

How Identity.io is Redefining Identity Protection in the Age of AI-Driven Fraud

Identity.io highlights its multi-layer approach to combating AI-driven identity fraud through injection attack prevention, deepfake detection, multimodal biometrics, and on-device authentication.

DOVER, Del., June 23, 2026 — [Identity.io](#), leading international company in touchless biometric identification and digital credential management solutions, has been featured in the newly released 2026 Injection Attack Detection Market Report & Buyer's Guide, published by Biometric Update in partnership with Goode Intelligence. The report examines the growing threat of injection attacks, a rapidly evolving form of biometric fraud in which attackers bypass biometric capture devices and insert manipulated, synthetic, or AI-generated content directly into identity verification workflows. As organizations increasingly adopt remote onboarding and [biometric authentication](#), injection attack detection (IAD) is emerging as a critical layer of identity assurance and fraud prevention.

In this context, Identity.io highlights how the fraud landscape has evolved beyond traditional presentation attacks involving printed photos, screens, or masks. Today, attackers can combine camera injection techniques with AI-powered deepfake generation to create highly convincing biometric forgeries capable of bypassing conventional liveness and presentation attack detection systems. To address this challenge, Identity.io has developed a defense strategy based on two independent security layers. The first focuses on injection attack prevention, protecting the integrity of the biometric capture pipeline by ensuring that biometric samples originate from a genuine physical camera and trusted execution environment. The second layer leverages passive liveness detection together with deepfake detection techniques to analyze biometric content, helping organizations verify the presence of a genuine user while identifying signs of AI-generated, manipulated, or synthetic facial imagery.

These complementary controls are designed to provide defense-in-depth against increasingly sophisticated attacks, ensuring that compromising one layer does not automatically compromise the other. [Identity.io](#) also emphasizes the importance of multimodal biometrics as a long-term response to the growing exposure of facial biometric data. With billions of facial images publicly available online, face biometrics have become a primary target for identity fraud. To strengthen identity assurance in high-security use cases, Identity.io enables fingerprint capture using standard smartphone cameras, adding an additional biometric factor that is significantly more difficult for attackers to obtain and replicate at scale.

Beyond addressing specific attack vectors, Identity.io views biometric security as a cornerstone of digital trust. As digital interactions increasingly replace in-person verification, organizations must ensure that users can prove their identity securely while maintaining control over their personal data. By combining advanced biometric technologies with reusable digital credentials, Identity.io helps organizations strengthen identity protection throughout the entire user journey, from onboarding and authentication to ongoing account access and transaction approval.

The company also believes that effective fraud prevention requires multiple layers of protection working together rather than relying on a single authentication factor. This is where multimodal biometrics plays a critical role. By combining facial biometrics with fingerprint authentication captured through standard smartphone cameras, organizations can significantly increase resilience against identity fraud while improving trust in digital services. This layered approach helps reduce the risk of account takeover, synthetic identity fraud, and AI-driven impersonation attacks, providing stronger security for both businesses and end users.

The report also discusses architectural approaches to [biometric authentication](#). In this regard, [Identy.io](#) outlines the advantages of performing biometric matching directly on the user's device rather than relying exclusively on centralized server-side comparisons. By executing the authentication process locally and matching against biometrics stored on the device, organizations can significantly reduce the feasibility of large-scale remote attacks. Traditional server-centric architectures create an environment in which any connected device can capture and submit biometric data for verification against centrally stored templates, increasing the potential attack surface. In contrast, a match-on-device approach requires the authentication process to take place on the specific device where the user's biometric credentials are registered. This architecture limits opportunities for remote manipulation and makes large-scale fraud campaigns considerably more difficult to execute.

As stated by Jesús Aragón, CEO of Identy.io, "The inclusion of Identy.io in this report reflects the work we have been doing to stay ahead of the rapidly evolving threat landscape driven by AI-generated fraud. As deepfakes, camera injection attacks, and synthetic identities become increasingly sophisticated, organizations need more than traditional liveness checks. Our approach combines injection attack prevention, passive liveness detection, deepfake detection, multimodal biometrics, and on-device authentication to provide a stronger foundation for digital trust and identity assurance."

As injection attacks and AI-generated identity fraud continue to evolve, Identy.io continues strengthening the integrity of both biometric capture and biometric matching processes, which will be essential for organizations seeking higher levels of identity assurance. By combining on-device authentication with injection attack prevention, deepfake detection, and multimodal biometrics, the company aims to provide a more resilient framework for defending against emerging threats.

About Identy.io

Headquartered in the U.S. with offices in Brazil, Mexico, Colombia, Spain, and India, Identy.io is the global leader in digital identity verification using contactless mobile biometrics. At Identy.io, we believe in multi-factor authentication, while advocating for the need to replace traditional identity verification methods—such as passwords, tokens, or OTPs (One-Time Passwords)—which do not guarantee the user's identity.

At Identy.io, we work with institutions to ensure identity verification in their business processes through the use of contactless biometrics from users' mobile devices. Our physical authentication

(liveness) protection makes biometrics secure and deployable at scale. For more information, visit <https://identity.io>