing healthcare fraud.

Travel

The travel industry is a beacon of light for the adoption of portable digital identity, backed by global standards and using government-grade security.

1 https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/

2 https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud

Remote digital services are transforming the travel industry enabling passengers to book tickets, prove their identity with government-issued documents, including passports, check-in to flights, all from the comfort of their home or office – before they leave to travel.

Key Applications

Deepfake detection is being used in four key applications:

1. Digital Onboarding

2. Biometric Authentication

3. Financial Transaction Security

4. Identity Verification

Digital Onboarding

Digital onboarding is the process of using technology to integrate new customers or employees into a service or organization. It is often called identity proofing or identity verification.

Biometrics is a vital tool for remote customer onboarding for a wide range of sectors with particularly high adoption in financial services.

Deepfake detection is a critical component for digital onboarding that prevents spoof attacks, ensuring that it is a real person and not a deepfake generated synthetic identity.

Identity verification and identity proofing are closely related but serve different purposes in the process of confirming someone's identity.

Identity proofing is the initial step where the goal is to **validate** that a person is who they claim to be. This involves collecting and analysing personal data and documents. It includes gathering information such as name, date of birth, and address, and verifying identity documents like passports or driving licenses. Often, biometric data (like fingerprints or facial recognition) is also used. The result of identity proofing is a validated identity that can be used for further verification steps.

Identity verification is the subsequent step that **confirms** the authenticity of the information and documents provided during the identity proofing stage. It can involve checking the validity of the documents and data collected. Methods can include comparing photographs on identity documents, validating biometric data, or verifying addresses and phone numbers.

Adoption of biometric onboarding services has been strong, driven by a combination of AML/KYC compliance, fraud reduction and digital transformation programs across sectors pushing onboarding to the home through remote, unattended, means.

Biometric Authentication

Biometric authentication is a security process that uses an individual's unique physical or behavioral characteristics to verify their identity, comparing the presented biometrics to a stored version (template).

Widely deployed modalities for biometric authentication include face and voice – two of the most deep-faked modalities.

Deepfake detection enhances face biometric authentication by ensuring that the presented face is a real, authorized, person. When deepfake detection is used, the biometric authentication process includes the detection of synthetically generated images, i.e., deepfakes.

Financial Transaction Security

There have been several accounts of financial fraud where large sums of money have been transferred to fraudsters believing they are dealing with legitimate colleagues, clients, or partners.

In addition to the examples already detailed in this report, In 2024, a report from Hong Kong Police said that a finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call. The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations.

The ability to detect deepfakes in this scenario would have saved the business at least $25m and is an important lesson for other organisations that manage financial transactions – not just financial institutions.

Identity Verification

Identity verification (IDV) establishes that a person is who they claim to be. It's used in a variety of situations including digital onboarding, for instance opening a bank account, proving how old we are (age assurance), travelling (especially when travelling across international borders), applying for, and starting, a job (employment onboarding), joining an educational establishment, including college and university, buying a new mobile phone, buying a new home.

Deepfake detection is now a critical component of identity verification processes, helping to ensure that the identity being verified is authentic and vendors are increasingly offering deepfake detection solutions, either stand-alone or integrated into IDV solutions.

Deepfake Detection Forecasts

Introduction

Market forecasting is very important in the Goode Intelligence (GI) research and analysis methodology especially when dealing with new or emerging markets and products.

GI has an excellent track record of forecasting in emerging technology areas including correctly predicting the growth of the mobile as an authentication device in 2009, the emergence of biometrics on mobile devices in 2011, and the growth in digital identity in 2015.

Market forecasting is one of the tools that GI uses in predicting the degree of success a new product or service will enjoy in the marketplace. The GI methodology considers areas such as *product awareness*, *distribution*, *price*, *fulfilling unmet needs* and *competitive alternatives*.

GI creates forecasts by gathering data from diverse sources like company filings, economic reports, and direct interactions (interviews) with both suppliers and buyers, some of which are bound by NDAs. GI then applies both quantitative methods and qualitative assessments (such as expert opinions) within financial models. These models are designed to estimate future performance by incorporating macroeconomic factors, industry trends, and company-specific details to provide a comprehensive view of expected growth and profitability

Revenue forecasting at Goode Intelligence (GI) involves collecting data from a variety of sources such as company filings, economic reports, and interviews with suppliers and buyers, often under NDA. This

information feeds into financial models that use both quantitative and qualitative methods, including expert opinions, to project future performance. These models consider macroeconomic factors, industry trends, and company-specific details. For revenue projections, GI calculates an average price, taking into account the variability in vendor pricing and potential discounts. The result is a comprehensive estimate of expected revenue growth and profitability for new or emerging products and markets.

We always welcome feedback from readers on the accuracy of the forecasts and are open to reflecting your opinion in future reports.

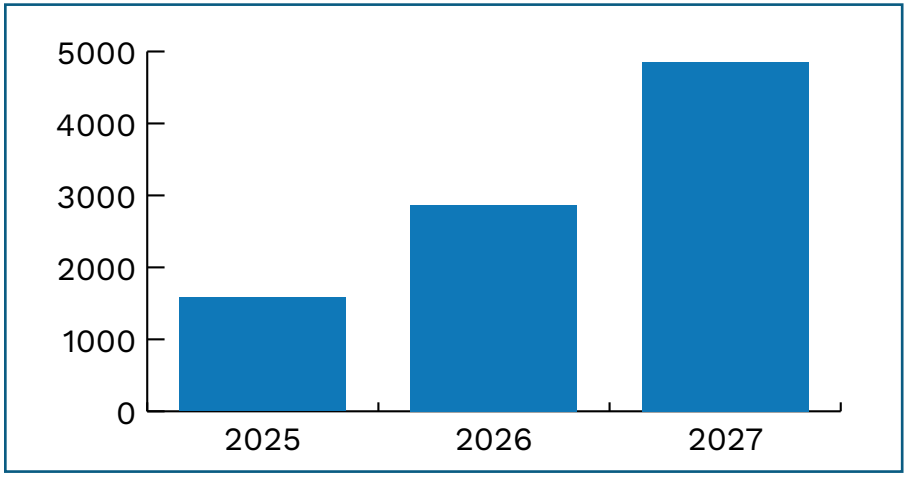
There are three-year forecasts, 2025-2027, covering:

1. Voice Deepfake Detection Checks
2. Face Deepfake Detection Checks
3. Total Deepfake Detection Global Checks
4. Total Deepfake Detection Global Revenue

Voice Deepfake Detection Forecasts – Checks

These forecasts are for total global voice deepfake detections made annually.

Chart 1: Voice Deepfake Detection Forecasts: Total Global Checks (m)



Source: Goode Intelligence © 2025

Table 1: Voice Deepfake Detection Forecasts: Total Global Checks (m)

	2025	2026	2027
Total	1581.81	2867.09	4850.28

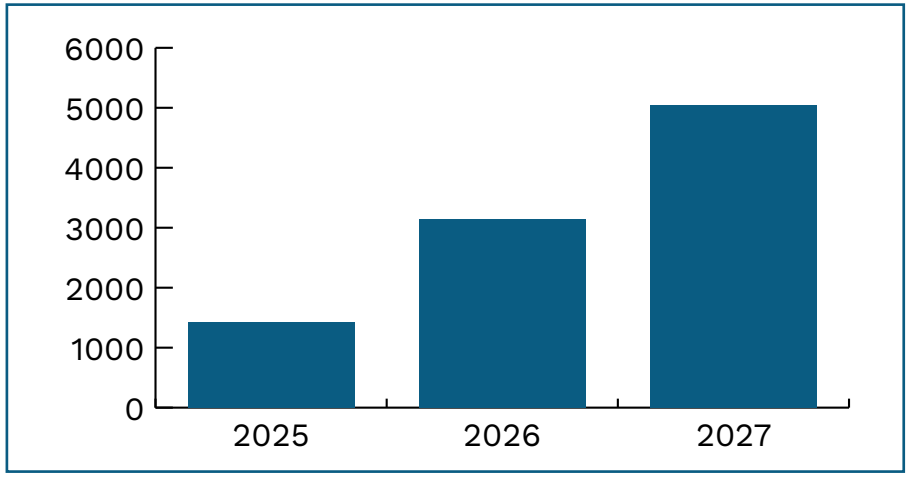
Source: Goode Intelligence © 2025

Voice Deepfake Detection Checks will exceed 4.85 billion annually by 2027

Face Deepfake Detection Forecasts – Checks

These forecasts are for total global face deepfake detections made annually.

Chart 2: Face Deepfake Detection Forecasts: Total Global Checks (m)



Source: Goode Intelligence © 2025

Table 2: Face Deepfake Detection Forecasts: Total Global Checks (m)

	2025	2026	2027
Total	1432.71	3147.09	5050.28

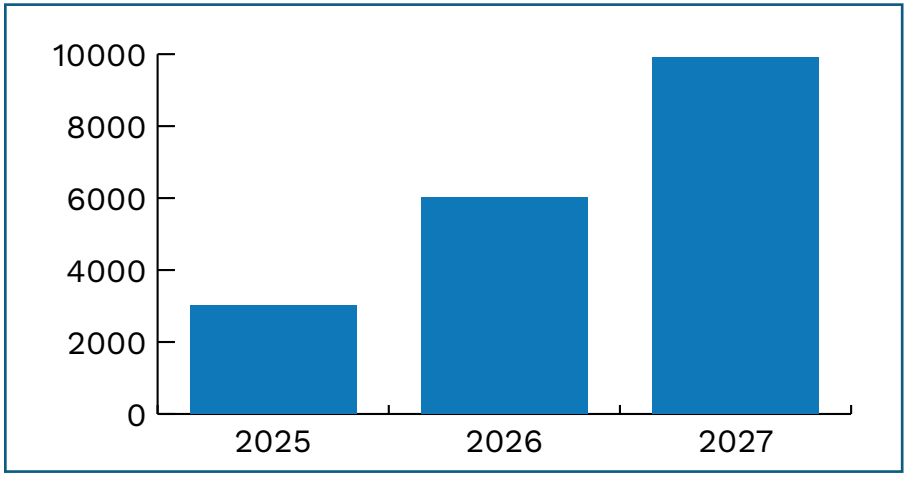
Source: Goode Intelligence © 2025

Face Deepfake Detection Checks will exceed 5.05 billion annually by 2027

Total Deepfake Detection Forecasts – Checks

These forecasts are for total (voice and face combined) global deepfake detections made annually.

Chart 3: Total Deepfake Detection Forecasts: Total Global Checks (m)



Source: Goode Intelligence © 2025

Table 3: Total Deepfake Detection Forecasts: Total Global Checks (m)

	2025	2026	2027
Total	3014.52	6014.18	9900.56

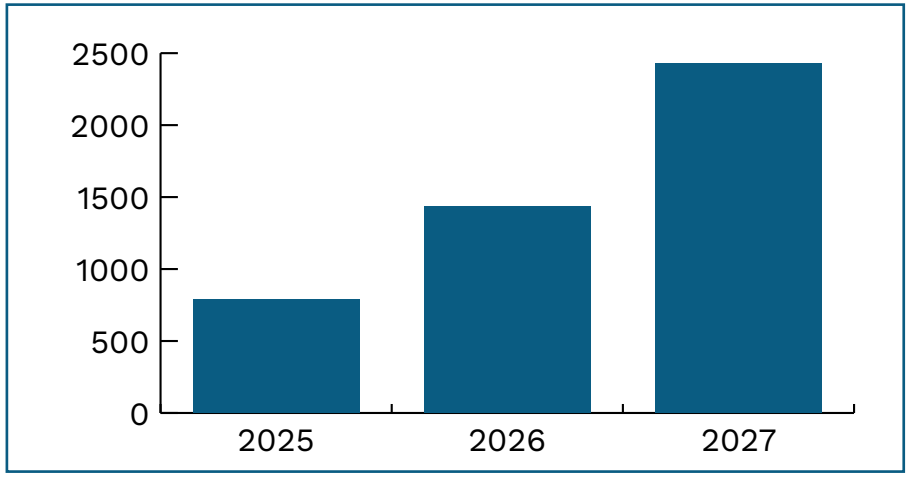
Source: Goode Intelligence © 2025

Total Deepfake Detection Checks will exceed 9.90 billion annually by 2027

Voice Deepfake Detection Forecasts – Revenue

These forecasts are for annual global voice deepfake detection revenue in US Dollar (million).

Chart 4: Voice Deepfake Detection Forecasts: Total Global Revenue (m)



Source: Goode Intelligence © 2025

Table 4: Voice Deepfake Detection Forecasts: Total Global Revenue (m)

	2025	2026	2027
Total	790.91	1433.55	2425.14

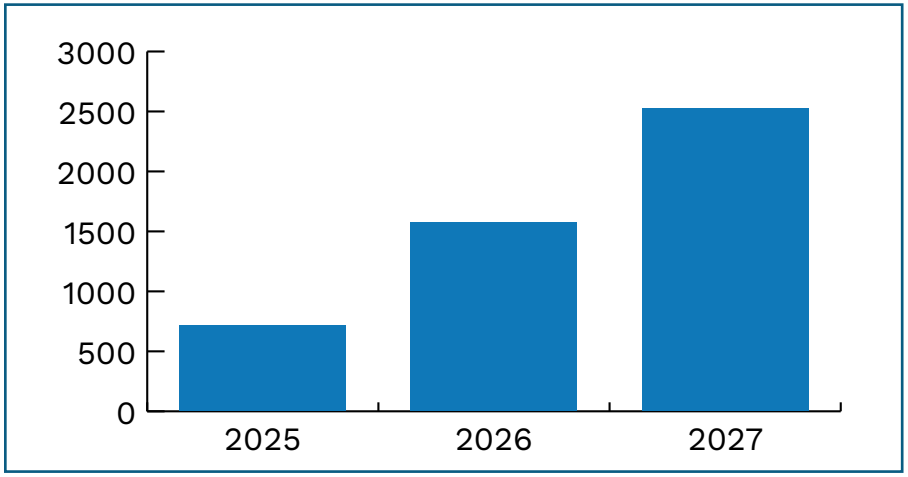
Source: Goode Intelligence © 2025

Voice Deepfake Detection Revenue will exceed $2.42 billion by 2027

Face Deepfake Detection Forecasts – Revenue

These forecasts are for annual global face deepfake detection revenue in US Dollar (million).

Chart 5: Face Deepfake Detection Forecasts: Total Global Revenue (m)



Source: Goode Intelligence © 2025

Table 5: Face Deepfake Detection Forecasts: Total Global Revenue (m)

	2025	2026	2027
Total	716.36	1573.55	2525.14

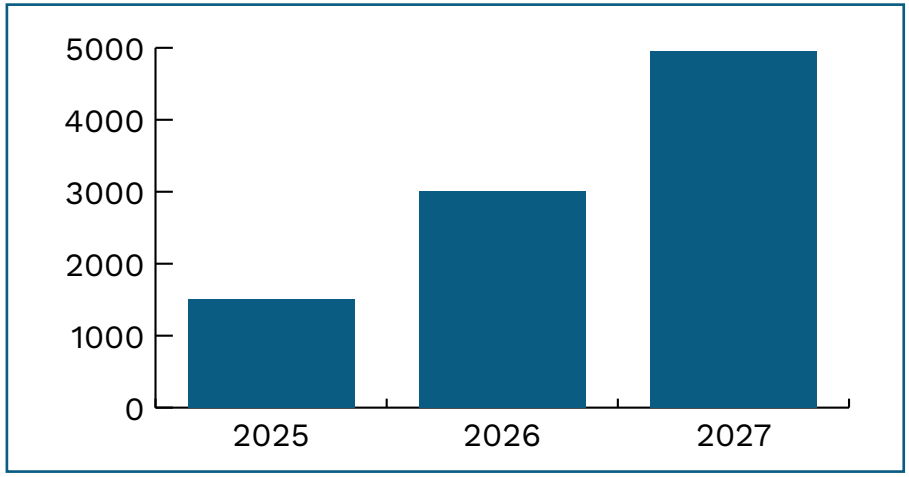
Source: Goode Intelligence © 2025

Face Deepfake Detection Revenue will exceed $2.52 billion by 2027

Total Deepfake Detection Forecasts – Revenue

These forecasts are for annual global total (voice and face combined) deepfake detection revenue in US Dollar (million).

Chart 6: Total Deepfake Detection Forecasts: Total Global Revenue (m)



Source: Goode Intelligence © 2025

Table 6: Total Deepfake Detection Forecasts: Total Global Revenue (m)

	2025	2026	2027
Total	1507.26	3007.09	4950.28

Source: Goode Intelligence © 2025

Total Deepfake Detection Revenue will exceed $4.95 billion by 2027

Deepfake Detection Buyer's Guide

This guide provides potential buyers of deepfake detection products and services with information on how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing deepfake detection solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of deepfake detection vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strives to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a "best efforts" basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

Common terms and definitions

Deepfake - A piece of fake or altered digital media, typically used to impersonate an individual, created using artificial neural networks, deep learning algorithms and other generative AI technologies.

Deepfake Detection - Analyzing media to detect fake videos or images that have been generated using deep learning and GenAI.

Algorithm - A finite set of mathematical instructions that defines a sequence of operations. When input into a computer, they can be used to perform computations and/or data processing.

AML - Anti-money laundering; systems and tools to prevent the crime of money laundering.

Artifact - A telltale sign left behind in a deepfake generated by a GAN, which can enable easier detection.

Biometric Authentication - The process of ensuring a human is who they say they are through the analysis of biometrics such as faces, voices or fingerprints.

Biometric Injection Attack - A type of fraud attack in which biometric data, such as a face or voice, is digitally "injected" into a live media stream using malware or malicious code.

Cheapfake - A piece of fake or altered media created using conventional (i.e. non-algorithmic) and easily accessible technology; for example, a fake ID created using Photoshop.

Deep Learning - A subset of machine learning that uses multiple layers of artificial neurons, called deep neural networks, which are trained on data that enables them to make decisions in tasks such as classification and regression. Capable of unsupervised raw data processing and pattern recognition, deep learning is meant to mimic the way neurons in the human brain process information.

Face swap - Replacing or superimposing one person's face over another in an image or video.

Fraud-as-a-service (FaaS) - Networks of fraudsters who work for hire on behalf of those are willing to pay. FaaS entities offer their services in tiers, which can be ordered like a phone plan.

GAN - Generative adversarial network. A system of competing neural networks that analyze data and train each other to make their outputs more realistic.

Generative AI/GenAI - A catch-all term for algorithmic technology that learns the underlying patterns and structures of training data and uses generative models to produce new text, images, videos, or other content, typically based on a user prompt.

Hashing - A one-way process in which an algorithm called a cryptographic hash function takes an input of any size and converts it to a fixed-size alphanumeric output, called a hash value or hash – a distinct string of random characters. In biometric hashing, the source input is biometric data such as a face, fingerprint, iris or palm scan.

Identity Verification - The process of confirming that a person is who they say they are, using tools such as identity documentation and biometrics.

Likeness Protection - Services that protect the likeness of a celebrity or high-profile figure, which may have inherent value or influence.

Liveness / Liveness Detection - Technology designed to tell whether a user is a real, living human. Historically referred to as Presentation Attack Detection (PAD), liveness detection has gained prominence with the rise of deepfakes.

Know Your Customer/KYC - Regulations and guidelines requiring businesses to verify customers' identities and assess risks involved with maintaining a business relationship with them. From a regulatory standpoint, KYC is a subset of AML.

Neural Network - A machine learning program or computational model, the design for which is based on the structure and activity of the human brain, such that it might make decisions in a similar way.

Voice Synthesis - The application of deep learning models to generate, from written text, synthetic speech that replicates the tone, pitch and cadence of a human voice.

What do you look for in a deepfake detection supplier

This section provides a guide for buyers in what to look for in a deepfake detection supplier.

It is important to repeat that this guide should not be used as the sole method for assessing deepfake detection solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

This report identifies the following baseline criteria for measuring whether a deepfake detection is suitable.

1 **Cost - does it meet your budget expectations:** This is especially important when dealing with suppliers that charge per transaction, which is often the case. If you are entering into a per transaction contract, have you sized your requirements for now and for future growth and does your budget meet this?

2 **Accuracy and Speed:** The software should have high accuracy (low false positives and false negatives) and be able to process media quickly.

3 **Detection of specific deepfake techniques:** Deepfakes are created using various methods (e.g., face-swapping, face reenactment, GAN-based generation). Ensure the solution detects these different approaches.

4 **Multi-Modal Analysis:** Does it analyze images, videos, and audio? Deepfakes can involve any or all of these, so a comprehensive solution should address all possibilities, according to research from The Alan Turing Institute.

5 **Detection of subtle inconsistencies:** Look for features that can identify artifacts like blurring, color differences, unnatural lighting, or inconsistencies in facial features (eyes, mouth, hair) and body parts (hands, fingers).

6 **Bias:** Ensure the solution has been tested for bias and is fair in its analysis of different types of media.

7 **Biometric-based detection:** Some solutions analyze subtle physiological indicators like heart rate or pulse through skin analysis, which can be difficult for deepfakes to replicate.

8 **Security:** Does the supplier have cybersecurity certifications and adhere to cybersecurity guidance / best practice?

9 **Does it meet your specific usability requirements?** The ability to fit in with your usability (UX) requirements is an important consideration when choosing a deepfake detection supplier.

10 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

11 **Integration:** Check whether the solution can be easily integrated into existing systems and workflow.

Vendor Profiles & Case Studies

Biometric Update and Goode Intelligence have identified more than 40 vendors that provide deepfake detection and protection technologies. The technologies for deepfake detection and protection are in many cases developed by companies that draw on extensive experience with user authentication and fraud prevention. Several newer deepfake detection and protection providers were founded specifically to address the threat of deepfakes. In many cases, deepfake and protection solutions are used in combination with liveness and injection attack detection solutions, often being bundled (aggregated) into a combined solution. The vendors profiled use a variety of techniques and offer software for a range of applications, but are united by a mission to stop deepfake fraud.

Aurigin.ai

aurigin.ai
info@aurigin.ai
Giesshübelstrasse 62B
8045 Zürich

Aurigin.ai delivers market-leading detection of synthetic speech with high accuracy, real-time performance and lightning fast integration. Its tech powers digital-trust companies in voice authentication, cybersecurity and fraud prevention, securing enterprises, banks, defense, and government communications so phone calls, video meetings, and contact centers remain protected against impersonation and deepfake attacks.

Aurigin.ai delivers voice deepfake detection technology via SaaS and API to make it deployable on cloud or lightweight hardware. The SaaS consists of a desktop app for real-time alerts and a web app for file analysis.

The API integrates with minimal code. Pricing spans free-tier, usage-based API credits, per-seat desktop plans, and enterprise options for custom, on-premise or fully local deployments.

The firm's technology achieves 98 percent-plus accuracy with a false positive rate below 2 percent. Detection runs in under 50 milliseconds, requires only 3 seconds of audio, and works across 40 languages. It is robust to re-recordings, low-quality phone calls, background noise and new voice cloning technologies without retraining.

At the bit level, generative AI will soon produce voices indistinguishable even for machines, as it already can for the human ear. AI versus AI alone will not work anymore. That's why our approach is future-proof: we combine multiple layers including deceptive content analysis, source identifiers, voice clustering, voiceprint matching, watermarks and style fingerprinting.

Aurigin.ai Secures Police Command Center

The national police command center manages some of the country's most sensitive communications, where senior officials receive and relay orders of critical importance. These include authorizations for counter-terrorism operations, deployment of armed forces and coordination of emergency responses. Any falsified instruction – a terrorist group or fraudster impersonating a government or military official – could result in catastrophic outcomes, from misdirected units to paralyzed crisis response.

To secure this communication line, Aurigin.ai developed a real-time (<50ms latency) deepfake detection device that continuously analyzes room audio with 98 percent-plus accuracy and a below 2 percent false positive rate. As part of a strategic hardware partnership with Sennheiser, the solution was engineered to meet police-grade requirements: fully isolated from any networks for maximum resilience and data privacy. The model runs on a Raspberry Pi and acts like a "smoke detector" for synthetic voices, instantly alerting officials to impersonation attempts without disrupting daily communications.

Ongoing tests with the police have demonstrated that the system robustly identifies impersonated voices even in challenging environments with background noise, low audio quality, rerecordings and differing dialects. For the police, the technology adds a trusted layer of defense against one of the most advanced and dangerous forms of modern fraud.

"Aurigin.ai's delivers results in just seconds, analyzing as little as five seconds of audio with high accuracy. This speed is critical for us."

Keyless

keyless.io
media@keyless.io
Milton Gate 60 Chiswell Street
London United Kingdom EC1Y 4AG

Keyless provides facial biometric authentication, using face biometrics to authenticate users in-app at critical touchpoints – making payments, recovering accounts – without storing their biometric data anywhere. The company was founded in the UK in 2019. Its clients work in high-trust industries such as banks, fintechs, governments, and education institutions, including the largest neo-bank in the DACH region (Germany, Austria, and Switzerland) and the largest traditional bank in Italy. Prominent identity verification vendors like IDnow and Experian have integrated Keyless' biometrics to provide their customers with end-to-end identity services that encompass both verification and authentication.

Keyless believes most authentication methods (PINs, OTPs, call centers, FaceID, even passkeys) are weak, expensive or frustrating to use, and replaces them with a simple facial scan, checking both the user's face and device against those used at KYC.

Keyless deepfake detection runs automatically with every authentication, at no extra cost. It is multi-factor by design, combining passive liveness, device integrity checks and behavioral biometrics. To authenticate, users must have the original enrolled device – or another verified later via NFC. Since most deepfake attacks are remote, this makes deepfakes non-scalable.

Keyless' technology is continually tested and evaluated against industry-leading benchmarks. Keyless was evaluated by NIST in 2024 and 2025, ranking among the top 50 algorithms globally in the 1:1 test for face match verification for login scenarios, outperforming all direct competitors, and 11th globally in the 1:N test, achieving 99.93% accuracy from 1.6 million identities in a test of real-world identification scenarios like airport security. The NIST evaluation showed a False Match Rate (FMR) of 0.001 percent and a False Non-Match Rate (FNMR) of 0.25 percent.

When evaluated against FIDO benchmarks, Keyless achieved a False Reject Rate (FRR) of less than 0.33 percent, a False Accept Rate (FAR) of under 0.01 percent and 100 percent Presentation Attack Detection (PAD).

These results are indicative of a 'Face-to-ID' use case, demonstrating its model's high accuracy in verifying whether two facial images belong to the same individual or not.

Regarding standards, the current efforts to establish deepfake detection standards are affecting the market by adding complexity and costs for vendors. Keyless believes that focusing on developing separate deepfake detection standards is not a priority. The existing standards for Presentation and Injection attacks already provide robust protection against deepfakes. While deepfakes pose a real challenge, a single, effective, and credible set of standards for Presentation and Injection attacks remains sufficient, streamlining the approach for vendors and buyers alike.

Mobai

mobai.bio
info@mobai.bio
Studievegen 16, 2815 Gjøvik, Norway
+47 242 00 002

Mobai is on a mission to make the internet a safer place by redefining identity verification. In a world where passwords are outdated and deepfakes pose real threats, we enable users to prove they are real, genuine individuals – using nothing but their face. Mobai face verification is intuitive for users and adds a powerful layer of protection using strong attack prevention and privacy enhancing technologies.

Mobai delivers easy to use, secure facial verification, including embedded and standalone solutions for presentation attack detection (liveness detection), deep fake detection and inject attack detection. Mobai was founded by leading researchers in biometrics and cybersecurity in 2019 as a spin-off from the Norwegian University of Science and Technology (NTNU). Since then, it has collaborated with top-tier electronic identity, cybersecurity, and financial service providers across the Nordics, as well as with key EU agencies.

Mobai's Deepfake Detection uses advanced machine learning to quickly identify identity swaps, face editing and synthesized media in under 200ms. It scores 98 percent accuracy, ensuring a secure and seamless user experience while meeting industry standards for robust protection against sophisticated deepfake attacks. Mobai's technology is specifically designed for identity proofing and authentication, tackling the broader challenge of inject attack detection and prevention.

Deepfake standards are still emerging. Mobai's solutions comply with ETSI TS 119 461, addressing the critical requirements for detecting manipulated faces in standards for identity proofing. They also align with the inject attack detection standards from CEN/TS 18099, ensuring the technology meets rigorous European benchmarks for security and reliability.

Mobai has observed a significant increase in deepfakes and injection attacks, as attackers prefer scalable attack vectors where they can leverage automatic tooling (face swaps, use of emulators, etc). However, buyers must also protect themselves against simpler, low-tech methods that are easy to try, alongside developments and advancements in presentation attacks with cutting edge liveness detection.

Frame-level binary deepfake detection is rapidly becoming obsolete, as it fails to identify temporal inconsistencies and cannot withstand social media compression artifacts. The industry requires temporal, multi-modal, context-aware detection approaches that analyze videos across multiple frames to provide robust protection against sophisticated threats.

eIDAS: Secure Remote eID Issuance & Future Proofing

Mobai is working closely with a trust service provider in ensuring issuance of eID remotely, while preparing for the eIDAS 2.0 implementation of issuing eIDs and certificates. The scope is to ensure issuance leverages secure remote biometric capture to enable an identity verification that results in a strong binding to the person being issued an eID.

In such a workflow the risk of presentation attacks and inject attacks are significant. Thus Mobai deploys Presentation Attack Detection (PAD) and Inject Attack Detection (IAD) solutions, which combine its ISO/IEC 30107 tested liveness detection together with a holistic injection attack detection methods to ensure that a live, genuine user is performing the identity verification and subsequent authentications.

The trust service provider is operating in a regulated market, with multiple changes in regulation and development

of standards in the field. Together with the assistance of Mobai, **they are able to provide evidence needed for auditing processes and to show compliance with key regulatory requirements**, including how they leverage biometrics and actively monitor the threat landscape, assess risk and improve systems to ensure conformity with best practices for remote identity proofing.

Mobai says that, when it started the delivery, the trust service provider's legacy biometrics were slow and struggled with false rejections. Together with Mobai they **optimized a user experience of the identity proofing tailored for their issuance process and** achieved a 10 times reduction in speed of processing of the biometric components.

Oz Forensics

ozforensics.com
Office 384, Saih Shuaib bldg 2 area,
DIC, Dubai UAE

Oz Forensics is a global leader in preventing presentation and synthetic biometric attacks, while prioritizing positive customer experiences. Founded in 2017 and headquartered in Dubai, Oz helps thousands of customers across multiple continents to mitigate risks associated with identity fraud, around the clock. Its clients range from governments, to eKYCs, to banks and financial institutions, to travel companies and document processing organizations.

The democratization of technology and GAN pipelines that optimize the capabilities of bad actors has made it crucial to have a multi-modal approach to deepfake detection. Single-cue artifact analysis, especially techniques that look for simple physiological anomalies such as unnatural eye-blinking, lip movement and mismatches and compressions, will soon be outdated; today's generators frequently fail to deliver quality videos in these small details but are fast improving.

Oz Forensics believes standards and certifications help reduce vendor-selection risk and encourage interoperability, and should be a first aspect in shortlisting a liveness solution.

The firm's biometrics and liveness detection tools have been certified by leading standards bodies. Its facial liveness detection product to counter deepfakes and spoofing is compliant with ISO-30107 via iBeta and NIST.

In lab tests by iBeta, it achieved a False Acceptance Rate of 0, a False Rejection Rate below one percent, and a Conversion Rate of 97 percent on first attempt and up to 99 percent overall.

The Oz Forensics SDK is available for web, iOS and Android.

Security Meets Simplicity: Unico + OZ Identity Journey

Unico, one of the world's largest identity validation networks, faced mounting challenges: increasingly sophisticated fraud attempts, 24/7 operational demands, and the need for a seamless user authentication experience. Unico, which operates largely in Brazil, sought a scalable, robust liveness detection solution – and found its partner in Oz Forensics.

After implementation of Oz's technology, Unico's conversion rate increased from 95.8 to 99.7 percent, even while handling millions of authentications per month. Among users over 60 years old, conversions rose by an impressive 70 percent, thanks to the solution's intuitive and frictionless design.

The biometric capture time was also significantly reduced, improving onboarding speed across all user

profiles, regardless of device or platform (iOS, Android, Web). With accurate detection of spoofing and deepfakes, Oz further strengthened the integrity of Unico's authentication flow.

Client feedback was immediate and enthusiastic: many requested to expand Oz's solution across their operations, due to its simplicity and the resulting conversion rates.

Paravision

paravision.ai
info@paravision.ai
San Francisco, California

Founded in 2013 in San Francisco, Paravision is a leader in trusted Identity AI, delivering carefully crafted AI building blocks that are ethically developed, conscientiously sold, and built for the next generation of digital identity. The company consistently ranks among the top global performers in leading biometric benchmarks, including NIST's Face Recognition Technology Evaluations (FRTE) for 1:1 Verification and 1:N Identification, the U.S. Department of Homeland Security's Biometric Technology Rally and Remote Identity Verification Test (RIVTD), and the Age Check Certification Scheme (ACCS).

Paravision's face recognition, liveness, deepfake detection, and age estimation technologies are easy to deploy across major platforms—from cloud to edge—and are trusted by governments, fintechs, and identity verification providers for identity authentication, fraud prevention, and forensic analysis.

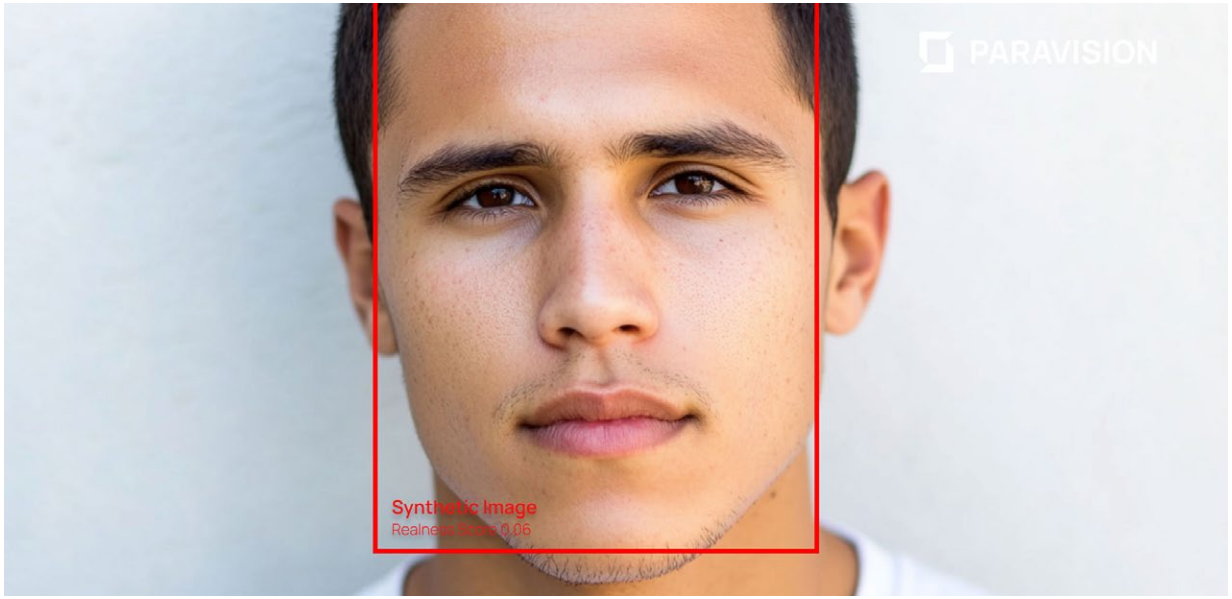
As generative AI tools become more accessible, deepfakes and synthetic face imagery have emerged as some of the fastest-growing and most sophisticated fraud vectors. To address this, Paravision launched Deepfake Detection 2.0, a cutting-edge solution that detects digitally manipulated and fully synthetic faces, including face swaps, expression swaps, and AI-generated faces created with GANs and diffusion models. The solution works in tandem with Paravision's Liveness Detection to provide layered protection against both digital and physical presentation attacks in a single capture.

In the absence of a globally recognized benchmark for deepfake detection, Paravision developed an internal test framework validated on over 700,000 real and synthetic images across demographics. On this rigorous, diverse benchmark, Deepfake Detection 2.0 achieves a BPCER of less than 1% at an APCER of 1%.

Trusted for both high-volume identity verification and government-scale deployment, Paravision's deepfake detection technology has transitioned from R&D to production through a multi-year implementation with a Five Eyes government partner. This operational-grade system protects national, enterprise, and citizen-facing services from the accelerating threat of synthetic media, delivering critical security at the highest levels of trust.

Deepfake Detection: From R&D to Real-World Impact

Paravision, a leader in trusted Identity AI, has transitioned its Deepfake Detection solution from research to operational deployment through a production-grade program with a Five Eyes government partner. This partnership builds on a multi-year collaboration that began in 2022, expanded in 2023, and entered its implementation phase in late 2024. The goal: protect national, government, and enterprise communications and identity systems from the escalating threat of synthetic media.



Paravision's Deepfake Detection 2.0 achieves exceptional performance through a proprietary dataset of over 1.6 million synthetically generated images and evaluation against more than 700,000 manipulated or real-world samples. The model achieves an Equal Error Rate (EER) of just 0.98 percent. Paravision's technology identifies both manipulated faces (such as face swaps or expression swaps) and entirely synthetic faces created via GANs or diffusion models. With flexible deployment options including Docker containers and SDKs, it can be integrated into identity verification, media authentication, or fraud prevention workflows across sectors.

As part of this partnership, Paravision is operationalizing its solution for live government and enterprise environments where speed, accuracy, and robustness are critical. The combination of Deepfake Detection and Paravision's Liveness solution forms a powerful foundation for Authentic Identity, defending against both physical and digital presentation attacks. This deployment underscores Paravision's ability to help secure digital identity and information integrity at the highest levels of trust.

Pindrop Security

pindrop.com
info@pindrop.com
817 West Peachtree Street NW, Suite 770,
Atlanta, Georgia, United States
404 721 3767

Pindrop is a leading player in voice biometrics and intelligence, specializing in audio deepfake detection and voice security for contact centers and beyond. Founded in 2011, it works with some of the largest financial institutions – banking, insurance and investment firms – in particular to protect those with high-risk call centers from synthetic voice fraud. It has also seen strong adoption of the Pindrop® Pulse deepfake detection tool within the media, healthcare and retail sectors. In 2025, the company surpassed $100 million in Annual Recurring Revenue (ARR).

Pindrop's models have been trained on over 20 million utterances, from more than 530 different TTS engines, covering more than 40 languages. Its platform sets the standard for voice security through a combination of secure authentication, powerful fraud detection and cutting-edge deepfake detection.

Pindrop® Pulse analyzes liveness for more than 130 million calls annually in enterprise environments, a scale unmatched in the industry. Leveraging AI to identify unique audio patterns and distortions, it helps businesses safeguard sensitive customer information, protect against synthetic voice attacks, and minimize financial losses.

Pindrop Pulse® Inspect, built for media, governments, nonprofits and social media companies, allows organizations to verify audio content post-event. Recently, it launched Pindrop® Pulse for meetings in beta with several large financial institutions; this product, available for Zoom, Microsoft Teams and Webex, brings deepfake detection to meetings by analyzing audio and video content in real time.

Currently, deepfakes make up a little over 2 percent of all fraud attacks, but that proportion is growing rapidly. Pindrop's 2025 Voice Intelligence & Security Report, which analyzes over 1.2 billion calls, revealed that deepfake attacks surged over 1,300 percent in 2024. As the wave grows, manual detection, which many companies still rely on, will not work. Even now, the success rate of humans detecting audio deepfakes is just 54 percent.

Pindrop's tech has achieved 99 percent accuracy in detecting deepfakes from known text-to-speech (TTS) engines, and about 90 percent accuracy when it comes to zero-day or previously unseen synthetic voices. A recent NPR study tested other solution providers and found Pindrop to be the most accurate.

Deepfakes are the fastest-growing fraud type, especially in the insurance, retail and banking industries. Deepfake generators are evolving fast, often utilizing adversarial techniques to strip or bypass watermarks or known artifacts. Without combining liveness and behavioral analysis, systems may soon be inadequate against zero-day or adversarial attacks. That's why Pindrop believes layered security is essential.

Credit Union halves authentication time with Pindrop

The 86-year-old Michigan State University Federal Credit Union (MSUFCU), with $7.7 B in assets, implemented Pindrop Protect and Passport, integrated with Five9. Before, each call involved a lengthy IVR authentication (about 90 seconds), leading to rising call times (now about 8.5 minutes) and growing fraud exposure, including deepfake threats.

The challenge was improving long authentication times that increased agent workload and cost per call. IVR/IVA lacked visibility into fraud, and synthetic calls were rising – about 200,000 out of 21 million in 30 days.

Pindrop's solution streamlined caller verification, letting agents authenticate quickly and enhancing fraud investigation capabilities. Within 90 days, results showed a 50 percent reduction in average Member Authentication Time, from 90 seconds to 45 seconds. Call handling got more efficient, and faster authentications reduced support cost and improved member experience.

By cutting auth time in half, MSUFCU improved operational efficiency, agent productivity, and security at scale – without needing drastic overhauls.

Polyguard

polyguard.ai
info@polyguard.ai
309 E 9th St., Apt 2A, New York, NY 10003
250-216-5112

Polyguard

Polyguard is the only software company focused solely on preventing deepfake attacks, not just detecting them. It provides real-time, continuous identity verification during interviews, video conferences, and sensitive operations like financial transactions or password resets. Professional services firms use Polyguard to secure client communications. Executives rely on it to verify internal comms. HR and compliance teams use it for hiring and location-risk management. IT teams use it to protect account access and handle sensitive requests like MFA resets or privilege escalations.

Polyguard prevents impersonation in sensitive workflows by verifying the real human behind the screen, continuously and in real time. Using device-local biometrics, presence validation and verifiable audit logs, Polyguard reduces liability and restores trust. Polyguard is privacy-first by design: all personal data stays exclusively on the user's smartphone.

And deepfakes? Polyguard doesn't detect deepfakes – it prevents them. Polyguard rejects passive deepfake detection. Every interaction uses active identity verification: real-time face matching, presence validation, and cryptographically signed proofs. They verify the actual person taking the action, not just the file they upload or the voice on the call. Credentials in Polyguard are combined into a signed bundle; once unlocked with on-device facial recognition, it can be shared within video calls, or attached to emails or API calls. Verification is offered as a software service and priced per seat, allowing unlimited use.

Deepfakes are a subset of a broader problem: identity misuse. Polyguard sees more human-in-the-loop fraud using synthetic identities and credential sharing than pure AI-generated attacks. Focusing solely on deepfakes misses this larger and more common threat vector. The only durable solution is to verify the human – not the media.

Reality Defender

realitydefender.com
Hello@realitydefender.ai
60 Hudson St, Suite 1807,
New York 10013, NY

Reality Defender is an RSAC Innovation Award-winning cybersecurity company that helps enterprises and governments detect deepfakes and AI-manipulated media. The company's platform protects call centers from voice fraud, secures video conferencing meetings from impersonations, detects manipulated media in journalistic and broadcast content, and safeguards government and enterprise communications.

With privacy-first architecture, industry-leading multimodal and multi-model detection, and global partners such as Booz Allen, NVIDIA, IBM and Accenture, Reality Defender has defined synthetic media defense for customers including CBS, BNY, The Port of Los Angeles, Palo Alto Networks, MediaCorp, and Deloitte, alongside global banks, defense agencies and multinational corporations that remain confidential.

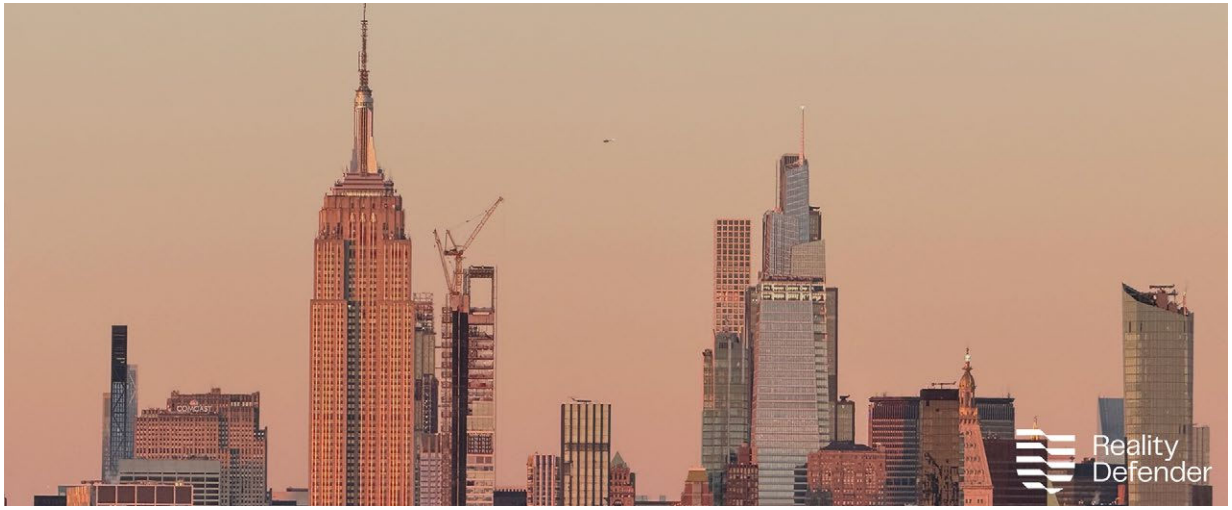
Reality Defender offers real- and near-time deepfake detection for images, audio, video and text. The company's recently introduced context-aware model analyzes beyond facial features, using multiple proprietary techniques to identify manipulated images and video with superior accuracy. Powered by custom AI models trained on vast datasets, Reality Defender integrates seamlessly into existing systems via API or as a platform, protecting organizations from AI-generated threats.

As a prime example of deployment, the NATO Strategic Communications Centre of Excellence used Reality Defender to analyze 363 videos from pro-Kremlin sources on VKontakte, surfacing deepfake propaganda during the Ukraine invasion. In short order, the system confirmed 12 deepfakes and flagged additional suspicious content delivering high-confidence results with zero false positives.

Bad actors can strip or bypass legacy detection techniques like watermarks, making them unreliable. Reality Defender takes a different approach, using a patented multi-model ensemble that concurrently and directly analyzes multiple modalities . This generator-agnostic, context-free, and continuously updated architecture ensures resilience against zero-day and adversarial deepfakes, providing enterprises and governments lasting protection.

Global Bank Detects Synthetic Voice Fraud with Reality Defender

AI voice fraud has quickly evolved from a theoretical concern into a tangible threat for global financial institutions. A tier-one bank managing billions in daily transactions experienced a rise in synthetic voice calls that bypassed defenses such as voice biometrics and callback checks. The company's fraud and risk teams lacked visibility into synthetic voice threats and needed a detection platform capable of operating in live, high-volume environments.



The bank partnered with Reality Defender to assess and secure its call centers and conferencing platforms, including Meet, NICE, Twilio, and Five9. Reality Defender's deepfake detection platform analyzed more than 2 million customer calls across U.S. and LATAM operations, including sensitive workflows like authentication and executive escalations. Results were returned in real time to more than 600 frontline staff without disrupting workflows or requiring changes to existing telephony systems.

Key outcomes included the detection of more than 1,000 synthetic voice calls that had previously evaded traditional fraud controls. This gave fraud teams visibility into AI-generated threats and enabled new triage and escalation processes.

By deploying Reality Defender, the bank established a proactive defense against synthetic voice fraud, proving that large-scale detection can be achieved without compromising customer experience. The partnership demonstrates how financial institutions can stay ahead of evolving AI threats while meeting emerging regulatory expectations for fraud prevention.

As the CTO of the bank's private client division put it:

"Our implementation of Reality Defender's AI detection technology exemplifies our approach to security innovation. By integrating Reality Defender into our contact centers, we've added a powerful layer in our defenses against voice fraud."

ROC

roc.ai
bd@roc.ai
1290 N Broadway #1200, Denver, CO 80203
+13033176118

ROC is the only multimodal biometrics and Vision AI provider, supporting trusted identity and situational awareness for the U.S. military, law enforcement and FinTech. The Colorado firm powers real-time intelligence across every operational domain: identity, tactical video analytics, digital evidence and ABIS.

In 2024, injection attacks surged 9 times – fueled by a 28-times spike in virtual camera exploits – especially in remote onboarding, virtual KYC and adversarial testing. These AI-native threats are now the top concern in national security and FinTech identity pipelines.

ROC's Camera Injection Attack Detection pairs seamlessly with the ROC Identity Toolkit, which features face recognition, single-frame passive liveness, age estimation and face analytics. The result is a complete biometric verification platform spanning the spectrum of authentication, deepfake detection and fraud prevention. ROC Camera Injection Attack Detection exposes virtual cams and synthetic sources with over 95 percent precision and is compliant with iBeta Level 2 (ISO 30107-3) standards for advanced Presentation Attack Detection (PAD).

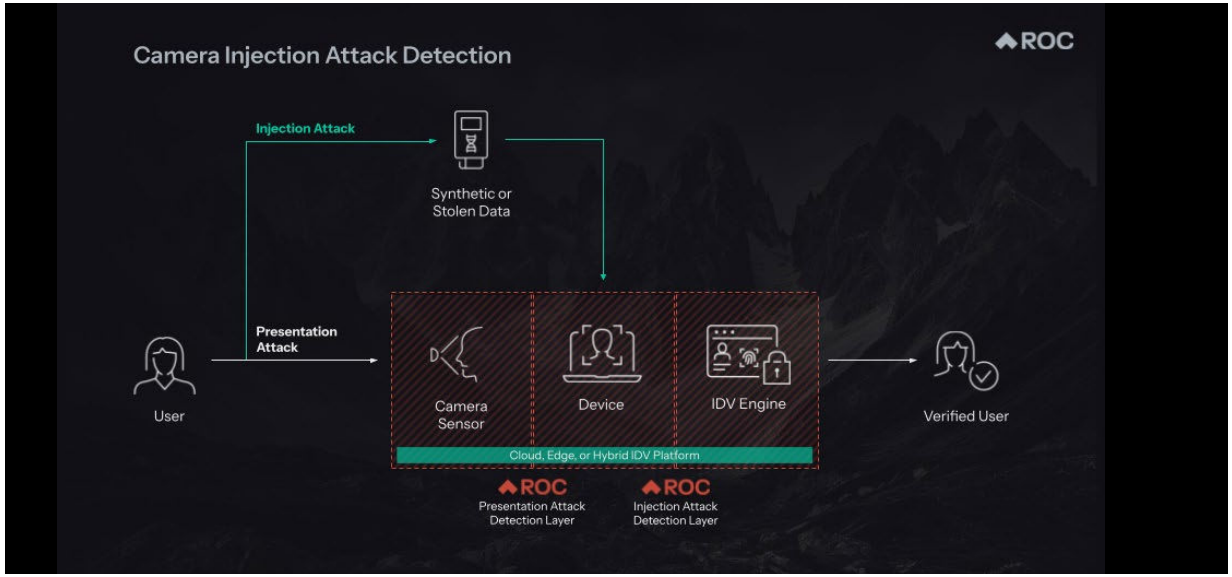
Single-modality deepfake detectors, especially those reliant only on pixel-level analysis, are increasingly fragile. As generative models improve, purely visual detectors will be bypassed by AI capable of replicating skin texture, eye motion and compression artifacts. Long-term resilience requires multimodal fusion and real-world signal integrity checks.

ROC is pushing for stronger, NIST-style protocols and real-world threat models to validate detection performance. Standards will define procurement confidence – and determine which tools survive operational deployment.

ROC Camera Injection Attack Detection

Stop Deepfakes at the Source with Injection Attack Detection

In recent years, deepfakes have become a critical threat, eroding trust and compromising the integrity of IDV systems. As fraud evolves at the speed of AI, bad actors are now entering systems through a new attack vector: injection attacks. Instead of spoofing a selfie with a photo, video, or mask, attackers now bypass the camera layer entirely, injecting synthetic video streams, avatars, or virtual cams straight into the IDV pipeline.



Traditional liveness wasn't built for this. In 2024, injection attacks surged 9x, fueled by a 28x spike in virtual camera exploits, with standard defenses struggling to keep up.

ROC Camera Injection Attack Detection is the first solution of its kind engineered to catch synthetic inputs at the source. A tripwire for stolen or synthetic imagery, it uses advanced camera forensics to expose deepfakes, virtual cams, emulated face swaps, and synthetic sources with 95%+ precision.

How Injection Attacks Work:

1. Injection attacks insert false biometric data, like deepfake videos or scraped imagery, directly into the IDV system.
2. These bypass the physical camera, exploiting weaknesses in traditional software-based liveness checks.
3. Success! Injection attacks are more successful because they avoid sensor input, easily fooling standard PAD algorithms.

While iBeta PAD testing provides a solid foundation, it doesn't address injection attacks. ROC's next-gen camera forensics layer closes this gap before a single frame is processed.

Stop this new face of fraud. Integrate into any IDV platform via ROC SDK.

Voxmind

voxmind.ai
contact@voxmind.ai

Voxmind is a UK-based AI voice biometrics company founded in 2024, specializing in speaker authentication and deepfake voice detection. Its patent-pending phoneme-frequency extraction engine analyses vocal tract biomechanics to verify identity and detect AI-generated or cloned voices, delivering language-agnostic security by design, not by training on individual languages. Because detection operates at the phoneme-frequency level, analyzing vocal biomechanics rather than language-specific patterns, accuracy is consistent across any language and accent without retraining.

In the telephony channel specifically, voice deepfakes are overtaking traditional social engineering as the primary attack vector. Voxmind's voice biometric SDK is embedded via OEM agreement into enterprise IP phone hardware for a global unified communications provider, and the company is engaged with U.S. community banks seeking real-time deepfake detection to protect high-value wire transfer authorization over phone channels.

On the ASVspoof 2021 Logical Access benchmark – the standard academic benchmark for audio anti-spoofing evaluation – Voxmind's anti-spoofing engine achieves 0.78 percent Equal Error Rate (EER, measuring the threshold at which false acceptance and false rejection rates are equal). On the Deepfake track, it scores 2.65 percent. Those numbers put it below published baselines for both categories.

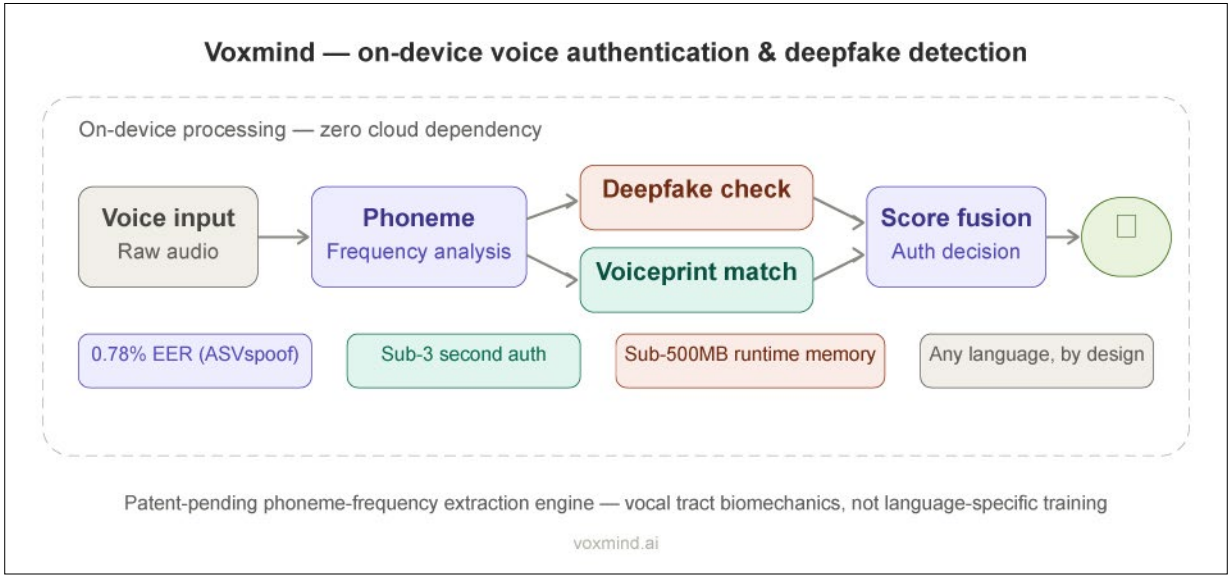
Formal standards for audio deepfake detection remain nascent compared to face, ISO/IEC 30107 covers presentation attack detection but was designed primarily for visual biometrics. This creates both risk and opportunity. For buyers, the absence of standardized audio benchmarks makes vendor evaluation harder and favours vendors who can demonstrate verifiable security posture. Voxmind is pursuing ISO 27001 certification and SOC 2 Type II readiness independently, so prospects can evaluate documented controls rather than relying on self-reported accuracy claims alone.

Voxmind SDK Powers Voice Login on Enterprise IP Phones

A global unified communications provider needed to add voice-login authentication to its enterprise IP desk phone range; enabling users to unlock their phone with their voice instead of a PIN. The challenge was substantial: the SDK had to target sub-500MB of runtime memory on constrained phone hardware, authenticate speakers in under three seconds, detect deepfake and cloned voices in real time, and work in any language without per-language model training.

Traditional voice biometric approaches require large cloud-hosted models and are typically trained per language. Neither constraint was acceptable for an on-device deployment spanning global enterprise customers.

Voxmind's patent-pending phoneme-frequency extraction engine solved both problems simultaneously. Because the engine analyses vocal tract biomechanics; the physics of how a speaker's anatomy shapes sound, rather than language-specific acoustic patterns, it is language-agnostic by design. A single model serves any language without retraining.



And because phoneme-frequency analysis operates on compact spectral representations, the full authentication and deepfake detection pipeline fits within the device's memory envelope.

The SDK was embedded via OEM agreement into the provider's phone firmware across its enterprise desk phone line. Every voice-login attempt now runs speaker verification and deepfake detection concurrently, with the anti-spoofing engine achieving 0.78% Equal Error Rate on the ASVspoof 2021 benchmark, returning an authentication decision and a deepfake confidence score within three seconds.

For the provider, this delivers a hardware-differentiated security feature that no competitor currently offers native voice biometric authentication with built-in deepfake protection, targeting fully on-device processing with zero cloud dependency for the authentication decision.

Youverse

youverse.id
sales@youverse.id
Taguspark, Núcleo Central, 147
2740-122
Oeiras, Lisbon, Portugal

EU-based Youverse helps businesses and developers create safer digital experiences with proprietary biometric algorithms that power document checks, passwordless authentication, face matching, liveness detection and age estimation. From onboarding to login, Youverse's tools block deepfakes, protect data and give people control of their digital identity. Its customers include enterprises in banking, iGaming, hospitality and mobility.

Deepfakes are one of the fastest-growing fraud vectors, rising steadily alongside API-level injections and classic spoofs. In financial services, for example, deepfakes already rank among the top three methods. Yet document manipulation remains widespread, as seen by more than half of businesses, and screen-replay/printout spoofs still dominate facial attacks. Youverse chooses to treat all threats as priority risks and provide complete protection, covering presentation and injection attacks with liveness and injection defense by default.

Because the trend is steep: traditional forgeries still lead today, but deepfakes are closing the gap quickly. Relying on single-layer, L1-only artifact tricks is like locking the front door while the windows are open. Attackers have moved on to real-time, prompt-adaptive synthesis and API-level injections that skip the camera pipeline altogether. The defense needs to be multi-layered and combined with quality standardized compliant solutions like Level 1 & 2 as well as CEN/TS 18099-conformant injection defense, securing the capture path end-to-end. The combination of multiple defenses becomes much more than the sum of the parts.

Youverse's liveness detection engine is compliant with ISO/IEC 30107-3 (Level 1 & 2) and designed to be conformant with CEN/TS 18099 to detect presentation and injection attacks, including deepfakes. It stores no biometric templates or PII. Face matching performance is validated against independent NIST benchmarks with False Rejection Rate from as low as 0.3 percent for False Acceptance Rate of 1 in 1 million.

Youverse's Liveness Detection API can be used standalone or alongside other companies' APIs such as age estimation, document verification, and more. Pricing is transparent and volume-based, with plans starting at 99 euros per month, so teams can start small, validate quickly and scale without heavy upfront commitments.

How a gambling operator beat bots and deepfakes

A fast-growing EU gambling operator was hit by identity abuse on two fronts: screen-replay spoofs during sign-up/age checks and a rising trickle of real-time deepfakes during high-value withdrawals and bonus abuse rings. Manual reviews were piling up, withdrawal SLAs were slipping, and compliance was worried about privacy exposure under GDPR/AML.

They implemented Youverse Liveness Detection API on web, iOS, and Android, focusing on two flows: (1) first-time account creation and (2) step-up checks on risky events (suspicious logins, large withdrawals, payment method changes, and bonus redemption spikes).

Outcomes after 90 days

- 60% drop in successful impersonations at onboarding; 45% fewer multi-accounting attempts tied to bonus abuse.
- 48% reduction in successful account takeovers.
- Manual reviews are down by 35%.

Onboarding shifted to a risk-based model: passive detection was the standard, and active liveness detection was triggered when something drifted. For money movement, they added step-up checks on cash-out and payment events so that liveness kicked in for large or rapid withdrawals, new payment instruments, and other high-risk transactions. Promotions had the same logic, with liveness gating high-value bonus redemptions and accounts flagged as part of suspected multi-account clusters. The net effect was fast UX, tighter risk controls, and simpler audits spanning AML, KYC/age verification, and responsible-gaming obligations.

Deepfake Detection Vendors Directory

1

1Kosmos

1kosmos.com

1Kosmos is a private company founded in 2017 and headquartered in East Brunswick, New Jersey, USA. The company specializes in digital identity proofing and passwordless authentication solutions, combining advanced biometrics with blockchain technology.

By actively identifying and thwarting injection attacks in real time, 1Kosmos' LiveID+ offers robust protection against the deceptive tactics of deepfakes.

A

Accura Scan

accurascan.com

Accura Scan is a global biometrics firm since 2019 with offices in India, Singapore, USA, Europe and the Middle East. It is a fintech and regtech ai-based global user verification company.

Accura Scan's cutting-edge deepfake detection capabilities leverage motion and texture analysis, alongside AI anomaly detection, to unmask AI-generated impostors in real-time.

AU10TIX

AU10TIX.com

AU10TIX is a private company founded in 2002 as a subsidiary of ICTS International. Headquartered in Amsterdam, The Netherlands, the company specializes in automating the verification of identity documents and biometrics to combat fraud and streamline customer onboarding processes.

Its multi-layered deepfake detection solution spots hard-to-catch GAN-generated fakes regular identity verification systems miss to beat fraudsters.

Aurigin.ai

aurigin.ai

Aurigin is a startup founded in 2024 and headquartered in Zurich, Switzerland. Its expertise originates from Sennheiser, McKinsey, ETH, and EPFL, blending audio heritage with cutting-edge AI research.

Aurigin delivers market-leading detection of AI-generated content,

synthetic speech, and deepfakes with 98%+ accuracy, real-time performance (<50ms latency), and integration in <3 lines of code. Offered as an API and SaaS, it enables endpoint protection, fraud prevention, and defense against misinformation.

AuthenticID

authenticid.com

AuthenticID specializes in identity safety through verification solutions. Founded in 2001 and headquartered in Washington, USA, it provides automated, AI-powered systems designed to verify an individual's identity quickly and accurately.

AuthenticID delivers deepfake detection technology to stop synthetic media attacks whether they are manipulated documents, images, or videos.

authID

authid.ai

authID Inc., formerly known as Ipsidy Inc., was founded in 2009 and is headquartered in Denver, Colorado, USA. The company specializes in providing secure, biometric identity verification and passwordless authentication solutions for both consumer and workforce applications worldwide.

authID.ai integrates liveness detection into its biometric authentication solutions to ensure that the individual being authenticated is physically present and not using fraudulent methods such as deepfakes.

Aware

aware.com

Aware is a global biometric platform company that uses data science and machine learning to tackle everyday business and identity challenges through biometrics for over 30 years.

Its Awareness Platform includes injection detection, active and passive liveness, and emerging deepfake countermeasures.

B

BioID

bioid.com

BioID GmbH is a private company founded in 1998, originating from a research project at the German research institute Fraunhofer IIS and headquartered in Nuremberg, Germany. BioID specializes in biometric authentication software, offering services such as facial recognition, certified liveness detection, and periocular recognition.

BioID's deepfake detection software secures digital identity verification from fraud, discerning whether a face found in an image or video is a deepfake, AI-generated or AI-manipulated.

C

Corsound AI

corsound.ai

Corsound AI is headquartered in Tel Aviv since 2020 and offers advanced voice intelligence and real-time AI-driven solutions.

Its technology decodes voice to identify deepfake fraud and verified individuals, at any scale.

D

Daon

daon.com

Daon is a private company founded in 2000 and headquartered in Fairfax, Virginia, specializing in biometric

authentication and identity assurance solutions. With additional operations in Dublin, Ireland, and regional offices in Serbia and Australia, Daon has a global presence in the identity verification and authentication sector.

The company offers advanced presentation attack detection (liveness) to prevent bypass with images, videos, masks or deepfakes. With use cases in financial services, government services, healthcare, telecom, travel and hospitality, Daon employs a number of tools to defend against the misuse of deepfake technology.

Deep Media

deepmedia.ai

Deep Media is a Media Intelligence platform company in San Francisco that protects consumers, creators, governments, and enterprises from synthetic media threats including deepfakes, impersonation, misinformation, and content manipulation.

The company offers a high-accuracy, scalable detection and media intelligence platform to enterprises and governments, to help protect against deepfakes and unethical AI.

Deepfake Detector

deepfakedetector.ai

Deepfake Detector is based in London, UK and offers an AI tool that can identify if an audio or video is a deepfake or real.

The solution provides a reliable means to filter out AI-generated content, offering probabilities as an initial guide for further investigation.

DuckDuckGoose

duckduckgoose.ai

DuckDuckGoose is one of the first companies worldwide dedicated exclusively to deepfake and GenAI content detection. Founded in 2020 and headquartered in the Netherlands, the company works with governments, financial institutions, and technology providers across multiple continents.

Its proprietary technology detects AI-generated and manipulated content in images, video, and audio with over 95% accuracy and a 0.1% false rejection rate. The DuckDuckGoose API integrates seamlessly into identity verification, authentication, and other security-critical processes.

F

Facia.ai

facia.ai

Facia.ai is a private company founded in 2022 and is headquartered in London, UK. The company specializes in biometric authentication systems, offering AI-powered 3D facial recognition and liveness detection technology designed to identify and verify individuals worldwide.

Facia's platform helps prevent fraud and identity theft by protecting against spoofing attacks, including deepfakes, and is utilized across various industries such as banking and financial services, healthcare, government, and education.

G

GBG

gbg.com

Founded in 1989, GBG's history in identity verification began in 2002. The company is headquartered in London, UK and is a London Stock Exchange listed company. GBG offers document and biometric security to

protect remote identity proofing from deepfakes and forgeries.

Certified passive liveness testing protects biometric verification against presentation attacks to the highest ISO/IEC standard. Its authentication and biometric verification delivers protection from identity fraud at every step, including biometric security to detect deepfakes, forgeries and impersonation.

I

ID R&D

idrnd.ai

ID R&D was founded in 2016 and is headquartered in New York City, New York, USA. In 2021, ID R&D was acquired by publicly traded Mitek Systems, a provider of digital identity verification solutions.

The company has performed extensive research on detecting deepfakes and injection attacks with its PAD technology. It was awarded a patent in 2023 for a new approach to detecting voice-based spoofing and deepfake attacks and in 2024 introduced a voice clone detection tool.

ID Dataweb

iddataweb.com

Virginia-based ID Dataweb is focused on preventing account takeovers and safeguarding users without compromising experience.

Its platform automatically identifies risky behavioral and environmental signals to secure businesses from threats such as deepfakes.

Idemia

idemia.com

France-based biometrics leader Idemia is at the center of an initiative to develop a deepfake detection toolkit for the government of France.

Idemia offers robust biometric liveness detection technology that is designed to resist deepfake-style spoofing (such as video or synthetic media).

IDVerse

idverse.com

IDVerse, formerly known as OCR Labs Global, is a private company founded in 2014 and is headquartered in London, UK with additional offices in Sydney, Australia, and Silicon Valley, USA. IDVerse specializes in AI-powered identity verification solutions, offering services such as biometric verification and face authentication. In December 2024, LexisNexis Risk Solutions announced a definitive agreement.

IDVerse's Deepfake Defender product is trained on AI-generated fraudsters and can detect micro anomalies to precisely assess human liveness. It works cross-platform with Android and iOS and is not hardware-dependent.

iiDENTIFii

iidentifii.com

iiDENTIFii was founded in 2018 and is headquartered in Cape Town, South Africa. It offers a digital identity verification solution.

It proves biometric liveness, facial verification, and validates data through secure triangulated authentication. It claims its technology is resilient to deepfake and digital replay attacks.

Incode

incode.com

Incode Technologies Inc. is a private company founded in 2015 and is

headquartered in San Francisco, California, USA. Incode specializes in AI-driven identity verification and authentication solutions. Its platform is utilized by industries including financial services, government, retail, hospitality, and healthcare, enabling customers to validate their identity using facial biometrics and government-issued IDs through web or mobile applications.

Incode's passive liveness technology detects and prevents fraud by identifying physical spoofs such as AI-generated deepfakes using advanced proprietary ML models and in-house AI.

Innovatrics

innovatrics.com

Innovatrics is a private company founded in 2004 and is headquartered in Bratislava, Slovakia. The company specializes in biometric solutions, offering products such as Automated Biometric Identification Systems (ABIS), digital onboarding toolkits, facial recognition platforms, and fingerprint and facial recognition algorithms.

Innovatrics' Video Injection Detection offers a robust solution by authenticating camera feeds directly. This approach protects against both video injection and man-in-the-middle attacks, keeping customers' identity verification process safe from deepfakes and fake identities.

iProov

iProov.com

iProov is a private company founded in 2011 and is headquartered in London, UK. The company specializes in biometric facial verification technology, providing solutions for secure online identity verification and authentication.

iProov offers a layered approach to injection attack and deepfake detection effective against sophisticated attacks.

J

Jumio

jumio.com

Jumio is a private company founded in 2010 and headquartered in Sunnyvale, California, USA. Jumio specializes in digital identity verification and authentication services, utilizing technologies such as artificial intelligence, biometrics, machine learning, and liveness detection.

Its solutions help organizations across various sectors, including financial services, digital currency, retail, travel, and online gaming, to onboard customers quickly, prevent fraud, and comply with regulatory requirements. Jumio validates the user's ID, corroborates it with a selfie and uses advanced liveness detection to ensure the person is actually present, not a deepfake.

K

Keyless

keyless.io

Keyless is a privacy-preserving biometric authentication technology firm with offices in the UK, Italy and Singapore.

The company recently launched its new injection attack detection capability, protecting businesses such as banks, fintechs, cryptocurrency platforms, and other high-risk industries from deepfake-driven attacks.

Kroop AI

kroop.ai

India's kroop AI provides a deepfake detection solution that identifies synthetic manipulations in videos, images, and audio.

The company claims to protect against misinformation, fraud, and identity misuse. Its solution is suitable for diverse use cases, ensures authenticity and safeguards reputations.

M

Mitek

miteksystems.com

Mitek Systems, Inc., established in 1986, is a publicly traded company headquartered in San Diego, California. Its toolkit includes passive liveness detection techniques to ensure that a user is physically present during the verification process.

It recently integrated Digital Fraud Defender (DFD) into its Mitek Verified Identity Platform (MiVIP), combining Mitek's proprietary biometric liveness with analysis of the content and channel of communications for signs of manipulation to protect against deepfakes, synthetic identity fraud and account takeovers.

Mobai

mobai.bio

Mobai, founded in 2019, is headquartered in Gjøvik, Norway. The company specializes in biometric face verification solutions, focusing on facial recognition, presentation attack detection, liveness detection, and morphing (deepfake) detection.

Its services are designed for identity verification and authentication for service providers in regulated markets, such as financial services.

N

Nametag

getnametag.com

Nametag was founded in 2020 and provides integrated identity verification and account protection solutions. The company is headquartered in Seattle, Washington.

With its Deepfake Defense product using advanced cryptography, biometrics and AI, Nametag detects and blocks sophisticated attacks.

O

Oz Forensics

ozforensics.com

Oz Forensics, founded in 2017, is headquartered in Dubai, United Arab Emirates and was acquired by Unico, a Brazilian ID company, in September 2024.

Oz Forensics specializes in biometric and deepfake identity fraud prevention, offering solutions such as liveness detection and biometric verification to both private and public organizations globally.

P

Paravision

paravision.ai

Paravision, founded in 2013, is headquartered in San Francisco, California and specializes in advanced computer vision technology focusing on the ethical development of software

related to face biometrics, including passive, single-frame face liveness and deepfake detection.

The company's deepfake detection technology was developed over a multi-year collaboration with a Five-Eyes government. Its offerings are utilized across various sectors, including digital identity verification, government programs, travel and border security, stadiums and events, automotive, payments and retail, and physical security.

Persona

withpersona.com

Founded in 2018, Persona is headquartered in San Francisco and is available in 200+ countries and territories and 20 different languages. Persona serves any business that needs to verify its customers online.

Persona's identity verification solutions, such as liveness detection, help combat threats such as deepfakes by ensuring the authenticity of user identities.

Pi-labs

pi-labs.ai

pi-labs is an Indian-based cybersecurity and intelligence solutions firm specializing in deepfake detection, blockchain-backed evidence management, and forensic video analytics.

Its Authentify solution is a deepfake detection engine using AI++ techniques to eliminate deepfakes from the Internet and is used by law enforcement agencies, intelligence teams, and cybersecurity firms.

Pindrop

pindrop.com

Pindrop, a privately held company headquartered in Atlanta, GA, was founded in 2011 and is venture-backed.

Pindrop prevents fraud through cutting-edge voice authentication and deepfake detection technologies. Its solutions identify and mitigate threats in real time. Its proprietary, text-independent voice biometric engine passively identifies legitimate and fraudulent callers by voice alone.

Polyguard

polyguard.ai

Polyguard is a New York-based firm founded in 2024 and is focused on anti-fraud technology with its real-time deepfake detection tool.

It delivers proactive protection against call spoofing, hijacking, and impersonation for voice, video, and messaging in the call centers. Its 3D facial recognition and hardware attestation blocks digital fakes and device tampering.

R

Reality Defender

realitydefender.com

Reality Defender is headquartered in New York City and was founded in 2021. The company secures critical communication channels against deepfake impersonations in real time and at scale.

Its multimodal solutions detect AI impersonations across any multimedia format, enabling automated alerts and flexible deployment options across the tech stack. Its enterprise-grade

API and web app detects AI-generated and manipulated content across audio, video, images, and text.

ROC

roc.ai

ROC, established in 2015, is headquartered in Denver, Colorado and specializes in developing advanced biometric and computer vision solutions, including facial recognition, fingerprint recognition, iris recognition, and object detection.

ROC offers software to detect deepfakes and biometric injection attacks that bypass traditional liveness detection technologies. Camera Injection Attack Detection draws on proprietary algorithms to identify the unique digital signatures left by deepfakes, virtual cameras, face emulators and other synthetic inputs.

S

Sensity

sensity.ai

Sensity AI, founded in 2018, is headquartered in Amsterdam, Netherlands. The company specializes in developing advanced cybersecurity technologies aimed at detecting and combating AI-generated threats, particularly deepfakes.

Its platform offers comprehensive detection tools for videos, images, audio, and identities, serving sectors such as law enforcement, KYC vendors, social media platforms, and defense agencies. Its solutions identify AI-generated content that can compromise facial recognition and liveness checks.

Socure

socure.com

Socure, established in 2012, is a private firm headquartered in Incline Village, Nevada, USA, with a regional office in Chennai, India.

Socure's liveness detection solutions include deepfake detection and injection attack detection capabilities. The company serves the financial services, government, gaming, healthcare, telecom, and e-commerce industries.

T

Thales

thalesgroup.com

Thales is a global leader in cybersecurity and is headquartered in Austin, Texas. Its deepfake detection metamodel addresses the problem of identity fraud and morphing techniques.

Thales's AI accelerator cortAIx, developed a metamodel capable of detecting AI-generated deepfakes. The Thales metamodel is built on an aggregation of models, each of which assigns an authenticity score to an image to determine whether it is real or fake. The company offers a range of solutions to enhance security measures against deepfakes in digital onboarding for banks and financial institutions.

U

Unissey

unissey.com

Unissey, founded in 2018, is headquartered in Paris, France and specializes in AI-driven facial biometric identity verification solutions.

Unissey has developed a remote identity verification solution using facial biometrics to fight against deepfakes using media-agnostic technology that analyzes the entire environment to detect signs of an attack.

W

World

world.org

Tools for Humanity is the parent company of the World (formerly Worldcoin) project. It is a global technology company building open-source solutions to empower individuals and communities.

Deep Face uses World ID authentication to protect against malicious deepfakes online. Built for real-time communication, Deep Face lets you confirm that the person you're speaking with is a real human, not a deepfake. The other person can easily prove they're not a deepfake in a few steps using face authentication. Anyone can create a Deep Face request in World App. To respond to a Deep Face request, you need World App and an Orb-verified World ID.

Y

Youverse

youverse.id

Youverse was founded in 2019 as YooniK before rebranding in 2023. It is a private company headquartered in Lisbon, Portugal.

YouAuth is a decentralized authentication solution with deepfake detection utilizing a zero-knowledge architecture for enhanced privacy protection.

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS