Biometrics Institute Concepts and Solutions Report

Biometrics: Keeping it Real

March 2026 **Silver Jubilee edition** celebrating 25 years of Responsible Biometrics

Synthetic deepfakes, real consequences: safeguarding biometrics from AI-driven fraud.

Jean Fang Lead Consultant Digital Identity
Consult Hyperion, consulting by Fime

The rising tide of biometric deepfakes

Biometric factors have become the backbone of modern authentication and identity verification systems. In an era where digital identity is paramount, binding a user's unique biometrics to their identity is increasingly essential for secure onboarding and ongoing authentication. Identity proofing establishes the uniqueness and validity of an individual's identity through the identity verification (IDV) process, while authentication represents the process of establishing confidence that the person is the same individual who originally enrolled.

But as generative AI tools become widely accessible, the same technologies that enhance convenience now fuel an unprecedented wave of identity based fraud. Deepfakes in the form of synthetic audio, image, or video created using advanced AI tools have rapidly evolved from novelty threats to one of the most dangerous risks to biometric verification today. High profile incidents, such as the multi million dollar fraud involving a deepfaked CFO in a video conference, demonstrate that these threats are no longer theoretical but operational at scale. Experian's 2026 fraud forecast identifies deepfake impersonation as one of the world's top emerging threats, noting that over USD 12.5 billion in consumer fraud losses were recorded in 2024 alone, according to FTC data.

How deepfakes compromise biometric verification

Biometric deepfakes can originate through two primary approaches:

- Synthetic identities: the creation of entirely non existent personas using AI generated traits.
- Impersonation of legitimate users: whereby attackers recreate an existing individual's biometric traits to bypass the security check and gain access.

Either way, the deepfake media needs to be presented to the biometric verification system through a channel in order to compromise the process. We can categorize these into two main attack vectors, and each requires different defensive mechanisms.

Presentation attacks

Fraudsters display deepfake media directly to the biometric capture device. These attacks are not new, but their sophistication has grown, often without requiring significant expertise, due to the availability of AI tools. The shift toward real time video manipulation significantly lowers the barrier to bypassing weak or outdated liveness detection mechanisms.

Injection attacks

More severe, injection attacks bypass the built in camera or microphone used during the live capture process. Deepfake media is fed digitally into the biometric pipeline through:

- Virtual cameras or external sensors.
- Application hooking on compromised or rooted devices.
- Attacks on secure execution environments.
- Network based manipulation, including man in the middle or AI agent proxies.

As generative AI accelerates, additional layers of security controls in verification workflows must adapt to defend against unprecedented realism and automation in deepfake production.

Mitigating threats from deepfakes and system vulnerabilities

To deploy digital services leveraging biometric technologies that provide a resilient and trusted KYC, identity verification, or authentication process, organizations should adopt a holistic view when defining and evaluating deployment options, covering everything from individual components to the overall system architecture.

Biometric technology selection and qualification
Modern biometric systems need multilayered defenses, including:

- Advanced liveness detection mechanisms with different approaches, which may include active, passive, or challenge response methods.
- Security instrumentation to detect injection attempts or abnormal patterns.
- Internal and external testing to ensure resilience under various simulated attack conditions, from development and qualification teams to independent third party experts.
- Use of industry standards and compliance validation, such as ISO/IEC 30107 for presentation attack detection and emerging standards like CEN/TS 18099 and ISO/IEC AWI 25456 for injection attacks.

Multi factor strengthening

Deepfakes exploit single point biometric weaknesses. Defenses should therefore combine additional factors to increase the difficulty for fraudsters to compromise the full process. These may include cryptographic credentials with phishing resistant capabilities, device binding to ensure authentication originates from a trusted device, and behavioral biometrics, which are harder to synthesize convincingly.

Lifecycle based checkpoints

To counter the threat, defenses must span the full user lifecycle, from onboarding to account recovery, wherever biometrics are used. Key biometric checkpoints include:

- Enrollment and biometric binding: Ensuring the legitimate user is present at the start prevents downstream fraud.
- Authentication or identification: Depending on the use case and implementation, strong liveness checks and multimodal verification mitigate deepfake impersonation.
- Step up authentication: Critical for password resets or high risk transactions.
- Recovery procedures: Increasingly targeted by fraudsters, as they can lead to account takeovers with greater impact.

Different use cases require different assurance levels. High risk financial or governmental workflows demand more robust biometric and device based controls.

Strengthening governance and reinforcing reliability

Deepfakes pose a systemic threat. Effective mitigation requires robust governance as much as technology. While regulators are encouraging industries to leverage biometric technologies for remote identity verification and authentication, it is crucial for organizations to conduct comprehensive analysis and exercise caution as accountable parties when integrating biometric verification into their processes.

Deepfake driven biometric fraud is no longer a theoretical risk; it is a rapidly expanding, industrialized threat. With deepfake incidents increasing in key regions and biometric fraud attempts surging globally, defending digital identity verification requires coordinated action, robust testing, and alignment with recognized standards and regulatory enforcement. By adopting layered defenses across the user lifecycle and reinforcing biometric systems with advanced detection and security controls, organizations can stay ahead of increasingly sophisticated deepfake attacks.

fime × consult hyperion
consulting by fime

Making innovation possible.

Making the world work.

Payments | Smart mobility | Digital identity

Contact us at fime.com