UNICO BIOMETRIC UPDATE.COM

Authenticity vs. Deepfake:

Who Validates What's Real?

Insights from hundreds of millions of identity verifications by Unico

What are deepfakes?

Many incredible moments in hit Hollywood movies, like stars appearing as their younger selves, or playing two different characters within the same scene, were made possible with the development of **AI** technology. The same kind of technology that enabled these memorable scenes is now widely available, and being put to a more nefarious use.

Deepfake images can manipulate how a person's face appears, place a fabricated face onto an identity document, or even generate the likeness of someone who does not exist. As a result, they have become an increasingly common tool in online fraud attacks. While businesses across many industries have been targeted with deepfake-enabled fraud, organizations that provide higher-value services—particularly those granting access to financial accounts, such as financial institutions, retail platforms, and online gambling services—are especially frequent targets.

The problem is further amplified by the widespread availability of **generative AI** tools. Today, an online criminal no longer needs deep expertise in artificial intelligence or digital imaging to produce convincing deepfakes and launch attacks against businesses.

Movies are now real life.

How fraudsters use AI to outsmart biometric engines

As generative AI tools become more accessible, fraudsters are rapidly expanding the range of techniques used to bypass identity verification systems. Deepfakes now play a central role in many of these attacks, enabling criminals not only to impersonate real individuals but also to create entirely new identities or coordinate more complex fraud schemes. These methods often combine **synthetic media** with broader operational strategies designed to exploit weaknesses in identity verification workflows.

The cases described below are not necessarily the most common forms of fraud. Rather, they illustrate how attackers are increasingly demonstrating a deeper technical understanding of identity verification technologies and the defenses designed to protect them. These examples highlight emerging techniques observed by Unico's analysts and provide insight into how sophisticated fraud is evolving.

Deepfakes can be used to manipulate either an identity document or the selfie typically compared against that document during identity verification. Because these attacks rely on advanced technologies and are often deployed as part of a broader strategy to bypass the defenses implemented by the target system, they are classified by Unico specialists as **Sophisticated Fraud**.

Impersonation attacks are a well-known fraud type. A common example of this kind of attack is when a person receiving a government benefit (such as a pension) dies, and one of their relatives assumes their identity to continue collecting the payments.

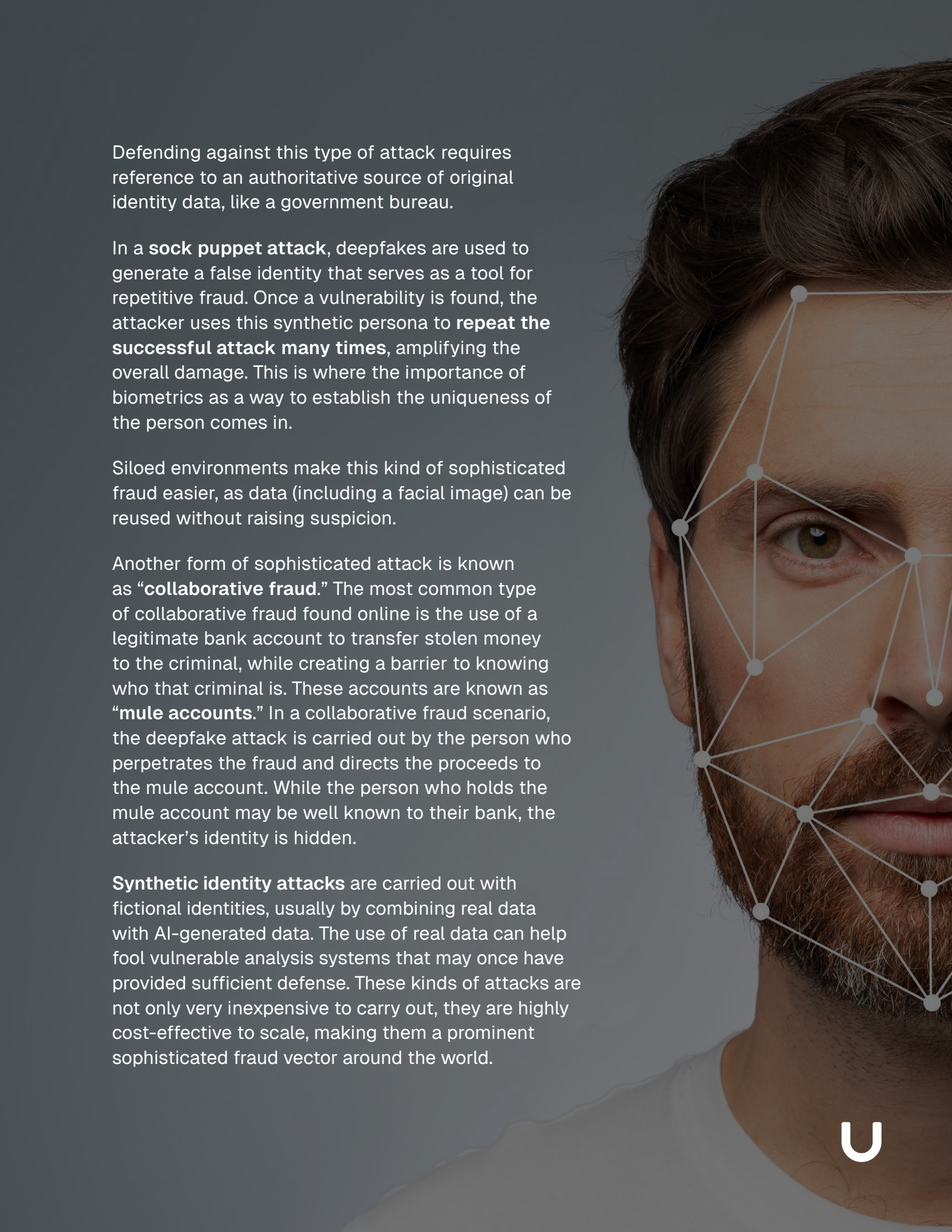
Defending against this type of attack requires reference to an authoritative source of original identity data, like a government bureau.

In a **sock puppet attack**, deepfakes are used to generate a false identity that serves as a tool for repetitive fraud. Once a vulnerability is found, the attacker uses this synthetic persona to **repeat the successful attack many times**, amplifying the overall damage. This is where the importance of biometrics as a way to establish the uniqueness of the person comes in.

Siloed environments make this kind of sophisticated fraud easier, as data (including a facial image) can be reused without raising suspicion.

Another form of sophisticated attack is known as "**collaborative fraud**." The most common type of collaborative fraud found online is the use of a legitimate bank account to transfer stolen money to the criminal, while creating a barrier to knowing who that criminal is. These accounts are known as "**mule accounts**." In a collaborative fraud scenario, the deepfake attack is carried out by the person who perpetrates the fraud and directs the proceeds to the mule account. While the person who holds the mule account may be well known to their bank, the attacker's identity is hidden.

Synthetic identity attacks are carried out with fictional identities, usually by combining real data with AI-generated data. The use of real data can help fool vulnerable analysis systems that may once have provided sufficient defense. These kinds of attacks are not only very inexpensive to carry out, they are highly cost-effective to scale, making them a prominent sophisticated fraud vector around the world.



How do criminals create and use deepfakes?

AI tools have made it possible for anyone to create deepfakes. Open source tools, APIs and **deepfake-as-a-service** subscriptions make powerful technology widely available and affordable to criminals.

In some cases the deepfake face may be created from scratch by the attacker using these generative AI tools, but in the majority of cases, such as in impersonation attacks, a source image is used. While earlier versions of generative AI required several images or a video to create a deepfake that can perform actions – such as to defeat active liveness detection -- a **single photo** is now sufficient. The tools that have made deepfakes easier to create and use also make it easy for hackers to script appropriate responses, or even complete them in real-time.

According to Unico's fraud detection specialists during their 2025 audits, deepfake attackers will often use specialized hardware tools, like curved monitors, to avoid the flatness that gives away images presented on a flat screen. Similarly, some attackers have even been seen combining mirrors in their setups to mask that the image is synthetic and fool algorithms that detect skin texture.

Unico's specialists identified that while attackers often use tripods for stability, only advanced fraud protection systems flag the total absence of **micro-movements** as a clear indicator that a human is not holding the device.

In some cases, attackers use a high-definition projector or other phones to present the deepfake to the camera, which is known as a **presentation attack**. Other kinds of presentation attacks include high-quality latex masks. These kinds of masks are very difficult to detect, but are also expensive to produce and can spoof only one face.

Deepfakes are also delivered through **injection attacks**, which bypass the camera of the hacked device to deliver the image. Injection attacks represented over 45% of the fraud attempts stopped by Unico's liveness detection in 2025.

In **morphing (or "blending") attacks**, the face of the attacker is blended with that of another person. If effective, the resulting face can match the biometrics of both the attacker and the victim, while still passing a liveness check. Morphing attacks are also often delivered through injection.

In a **partial injection attack**, the criminal breaks into the back-end processes of the phone to modify code. This allows them to present their own face to the camera, and therefore pass liveness detection, but then swap the victim's face into the image or video.

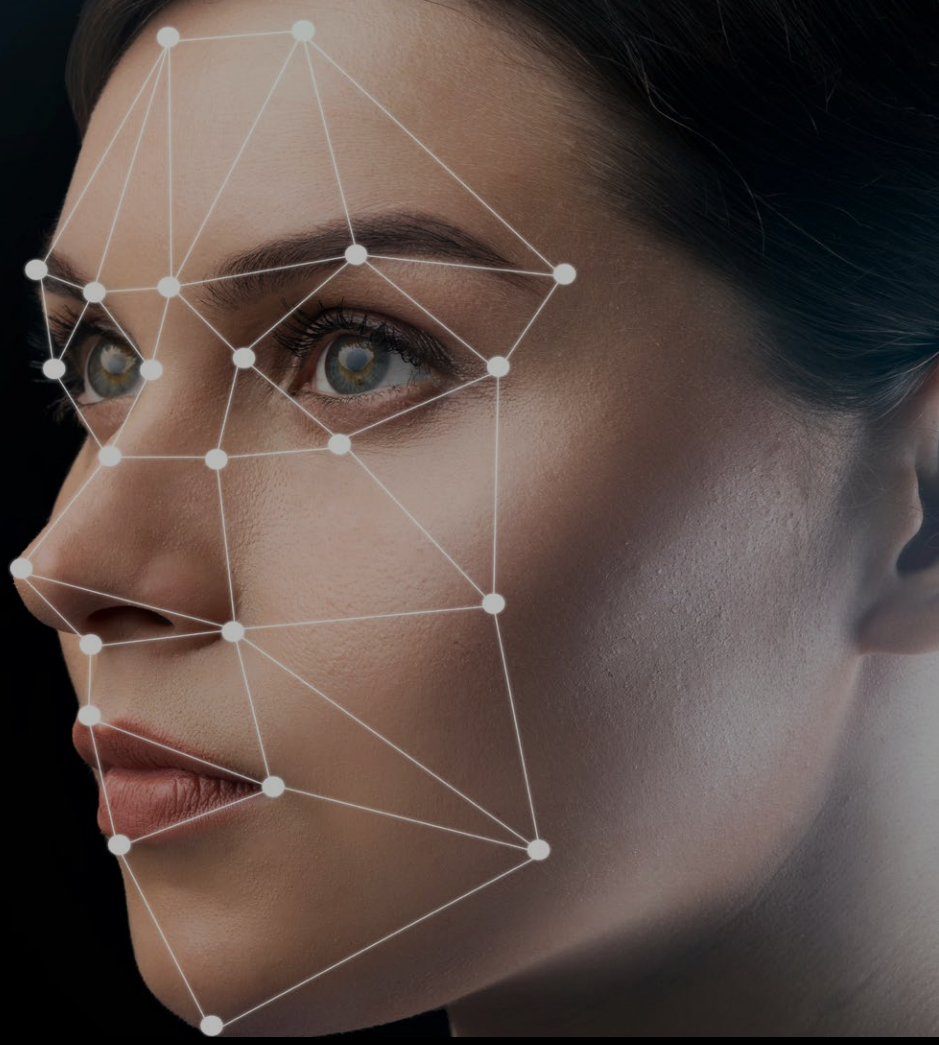
Deepfake defenses

Biometrics are the most reliable and easiest way to establish the uniqueness of an individual online. But deepfakes erode the trustworthiness of biometrics, forcing organizations to include robust liveness detection to ensure the biometric is provided directly by the person presenting the identity claim.

Liveness detection is often misunderstood, and is not carried out by spotting lighting mismatches or lip-synching errors.

Cryptographic proofs are sometimes applied to content to provide assurance of the source it comes from. But jailbroken devices can spoof the cryptography, providing false assurance of the data's reliability.

The only way to be sure of the legitimacy of the data is to control the environment in which it is captured.



Impersonation attacks can be detected by referring to **authoritative government sources**, like civil registries or tax numbers. Identity verification providers can also detect deepfakes by building their own registries, which can be used to catch signs of manipulation like frequently-repeated identical backgrounds in images.

Once strong liveness detection is in place, including **control of the capture environment**, the most important method for detecting incoming deepfake fraud attacks is to closely observe and learn lessons from real-world attacks as they are carried out.

The millions of identity verifications performed each year by Unico provide a wealth of knowledge about what kinds of deepfakes attacks organizations are experiencing and how they can be spotted.

How Unico's software fights deepfake fraud

Unico has blocked more than 1 million fraud attacks just with their liveness detection capabilities using its **comprehensive defense strategy**, while granting more than 100 million people access to their accounts and services.

Unico's **planet-scale** proprietary biometrics engine, works with the best liveness detection in the world, developed by Unico subsidiary Oz and proven compliant with the international standard for presentation attack detection through independent evaluation. It is capable of processing over 1 billion faces in under a second.

The software checks not just that the user's face matches their identity number, but that neither the ID nor the facial image has been replaced or tampered with. It also checks if the same face has been previously linked with another identity, by referring to **Unico's own registry** of fraud and identity data.

The Unico IDCloud platform also controls the capture environment to prevent attackers from injecting deepfakes into the data stream.

Unico combines these biometric technologies with a fraud decision engine that integrates government data sources, device signals like location and IP address, and hundreds of other risk signals.

The result is robust protection against the full range of sophisticated fraud and deepfake attacks which are plaguing businesses and governments around the world.

Forged in the heat of battle: Real-world know-how

Unico's expertise is forged on the front lines, combining state-of-the-art technology with real-world battlefield knowledge rather than relying solely on laboratory simulations.

Throughout 2025, Unico observed Brazil becoming a global epicenter for sophisticated fraud, with attack attempts skyrocketing by **1,082%** in a single year—an escalation detailed in our monthly evolution data.

This surge is fueled by the collapse in entry costs, where attacks that once required specialized hardware costing over **$1,000** are now executed with tools and "Fraud-as-a-Service" subscriptions costing as little as **$6**.

Unico Research (2024-2025). Data based on proprietary analysis of AI-accelerated fraud attempts and market projections.

State-of-the-art technical defense

To stop these evolving threats, Unico implements a multi-layered defense powered by **three orthogonal engines** working simultaneously to eliminate single points of failure, achieving a **99.7% conversion rate** with a **0% False Acceptance Rate (FAR)** in controlled environments. To defeat Injection Attacks (IAD), we utilize **RASP (Runtime Application Self-Protection)** embedded within the SDK to secure the app's perimeter, while their **liveness detection** engine is certified under the **CEN/TS 18099** international standard.

For Presentation Attacks, the system analyzes **volumetry** to identify the flatness of curved monitors and performs high-granularity analysis of skin texture and micro-expressions to detect ultra-realistic masks or mirrors. This entire ecosystem operates under a **24/7 monitoring and reaction protocol**, allowing Unico to identify and neutralize new bypass vectors in less than a day.

Agile evolution through strategic partnership

Unico operates as a live laboratory, constantly monitoring the shifting landscape of fraudster behavior and emerging attack patterns in real-time. This deep field visibility is shared with our technology partner, OZ Forensics, who develops our world-class liveness detection engine. By working in close synergy with a partner that owns the core technology, we achieve significantly higher reaction power and agility. This unique collaboration allows us to evolve our defenses as fast as the frauds themselves, deploying specialized updates that neutralize synthetic threats before they can scale across the market.

Want to know more about Unico solutions visit: Unico.io