Biometrics Institute Concepts and Solutions Report

Biometrics: Keeping it Real

March 2026

Silver Jubilee edition celebrating 25 years of Responsible Biometrics

Contents

1. Introduction 3
2. Amadeus: Responsible biometrics: why travel is the ultimate test 4
3. Attain Insight: Keeping It Real While Protecting Privacy: The Role of Anonymised Biometrics 7
4. Auraya: Validating Identity in the Era of AI: Why Continuous Monitoring and Ethical Defence Will Prevail 9
5. Aware: How Biometrics is Helping Solve the Digital Identity Trust Crisis 12
6. Biometix: openbq – Better biometrics, better outcomes 15
7. BixeLab: Proving Who's Real: Deepfakes, Injection Attacks, and Responsible Biometric Assurance 18
8. Brands Australia: Remote Identity Verification: Good Practices in Distributed Capture Environments 20
9. Cognitec Systems: Age Assurance for the Ages? 23
10. Entrust: Is AI outsmarting you? Deepfakes, Injection attacks, and the next generation of responsible biometrics 25
11. Facephi: The Last Mile of Seamless Travel: Empowering Passengers with Agent-based Biometric Consent 28
12. FaceTec: Videos Are No Longer Reliable Audit Evidence in the Deepfake Era 30
13. FACIA: Remote Identity Verification: Best Practices and Proven Solutions 32
14. Fime: Synthetic deepfakes, real consequences: safeguarding biometrics from AI-driven fraud 35
15. Fujitsu: From recognition to responsibility: strengthening live facial recognition through behavioural analytics 39
16. HID: The Future Is You: Biometric Trends That Will Redefine Identity in 2026 42
17. IDEMIA Public Security: Biometrics, Borders, and Travel: Is Seamless Travel Becoming a Reality? 45
18. IDEMIA Public Security: Deepfakes and Deception: Is AI Outsmarting Us? 47
19. Innovatrics: Beyond Face: Strengthening Remote Identity Verification with Palm Recognition 49
20. iProov: Virtual Camera Attacks: The Hidden Threat to Remote Identity Verification 51
21. Jumio: The Next Frontier: Reusable Identity at Scale 53
22. Paravision: Biometrics, Borders, and Travel: Is Seamless Travel Here? 55
23. Regula: Making Fraud Near-Impossible: Robust Remote Identity Verification 58
24. SAIC: A 'Real' Look at Evaluating Biometric and Identity Systems for Remote Identity 60
25. Signicat: From Static Images to Secure Identity: Why Video + NFC Is the Future 62
26. SITA: Factoring in The Human Factor 64
27. Speed Identity: From Counter to Kiosk: Scaling Live Enrolment with Automation 66
28. Thales: AI and Biometrics: The pathway to trusted identity in the age of deepfakes 68
29. Travizory: Biometrics, Borders, and Travel: Is Seamless Travel Here? 71
30. Trust Stamp: Biometric Security Modules: Enabling Proof of Humanness 73
31. Veridas: Real Identity in the Age of AI: Proving a Real Human on a Real Device 75
32. ZwillGen PLLC: All People May Be Created Equal; All Biometrics Are Not 77

1. Introduction

This Silver Jubilee edition of the 2026 Biometrics Institute Concepts and Solutions Report continues our commitment to exploring the practical and responsible application of biometric technologies. Building on the success of previous years, with our reports now having reached over 20,000 downloads, this latest instalment builds upon the core theme of our State of Biometrics Report by focusing on **keeping it real**. It provides a vital platform for our members to share the trends and solutions that are shaping the future of our industry.

In an era where the lines between the physical and digital are increasingly blurred, keeping it real is essential. As biometrics become more integrated into our daily lives, the focus must remain on authenticity, transparency, and the human impact. Public trust is the cornerstone of any successful implementation; therefore, maintaining robust controls and clearly defined governance is essential to ensuring these systems serve the public interest responsibly.

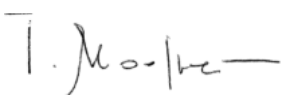
The submissions featured in this report represent the collective expertise of our global member community. They offer unique thought leadership, real-world case studies, and proven solutions designed to address the ethical and technical challenges we face today. This report addresses several key themes, including:

- **Deepfakes and synthetic media:** Addressing the question, "Is AI outsmarting us?" Submissions examine strategies for detection, the transition from visual inspection to "proof of personhood", and the role of liveness detection to prevent fraud
- **Border management and travel:** Investigating whether seamless travel is becoming a reality through digital passports, Electronic Travel Authorisations (ETAs), and interoperable verifiable credentials, and the complexities of managing biometric consent across borders
- **Remote identity and onboarding:** Best practices for secure remote identity verification (IDV) and reusable identity to reduce user friction, while addressing vulnerabilities like injection attacks
- **Ethics, governance, and inclusion:** Navigating legislative impacts and the vital distinction between "verification" and "identification" and a focus on drivers for social inclusion, ensuring systems work for all populations
- **Next-generation security:** Practical applications of multimodal approaches, including voice, palm recognition and behavioural biometrics, to strengthen live facial recognition as tools for account security and preventing identity theft

Please note that the Biometrics Institute does not endorse any of the specific submissions, products, or advertisements featured in this report. This compilation is intended to facilitate open discussion and knowledge sharing as we navigate the complexities of this rapidly evolving field together.

If you have questions regarding the content of a specific submission, please contact the respective authors directly. For any enquiries regarding the work of the Biometrics Institute, please do not hesitate to reach out to me.

Many thanks,



Isabelle Moeller
Chief Executive
Biometrics Institute

manager@biometricsinstitute.org

2. Amadeus: Responsible biometrics: why travel is the ultimate test

Trust in biometrics isn't built in labs- it's earned in real-world operations. The last decade made biometrics mainstream; the next will judge how responsibly it's used. The conversation is shifting from "Can we deploy?" to "Should we deploy, and under what controls?" That is not a philosophical shift, but a practical one. And one that reflects rising expectations for transparency, accountability, impartiality, clearly defined use and robust controls.

And what better proving ground than the travel and mobility industry? Airports, borders, cruise and maritime terminals are environments where stakes are high and visible. If biometrics works responsibly here, it can work anywhere. If it fails, confidence erodes everywhere.

From compliance to continuous responsibility

For years, responsible biometrics was treated like a checkbox—a one-time compliance exercise. That approach is outdated. Systems evolve, risks change, and adversaries adapt. Responsibility is a lifecycle, not a gate. It means continuous governance: measuring, auditing, and improving over time, not defending past procurement decisions. This shift matters because the stakes are high. In travel, failure isn't abstract. It's a missed flight, a stressful border crossing, or a loss of public trust.

The Biometrics Institute has long championed principles of transparency, accountability, and impartiality. These are operational imperatives as much as ethical principles. A responsible biometric programme cannot be treated as a procurement outcome. It must be embedded as an ongoing discipline, with governance that anticipates change and adapts to evolving threats.

Bias, privacy, and the human experience

Demographic performance gaps are real, but bias often starts before the algorithm. Poor lighting, inconsistent capture, or substandard equipment can create unequal outcomes. Inclusive design must extend to operations, with clear quality controls and fallback paths that protect dignity when automation fails. A false rejection isn't just a metric - it's a human experience, often in a stressful context. Responsible operators explicitly design for failure: clear assisted channels, dignified exception handling, and safeguards that prevent automation bias becoming institutional bias.

Privacy, too, must move beyond policy statements. It needs to be architectural - built into systems through data minimisation, retention discipline, and auditable access controls. Privacy-by-design isn't optional; it's essential to secure wholesale confidence in the system. Decentralised and on-device approaches are gaining traction because they reduce exposure, but they come with adoption challenges that require careful planning.

New threats demand new defenses

Generative AI has made deepfakes cheap and scalable, turning spoofing from a fringe risk into an industrialised threat for biometrics. Defense must be layered: Presentation Attack Detection (PAD) and liveness checks, secure pipelines, monitoring, and clear incident playbooks. Biometrics and cybersecurity are now inseparable. A biometric system isn't just a recognition engine - it's a socio-technical security system.

At the same time, multimodal biometrics, i.e. combining several biometric identifiers, offers resilience. It's not about "more tech"; it's about inclusion and risk containment. When one modality fails or is under attack, others provide fallback options, reducing friction and discrimination. Multimodality can be used ethically, as a tool to reduce exclusion, not as an excuse for unnecessary data collection.

Governance and accountability in a high-risk world

Regulation is tightening. Under the EU AI Act, biometrics in the migration/border control context, when used to identify a traveller based on a list of possible matches, is classified as high risk, demanding demonstrable governance: lifecycle risk management, robust security, and transparency that withstands scrutiny. Whether you operate in Europe or not, the signal is global - governments expect proof, not promises.

When you develop your own algorithms instead of purchasing them, the level of responsibility becomes greater. Developers are accountable for how their systems perform across different demographic groups, for maintaining security, and for ensuring transparency and auditability. Continuous testing and improvement are essential, especially as biometrics expand into high-throughput domains like maritime and casinos, etcetera.

Four questions that matter

To implement a truly responsible biometric program, ask:

- Can we prove fairness over time, in real conditions, with real populations?
- Are we securing the entire pipeline - not just the matcher?
- Are privacy commitments enforceable by design, not just described in policy?
- Do exception paths protect dignity and inclusion?

These questions cut through marketing and reveal operational reality. If accountability is vague, responsibility is theatre.

The bottom line: trust is earned, not marketed

Trust isn't a campaign. It's the outcome of strong controls, transparent governance, and fair experiences. Responsibility cannot be outsourced. It must be lived as an operational discipline. Done right, biometrics can enhance security and convenience while respecting rights. Now it's incumbent upon every biometric provider to show it. Every project we're involved with must earn public confidence rather than consume it.

Joined in 2012

Organisation: Amadeus
Name: Jeff Lennon, Vice President Strategic Sales EMEA Travel & Governments, AirOps
Telephone number: +47 945 07 097
Contact details: monica.hansen@amadeus.com

3. Attain Insight: Keeping It Real While Protecting Privacy: The Role of Anonymised Biometrics

The Challenge of Verifying Who's Real

Verifying who or what is real is becoming increasingly difficult. Deepfakes, synthetic identities, and increasingly sophisticated fraud techniques are eroding trust across digital and physical environments. Biometrics have emerged as a powerful tool for verifying authenticity and presence. A biometric signal can confirm that an interaction involves a real human rather than a bot or a fabricated identity. However, as biometric technologies become more widespread, public concern has grown about how biometric data is collected, stored, and used. High-profile data breaches have heightened fears of surveillance and loss of control.

This creates a fundamental tension: how can organisations keep systems secure and verify what's real, without compromising individual privacy? Anonymised biometrics offer a way forward, enabling strong verification and fraud prevention while limiting exposure of personal data and supporting responsible, ethical use.

Why Traditional Biometrics Alone Are No Longer Enough

Today, biometric data is more valuable, more mobile, and more exposed than ever. Centralised storage of identifiable biometric information amplifies the impact of breaches and raises legitimate concerns about long-term misuse. In parallel, advances in artificial intelligence have made it easier to replicate, manipulate, or spoof biometric traits, challenging assumptions about what constitutes a trusted signal.

There is also a growing gap between what technology enables, and what society accepts. Regulators and the public are questioning whether identification is always necessary and whether collecting highly sensitive biometric data is proportionate to the risk.

These pressures are driving a shift in thinking. Rather than asking how to strengthen biometric identification, organisations are increasingly asking whether identification is required at all. Traditional biometrics alone cannot meet this shift. New approaches are needed: ones that deliver assurance and security while reducing data exposure and respecting privacy expectations.

What Are Anonymised Biometrics?

Anonymised biometrics are approaches that remove Personally Identifiable Information (PII) from biometric data to ensure that the individual can no longer be identified. Once data is anonymised, there is no risk of a PII breach. With no way to extract personal information, the custodial responsibilities for managing PII and the associated costs are significantly reduced or eliminated. Additionally, data minimisation principles in many data privacy regulations (such as GDPR) require that only the minimum personal data be used to meet the application's purpose. A full biometric sample (such as a face image or fingerprint) often fails to meet this requirement, whereas an anonymised biometric does. Anonymised biometrics can be highly useful for presence verification, anomaly detection, and fraud prevention without knowing, or needing to know, the individual's identity.

Anonymisation Approaches and Uses

There are several different biometric anonymisation approaches – organisations need to select the approach based on how they need to use the biometric data. Approaches such as Differential Privacy and Data Masking protect individuals' privacy, but the resulting data cannot be used for verification, classification, or search.

An alternative approach is now available, called Search-Preserving Anonymisation (SPAn). With SPAn, biometric data is transformed to remove PII, while still enabling searching and matching against biometric datasets. This enables new applications for biometric information while meeting data minimisation and privacy requirements.

Anonymised identity verification is a key SPAn use case where legitimacy must be confirmed without exposing identity. This includes high-net-worth individuals, large, registered worker populations such as healthcare or construction, identity-sensitive or dual-identity roles (including undercover officers, intelligence operatives, sex workers, and protected witnesses), and sectors exploited by organised crime, such as real estate, transportation, and finance. Authentication scenarios, such as unlocking devices, vehicles or secure spaces, or proving who you are at a bank or government office, are all ideal use cases.

Identity classification, analytics, and collaboration are additional SPAn use cases. In environments such as hospitals, schools, universities, and retirement homes, SPAn supports classification without identifying individuals. It enables crowd composition analysis (e.g., students, staff, or visitors), people counting that distinguishes unique individuals, foot-traffic analytics, and inter-agency collaboration by allowing organisations to recognise identities in common much more efficiently, as well as international collaboration on organised crime, all without sharing personal or identifiable biometric data.

Privacy, Ethics, and Public Trust

Anonymised biometrics support key ethical principles, including data minimisation, proportionality, and purpose limitation. By design, they ensure that biometric signals are subject to protocols aligned with clearly defined purposes. This approach also starts from a position of strength when it comes to compliance with evolving privacy regulations and emerging biometric legislation around the world.

By separating verification from identification, anonymised biometrics help address many of the concerns that have historically limited public trust. They demonstrate that it is possible to deploy biometric technologies in ways that respect individual rights while still delivering meaningful security benefits.

Looking Ahead: The Future of Responsible Biometrics

As synthetic media and AI-driven fraud continue to advance, the need to verify authenticity will only grow. At the same time, expectations for privacy and responsible technology use will continue to rise.

Anonymised biometrics offer a practical path forward, enabling organisations to verify authenticity without exposing individuals' identities, and opens new doors for solutions to social issues that lack good solutions today, such as large, registered worker populations or worker occupations exploited by organised crime. By adopting privacy-preserving approaches today, the industry can ensure biometrics remain a trusted and effective tool for the future.

Organisation: Attain Insight
Name: Paul Hulford, CEO and Founder
Telephone number: +1 613 235 0200
Contact details: info@attaininsight.com

4. Auraya: Validating Identity in the Era of AI: Why Continuous Monitoring and Ethical Defence Will Prevail

Voice biometrics has become a cornerstone of modern security, offering greater convenience and robustness compared to passwords, PINs, or security questions. Yet its rise coincides with a profound shift: artificial intelligence is now capable of generating highly convincing synthetic identities at scale.

The greatest challenge facing the biometrics industry today is validating the authenticity of the biometric sample. Is the speaker a genuine human present at capture, or a synthetic artefact, voice clone, or injected signal?

This "Realness Challenge" underscores the vital importance of ethical biometrics and necessitates practical, layered strategies to mitigate the increasing threats driven by AI. We must move past the myth that any single security barrier can provide 100% protection against deepfakes forever, and instead embrace a dynamic, continuously adapting defence.

The Paradox of AI and Voice Biometrics

AI is both the engine and the adversary of modern biometrics. Machine learning models, particularly deep neural networks, are essential for feature extraction, voiceprint matching, and robust liveness detection. Yet, the same underlying technology enables attackers to create highly convincing synthetic identities and perform devastating attacks. And therein lies our paradox.

The Threat Landscape and the "AI Plateau"

The spectrum of AI-driven biometric fraud is rapidly expanding. AI models can now synthesise believable voices from relatively short recordings of audio, generating hyper-realistic digital proxies of real individuals. These voice clones are increasingly being used to bypass legacy voice-based identity checks or socially engineer contact centre agents.

Furthermore, attackers utilise digital injection to push this synthetic audio directly into the telecommunications pipeline, bypassing physical microphones entirely.

However, it is crucial to recognise that the threat landscape is unlikely to continue escalating at the breakneck speed we have witnessed in recent years. We are rapidly approaching the "AI Plateau."

The primary, well-funded objective of ethical generative AI development is to create synthetic voices and images that are indistinguishable from reality to the human ear and eye. We should not downplay this remarkable capability; there are incredibly positive, ethical use cases for this technology. From restoring the voices of those with speech impairments to revolutionising digital education, accessible interfaces, and content creation, the ability to generate believable synthetic media is a profound technological leap. The AI industry is virtually at that threshold today, with cheap systems able to produce synthetic voices and avatars in near real-time that easily fool humans.

Once generative AI consistently fools humans for these legitimate purposes, the massive commercial and economic incentive to make these models even better diminishes. Fraudsters largely rely on these commercially available, ethically developed tools repurposed for malicious intent. Because defensive AI analyses sub-audible artifacts, acoustic anomalies, and data far beyond human perception, the amount of time, computing power, and money required for a bad actor to train an AI solely to defeat a superior defensive AI becomes economically unviable. Ethical AI, designed to spot synthetics, will consistently outpace the bad actors who rely on tools designed merely to fool humans.

Moving Beyond "Point-in-Time": Continuous KYC (Know Your Customer)

The frontline defence against AI-driven fraud is Liveness Detection or Presentation Attack Detection (PAD). Traditional and early-stage PAD methods, while useful, struggle against advanced AI-driven attacks designed to emulate human speech patterns.

Relying on a single biometric modality and a single PAD method at a single point in time is no longer sufficient. True security requires Continuous KYC. As a user interacts with a BOT or a live agent, the biometric engine must continuously monitor the conversation. If a bad actor—whether a human social engineer or a fully automated, synthetic AI voice clone—attempts a "session takeover" by jumping on the line after the legitimate user has verified their identity, continuous monitoring instantly detects the change in speaker or the introduction of synthetic audio, revokes the verified status, and flags the interaction.

The Multi-Factor Fusion Strategy

To beat sophisticated AI, defence must be layered. A multimodal fusion strategy that combines evidence from multiple sources to make the job of beating the defence network exponentially more difficult.

This goes beyond just audio. By implementing continuous, fused analysis of multiple biometric and deterministic signals—such as voice, face, iris, lip-sync alignment, and real-time device trust data—organisations can triangulate trust with incredible accuracy.

Ethical Defence and the Path Forward

In the fight against AI fraud, ethical biometrics demands a zero-trust approach. Ethical biometric deployment requires responsible use of AI not just in detection, but in system management. Defensive AI models must be continuously tested, audited, and updated with the latest synthetic attack data to ensure algorithms evolve ahead of the threat, all while rigorously protecting the privacy of genuine user data.

The Future of Biometrics

The future of biometrics will not be defined by static barriers or singular breakthroughs. It will be defined by adaptability. Continuous monitoring, multimodal fusion, deterministic device intelligence, and evolving deepfake detection represent a shift from reactive security to resilient architecture.

As synthetic media becomes indistinguishable to humans, biometric systems must operate beyond human perception, analysing signal integrity, behavioural continuity, and contextual risk.

In an increasingly artificial digital landscape, the challenge is not simply recognising a voice. It is validating reality itself. Responsible, adaptive biometric systems will determine whether identity remains secure in the era of AI.

Joined in 2007

Organisation: Auraya Systems
Name: Paul Magee, CEO
Telephone number: +61 418 255 938
Contact details: paul.magee@aurayasystems.com

5. Aware: How Biometrics is Helping Solve the Digital Identity Trust Crisis

As digital identity systems scale globally, the industry is confronting a new reality: trust can no longer be inferred from credentials, documents, or even biometric matches alone. Generative AI has made it possible to convincingly simulate faces, voices, and behaviours at speed and at scale which is eroding the reliability of traditional identity verification methods.

In recent speaking sessions at identity and biometrics-focused events, Aware CEO Ajay Amlani has reframed this challenge with a simple but powerful observation: *identity lives in humans, not in systems*. Credentials, devices, and databases are abstractions—useful, but ultimately secondary to the human being behind the interaction.

In a world where digital representations can be fabricated, the defining question becomes not only *who* someone is, but *whether they are real and present at the moment of interaction*. Liveness detection has emerged as the mechanism that helps answer that question.

Biometrics as a Reflection of Human Recognition

Humans have always relied on physical and behavioural cues to establish trust. Faces, voices, and mannerisms are the original authentication factors. Biometrics simply digitise this instinctive process, enabling systems to recognise individuals in ways that feel natural and intuitive.

The widespread availability of cameras and microphones, combined with growing consumer acceptance, has accelerated biometric adoption. For many users, biometrics are now the preferred method of authentication. Biometric technology is faster, more convenient, and easier to use than passwords.

However, as Ajay noted, the same technologies that enable seamless experiences also create new attack surfaces. When AI can generate realistic biometric artifacts, matching a biometric template is no longer sufficient to establish trust.

The Shift from Identity to Liveness and Presence

Traditional identity verification focuses on answering a static question: *Does this data match a known identity?* Modern threats demand a dynamic answer: *Is a real human present right now?*

Deepfakes and synthetic identities exploit the gap between these two questions. A synthetic face may match a stored template. A blended identity may pass document checks. Without assessing liveness, systems risk validating artifacts rather than people.

Liveness detection directly addresses this challenge by evaluating the authenticity of the biometric interaction itself. It assesses whether biometric data originates from a live human being, rather than a replay, injection, or AI-generated construct. In doing so, liveness becomes the control that anchors digital identity back to human reality.

Active and Passive Liveness as Proof of Personhood

Liveness detection techniques generally fall into active and passive approaches, each offering different trade-offs.

Active liveness asks users to perform specific actions to demonstrate responsiveness. While effective against simpler attacks, these approaches can introduce friction and may be increasingly vulnerable as AI systems learn to mimic expected behaviours.

Passive liveness operates without explicit user interaction, analysing subtle signals such as motion consistency, texture, depth cues, and temporal patterns. When responsibly designed, passive methods can confirm presence while preserving usability and accessibility—an important consideration as biometric systems are deployed across diverse populations and use cases.

Critically, liveness should not be viewed as a binary gate, but as a probabilistic signal within a broader identity framework. Its strength lies in continuous evaluation and contextual application, rather than one-time enforcement.

Lessons Learned

Experience across sectors such as financial services, remote onboarding, and high-risk digital access highlights several consistent lessons:

- Liveness is foundational, not optional. Without it, biometric systems are vulnerable to synthetic inputs.
- Presence must be continuously assessed. One-time checks are insufficient in high-risk scenarios.
- Fairness and inclusion require intentional design. Liveness systems must perform consistently across demographics and environments.
- Governance reinforces credibility. Transparency around data handling, testing, and accountability builds public trust.

These lessons emphasise that liveness detection is not merely a technical feature, but a trust mechanism that must be governed responsibly.

Keeping Trust Human

As digital systems grow more intelligent and synthetic content becomes harder to distinguish from reality, the foundation of trust must remain human. Identity does not originate in databases or algorithms; it originates in people. Biometrics serve as a bridge between the physical and digital worlds, but liveness detection is what keeps that bridge grounded in reality. By confirming real, present human participation, liveness ensures that biometric systems continue to reflect the individuals they are meant to represent. In a future shaped by AI, responsible liveness detection will be essential to keeping identity real.

Joined in 2010

Organisation: Aware
Name: Delaney Gembis
Telephone number: +1 781 687 0393
Contact details: Delaney Gembis, marketing@aware.com

6. Biometix: openbq – Better biometrics, better outcomes

Biometric quality and openbq

Biometric quality is not merely a technical metric; it is a key to social inclusion, equitable access to services, and fundamental rights.

Biometric enrolment programmes now underpin public service delivery, financial inclusion, and border security, yet sample quality can be both the greatest challenge and the weakest link. This is true both in low-resource settings with poor lighting, sensor quality, or operator expertise as well as more advanced systems that rely on selfie enrolment or verification.

Poor quality drives higher recapture rates, inflated costs and, most critically, excludes marginalised groups reliant on reliable identity verification.

Biometix's open-source framework, openbq, tackles this systemic problem by providing a standards-aligned, multimodal quality assessment tool that delivers objective scores, diagnostic feedback, and scalable analytics.

Because the code, algorithms and scoring logic are public, regulators, auditors and organisations can verify privacy, fairness, and transparency. Its open-source licence, lightweight footprint and native MOSIP connectors make it easy to deploy for sovereign-data jurisdictions, NGOs, low- and middle-income governments alike.

Why biometric quality matters

Inclusion, diversity, and equity – Reliable identification depends on high-quality biometric data, however real-world capture conditions such as poor illumination, inadequate sensor pressure, user movement, medical conditions, low-cost equipment, or harsh environments, frequently produce subpar samples.

When digital identity programmes fail to obtain usable data from the most vulnerable (rural residents with limited lighting, older adults with dry skin, persons with disabilities who cannot adopt a prescribed pose), systematic exclusion follows; denied access to health care, social welfare, voting, education and financial services, perpetuating the inequities that digital identity is meant to erase.

The impact of low-quality data is threefold:

1. **Exclusion** – Higher enrolment failure rates for vulnerable users.
2. **Operational inefficiency** – Each failed capture triggers a recapture, extending enrolment time, increasing operational expenditure.
3. **Security erosion** – Poor samples raise misidentification risk and weaken anti-spoofing controls, undermining public trust.

A universally accessible, standards-aligned quality engine is therefore essential to deliver inclusive, secure identity programmes.

How openbq can help

openbq supports digital identity programmes by providing an openly available biometric quality assessment framework that delivers:

- **Open-source transparency** – Full code, including ISO-aligned quality algorithms, is on GitHub, letting regulators, auditors and organisations verify privacy, fairness, and non-discrimination.
- **Vendor neutral, standards-aligned metrics –** Implements key parts of ISO/IEC 29794 together with NFIQ 2 (fingerprints) and OFIQ (faces), giving a common language for evaluating biometric samples against internationally recognised thresholds.

- **Evidence-based policy making –** Reporting capabilities generate ready-to-use metrics that help policymakers target training, environmental or user interface upgrades or alternative capture methods to underserved communities.
- **Cost effectiveness** – Open-source licencing and minimal integration overhead let budgets focus on hardware, training and continuous quality-monitoring programmes that boost inclusion and equity.

How openbq does this

Standards alignment

openbq delivers an open-source, multimodal tool that implements ISO-aligned algorithms while remaining freely extensible. It applies ISO/IEC 297941 as a unifying framework and invokes modality-specific modules:

- **Face** – ISO/IEC 297945 (implemented via OFIQ) evaluates illumination, pose, resolution and occlusion.
- **Fingerprint** – ISO/IEC 297944 (implemented via NFIQ 2) measures ridge-valley contrast, pressure, and minutiae quality.
- **Iris** – ISO/IEC 297946 checks pupil/iris ratio, infrared illumination, and occlusion.

These widely referenced standards underpin most procurement specifications, regulatory guidelines, and academic research for biometric quality algorithms.

Technical approach

- **Modular plugin architecture** – New algorithms, additional modalities or custom organisational metrics can be added as plugins without altering the core code, preserving stability while encouraging innovation.
- **APIs and SDKs** – Language-agnostic REST endpoints (OpenAPI) and client libraries for Python, Java and C++ enable seamless integration with existing enrolment platforms, MOSIP deployments or bespoke verification pipelines.
- **Analytics & reporting layer** – Quality results can be visualised in a configurable analytic application and in comprehensive quality reports produced for analysis.

Practical benefits across use cases

Practical benefits emerge across a wide range of biometric deployment use cases, spanning procurement, migration, operations, and governance. By embedding objective quality measurement into each stage of the lifecycle, organisations gain clearer visibility of performance, risk, and inclusion outcomes, enabling more confident and accountable decision-making.

Procurement confidence is improved through objective, standards-based scoring that gives tender committees verifiable evidence of vendor performance. Embedding openbq-derived quality thresholds into procurement processes reduces the risk of selecting solutions that underperform in real-world deployments and strengthens transparency in decision-making. Legacy data migration is likewise enhanced through pre-migration audits that flag low-quality records for targeted re-enrolment, avoiding costly full-scale recapture while preserving historical data value and citizen trust.

Operationally, continuous analysis during pilots and live deployments exposes systemic issues such as sensor drift, operator fatigue, or poor environmental conditions, enabling timely corrective action. From a governance perspective, auditable quality metrics support regulatory oversight and inclusion objectives, while automated issue detection and capture feedback reduce re-capture rates, lower operational overheads, and accelerate enrolment timelines, delivering measurable efficiency gains at scale.

Future outlook – Transitioning openbq to a Digital Public Good

The roadmap rests on three pillars:

- **Pillar 1: Education first framework** – New tutorial series, certification pathways and "quality coach" guides will embed quality awareness into daily workflows, further lowering recapture rates for marginalised users.
- **Pillar 2: Community-driven improvement** – Researchers, industry partners, NGOs, and other stakeholders will contribute field insights and code enhancements, feeding directly into the openbq repository and submissions to ISO technical committees to help shape future standards.
- **Pillar 3: Open-source sustainability** – Ongoing governance, transparent road mapping and the open-source licencing ensure any organisation can adopt, extend and maintain the tool.

Together these elements will position openbq as a scalable, inclusive, continuously evolving digital public good for biometric quality worldwide.

Closing thought

Biometric quality is a cornerstone of equitable, trustworthy identity ecosystems. Objective, auditable scores enable early detection of low-quality captures, preventing exclusion and building public trust. An open, standards-aligned framework turns quality assessment into a visible driver of inclusion, allowing every individual, from bustling cities to remote villages, to participate fully in the digital society.

Joined in 2001

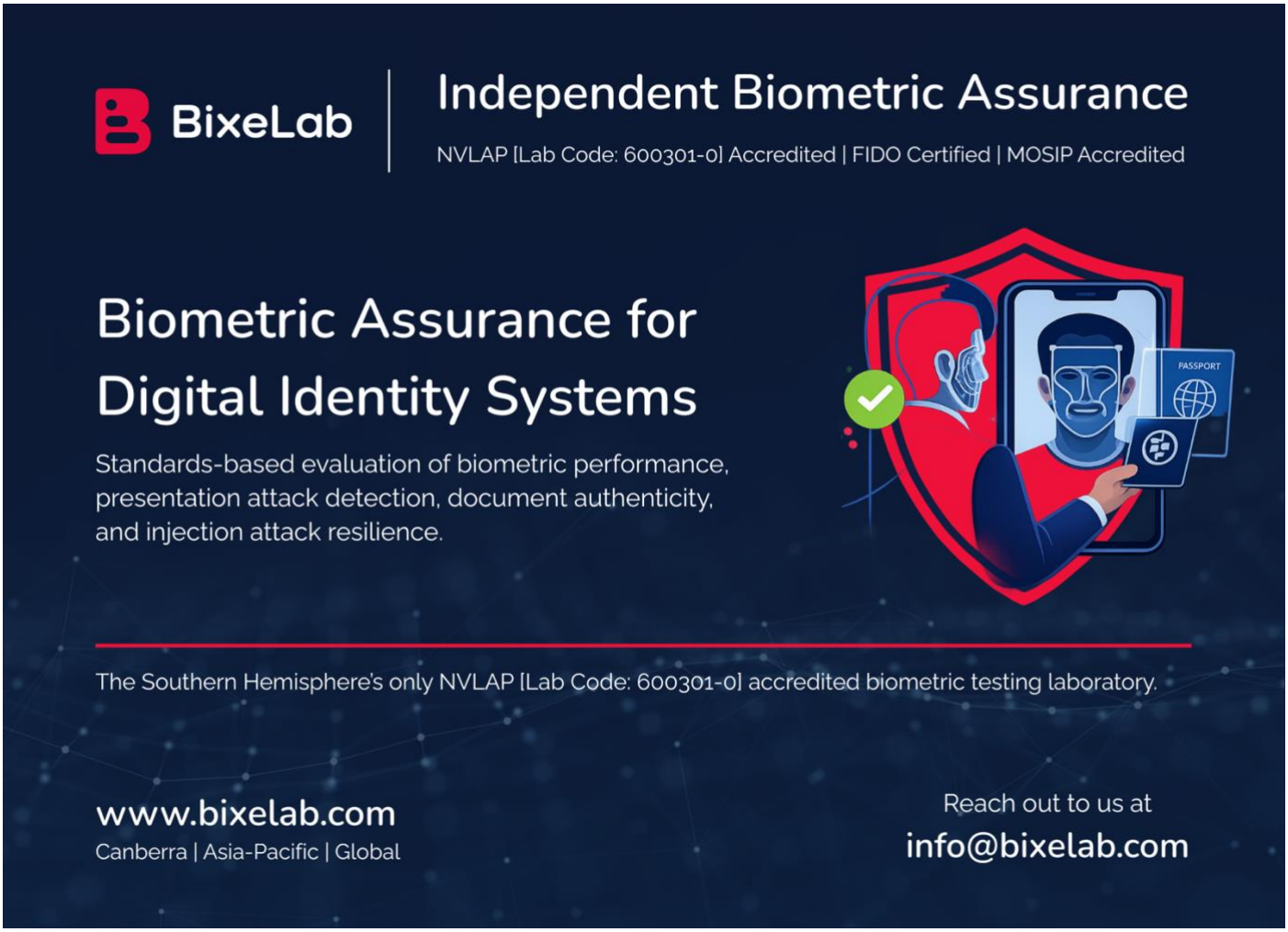
Organisation: Biometix
Name: Ted Dunstone, CEO
Telephone number: +61 419 990 968
Contact details: info@openbq.io

7. BixeLab: Proving Who's Real: Deepfakes, Injection Attacks, and Responsible Biometric Assurance

The act of passing off something fake as being real is not new – most likely, it is prehistoric in origin. Visual media that depicts events that never really happened has been around since the early days of cinema. Attempts to convince biometric systems of a slightly altered reality are a relatively recent development in this long history of artifice.

What has changed is scale, speed and ease of access.

Over time, the use of biometrics has shifted from convenience to security control. Furthermore, the widespread use means the stakes can be very high. Fraud, account takeover, synthetic identity crime, and AI-generated deepfakes have become industrialised. Voice cloning can be executed in minutes. Digital face swaps are widely accessible. Injection attacks bypass the camera entirely. Sophisticated imagery that previously took specialists months of effort to create now takes moments of CPU time. All this leaves the biometric world with a challenge: to what extent can a biometric decision be proven trustworthy?



In response, regulators increasingly require demonstrable assurance. European identity frameworks mandate injection attack detection testing and external validation before a technology can be deployed. Financial authorities in Southeast Asia are moving toward phishing-resistant authentication methods, anchored in biometrics and behavioural controls. Assurance must be evidenced. Trust now depends on measurable assurance, not merely stronger algorithms. Presentation attack detection is no longer sufficient on its own. Modern systems must protect sample capture integrity, detect the presence of manipulation, and secure transmission channels. Media injection, API replay, and stream

substitution have expanded the attack surface. New risks and opportunities have been introduced to the ecosystem as systems rely on user-supplied capture devices and their wide variations in their performance. Critically, technical subsystems with competing objectives must interact and often compromise, and this balancing act then further determines threat exposure.

All of us operate in this environment – test laboratories included. Laboratories support operators and technology providers alike through both individual component assessments and system-as-a-whole evaluations, and the key challenge is to ensure effective outcomes that also improve real-world security. In other words, threat modelling must be aligned with expected risks, potential ramifications, and economic reality. A bank onboarding flow faces different attacker incentives than a border control gate. A high-value payments channel attracts different threats than a low-risk login. In lower risk environments, testing extreme but unrealistic artefacts may generate headlines without improving security.

Conversely, the application of biometrics in defence or highly secure environments can attract very advanced and well-resourced attackers – perhaps even nation-states or complex organised threats. Where significant risk and consequences are possible, appropriately sophisticated test scenarios should be included to address potential threats. In short, an evaluation should address credible presentation attacks, synthetic media, injection techniques, and channel manipulation in line with deployment risk.

Such evaluations are critical to maintaining the security of the systems in play, but in isolation, they are not enough: holistic technical security should consider both an ongoing plan for lab assurance, as well as real-world observed outcomes.

Laboratory testing provides controlled coverage and statistical confidence. It establishes an evidence-based baseline under defined conditions. Conversely, production environments introduce scale, device diversity, and adaptive attackers. Passing a test is the starting point. Stability in operation ultimately determines resilience. Therefore, leading programs now combine independent evaluations by a qualified laboratory with ongoing technical review and appropriate governance escalation. This approach aligns measured performance with operational reality, and enables corrective action as threats evolve – rather than being bound only to formal evaluation cycles.

Public trust of biometric deployments depends on clarity of purpose, strict data minimisation, defined retention, measurable performance, and independent assurance. Responsible use of biometrics rests on appropriate governance, and such governance rests on solid, independent evidence. Increasingly advanced attacks have complicated the challenges of retaining public trust, and demand properly aligned assurance outcomes to underpin this.

No threat detection model can afford to be static. Generative AI will continue to improve, and attack vectors will continue to evolve. Strong governance must be both durable and adaptable, with transparent performance reporting, defined threat models, independent validation, and scheduled implementation review cycles. Regulators increasingly expect this structure, and leading users demand it to support public trust.

Organisation: Bixelab Pty Ltd
Name: Somya Singh, Operations Manager
Telephone number: +61 412 802 334
Contact details: info@bixelab.com; somya.singh@bixelab.com

8. Brands Australia: Remote Identity Verification: Good Practices in Distributed Capture Environments

Remote identity verification is now a standard part of identity checks across both government and commercial services, with processes that once took place in controlled environments increasingly being performed remotely or at distributed locations. While this shift improves accessibility and efficiency, it also introduces challenges that are not always immediately visible, particularly as these processes are applied across different environments, user groups and operating models.

In practice, many of the issues seen in remote identity verification are not caused by the verification technology itself but emerge earlier in the workflow at the point where identity evidence is captured. Factors such as capture quality, operating conditions and process consistency play a significant role in downstream outcomes. Responsible biometrics in a remote context, therefore, depends as much on strong operational controls, clear standards, and effective governance as it does on the technology used to verify identity.

Where remote ID verification commonly fails

Many of the challenges associated with remote identity verification do not sit in the verification itself, but emerge earlier in the workflow, often at the point where identity evidence is first captured. When capture takes place outside controlled environments, variations in lighting, background, pose, resolution, image compression and camera lens perspective can directly affect downstream outcomes, particularly where systems rely on consistent, standards-aligned inputs. Differences in camera focal length, distance to the subject and device positioning can introduce facial distortion that is not always obvious at capture, but materially impacts matching reliability later in the process.

Inconsistent application of capture processes is another common issue, particularly across distributed or assisted environments. Outcomes may vary depending on operator experience, environment, training, and adherence to defined procedures, while in self-capture scenarios, unclear guidance or poorly designed workflows can lead to repeated attempts, unnecessary re-capture or manual intervention.

Over time, this variability increases operational friction and reduces confidence in the overall process for both operators and the applicants/public. Exception handling is also a frequent point of breakdown. When identity checks fail, unclear escalation paths or loosely defined rules can result in ad-hoc decisions or informal workarounds that undermine both security and fairness. A lack of auditability can compound these issues, making it difficult for organisations to trace how outcomes were reached or demonstrate consistent application across locations.

Good practice principles

Treating high capture quality as a core control is central to improving outcomes in remote identity verification. Clearly defined and consistently enforced capture requirements reduce variability and support more reliable downstream verification, particularly where capture conditions cannot be fully controlled. Poor-quality inputs drive higher rejection rates, increase manual review and rework, and introduce avoidable friction and risk over time, reducing confidence in the process for both operators and applicants. Aligning capture processes with recognised standards further supports consistency across systems. International frameworks such as those developed by the International Civil Aviation Organisation (ICAO), supported by established facial image standards such as ISO/IEC 19794-5:2005 and ongoing ISO work including ISO/IEC 25447 addressing less constrained capture conditions, provide a widely accepted baseline for image quality and consistency as identity capture moves into more remote and distributed environments. In enrolment contexts, including for machine readable travel documents (MRTDs), where images do not meet these expectations, risk is introduced at enrolment and often only becomes visible later through higher false positive or false rejection rates during verification, particularly where non-compliant, altered or manipulated images are accepted into enrolment systems.

Clear and well-documented exception handling is a critical component of responsible remote identity verification. Defining when re-capture is required, when escalation is appropriate and how decisions are reviewed helps organisations prevent informal workarounds and support consistent outcomes, particularly within distributed networks.

Privacy considerations should be embedded into remote identity verification workflows from the outset. Applying principles such as purpose limitation, data minimisation and transparent communication helps ensure identity checks remain proportionate and understandable to users, while clear governance over data retention and access supports regulatory compliance and public trust.

Practical Implementation

When implementing remote identity verification, one of the first considerations is defining where different levels of assurance are required, as not all use cases carry the same level of risk. Lower-risk scenarios may be suited to streamlined self-capture workflows, while higher- risk or regulated use cases often benefit from additional controls, assisted capture or structured review processes. Being explicit about these distinctions helps organisations apply controls proportionately rather than uniformly.

Clear guidance at the point of capture is also critical, regardless of whether capture is assisted or unassisted. Simple instructions around lighting, positioning and image framing can significantly reduce variability and the need for re-capture, while consistent operator guidance helps maintain quality across distributed locations. Where assisted capture is used, clearly defined roles and responsibilities reduce reliance on individual judgment. Exception handling should be built into workflows from the start. Defining when re-capture is required, when escalation is appropriate and how decisions are reviewed, alongside tracking indicators such as re-capture rates, rejection reasons and manual intervention levels, helps organisations identify where processes need refinement. These insights can inform targeted training and clearer guidance, improving outcomes without adding unnecessary friction.

Finally, governance documentation should outline how identity data is managed throughout the process, including retention, access controls and user transparency. Clear governance supports accountability and reinforces trust as remote identity verification continues to scale.

Joined in 2009

Organisation: Brands Australia
Name: John Rule, Managing Director
Telephone number: +61 3 8324 0156
Contact details: john.rule@brandsaustralia.com

9. Cognitec Systems: Age Assurance for the Ages?

The truths and dangers are more evident than ever. Minors consuming digital content meant for a mature audience are more susceptible to developing symptoms of depression, anxieties and social isolation. In addition, untrained users of online shopping platforms easily fall victim to scams or addictive behaviour.

Countries around the world are formulating laws and regulations with the ambitious goal to keep underage users from spending too much time online, being subjected to cyberbullying, accessing dangerous or prohibited digital content, or from illegally purchasing goods through online channels.

While there is broad consensus on the importance and need for age assurance, there is much less agreement on who can and should conduct the age check, and at what age. Regulations are still being discussed and formulated, with global standards far from agreement. Even the terms and definitions remain unsettled, with age assurance and age verification often mistakenly interchanged.

At the moment, the term age assurance is defined as a broad term encompassing various methods to determine or estimate a user's age, while age verification defines a specific, more certain method within that scope. In other words, age assurance includes age verification as well as other techniques like age estimation and self-declaration.

Age assurance laws are currently present in the UK, the EU, the U.S. (at state levels), Australia, New Zealand, Canada, and Malaysia, with many other countries working on their own version. The laws vary widely by culture, jurisdiction, purpose, and enforcement method.

Australia is actively enforcing age assurance laws to control and deter social media access to all minors under 16. The UK Online Safety Act went live in August 2025, with regulation body Ofcom enforcing the age verification law. Relevant websites that are not complying with providing underage checks are subject to huge fines. The EU Data Protection Board adopted an age assurance statement with guiding principles that provide a framework for a consistent European approach to age checks.

The past year has seen businesses making huge investments to develop or purchase age assurance technologies that comply with these newly released regulations. Many of them complain that minors will find ways to circumvent these technologies, such as using VPN tunnels, or consume websites and social media channels from countries where such laws do not exist. These arguments and debates continue to question the feasibility and validity of age assurance schemes.

Legal battles erupted on multiple continents, with Big Tech companies and heavyweight advertisers ready to fight age check legislation. Especially in the U.S., the cries for freedom of speech and personal privacy are fuelling these legal disputes. Small businesses especially are pointing out the enormous costs of implementing such systems, calling it unlawful to demand these measures and cause substantial revenue loss. But their cries are met by more and more governments, lawmakers, communities and parents taking a magnifying glass to practices and values of gaming, adult content, and social media platforms.

Effective age assurance schemes, and their built-in biometric methods, are still in their infancy stage, and will see many changes and adaptations in coming years. Much hope lies in the world-wide adoption of digital wallets that can lead toward a standardised approach to identity and age verification for various onboarding and login methods in the digital world.

Other possibilities lie in zero-knowledge proofs (ZKPs) techniques that allow users to prove their age without sharing their birth date or ID documents. Behavioural biometrics might serve this method, or looking at certain patterns in internet and AI usage, all determining the user's age while minimising the risk of data exposure and breaches.

While novel approaches will emerge and some stick around, age estimation based on facial image analysis will definitely stay and advance to support various age assurance schemes. And more and more companies will compete to offer accurate, trusted solutions. The U.S. agency NIST is publishing regular independent test results of age estimation algorithms in the FATE Age Estimation & Verification test, giving testament to the increasing number of providers, and also the improving accuracy of their technologies.

A recent report from Liminal predicted the global age assurance market to grow from $5.7 billion in 2025 to $10.4 billion by 2029, driven by increasing regulatory enforcement, and demand for safer online environments. Many of these will incorporate biometric checks, from simple age estimation to multimodal age assessments. Yet another grand opportunity for the biometrics industry to contribute to a safer, trustworthy world for the (all) ages!

Joined in 2002

Organisation: Cognitec Systems
Name: Elke Oberg, Marketing Manager
Telephone number: +49 151 4614 8367
Email address for correspondence with Biometrics Institute: oberg@cognitec.com
Contact details: sales@cognitec.com

10. Entrust: Is AI outsmarting you? Deepfakes, Injection attacks, and the next generation of responsible biometrics

1. Introduction: when realism is no longer proof

Biometric systems were long built on a simple but powerful assumption: if a face looks real and is captured live by a camera, it represents a real person, physically present at the time of verification. Advances in generative artificial intelligence have disrupted this assumption. In 2026, deepfakes have reached a level of realism where visual inspection—by humans or traditional computer vision models—is no longer a reliable indicator of authenticity.

Deepfakes are no longer marginal. Industry data now shows that approximately one in five biometric fraud attempts involves a deepfake[1], reflecting both the accessibility of generative tools and the professionalisation of fraud operations. The central question is no longer whether deepfakes can be detected visually, but how systems can reliably prove real-time presence and capture integrity.

2. What deepfakes look like in real identity flows

In operational identity systems, deepfakes typically take three forms:

- **Face swaps**, where synthetic faces are overlaid onto real heads in a live or recorded video stream.
- **Fully synthetic media**, generated entirely by AI models and not corresponding to a real individual.
- **Animated selfies**, where a static image is transformed into a moving video mimicking natural facial motion.

[1] The quantitative data points, figures, and diagrams referenced in this paper are drawn from *Entrust, 2026 Identity Fraud Report: The Changing Face of Fraud*.

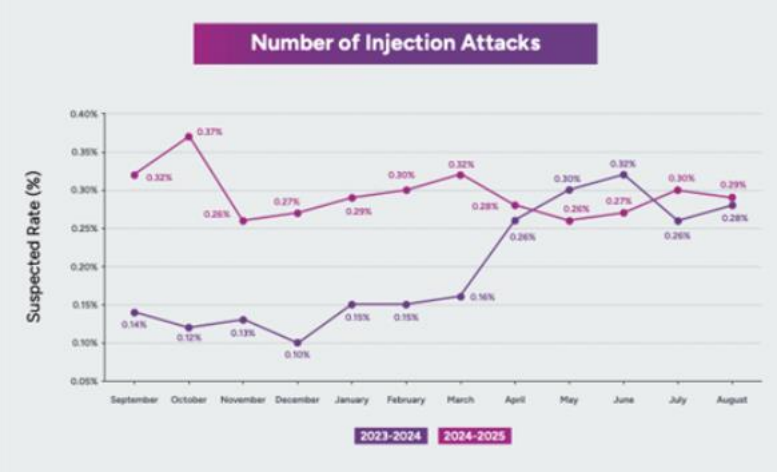
All three variants are observed across the identity lifecycle, including onboarding, authentication, and recovery flows. While they differ technically, they share a common objective: impersonation at scale. Increasingly, these attacks succeed not because visual imperfections are obvious—the media is often visually indistinguishable from genuine capture—but because it is delivered through technical pathways that bypass or weaken traditional safeguards.

3. The shift from presentation attacks to injection attacks

Historically, biometric spoofing focused on *presentation attacks*, such as photos, masks, or screens shown to a camera. While these methods of attack persist—including cases where deepfakes are presented as videos of screens—the most consequential evolution has been the rise of *injection attacks*. In practice, they have become the primary vector for submitting deepfakes into biometric systems. Injection attacks bypass the camera entirely by introducing falsified images or video streams directly into the camera feed, using techniques such as virtual cameras, device emulation, browser manipulation, or network-level payload tampering.

Injection-based attacks have increased by roughly 40% year-on-year and are now widely recognised as the primary delivery mechanism for sophisticated deepfakes. These attacks are effective because the software convincingly emulates legitimate devices and camera inputs, undermining controls that rely on environmental cues, metadata, or basic liveness checks. This marks a structural change in the threat model: the attack surface is no longer limited to the biometric itself, but extends to the device, software stack, and transmission channel.

Figure 1 — Suspected injection attack rate in biometric verification flows (2023–2025)



The chart shows a step increase in suspected injection attacks in late 2023–24, followed by sustained stabilisation through 2024–25, suggesting they are now a persistent feature of the biometric threat landscape.

4. The evolving role of liveness detection

Liveness detection remains essential. Passive and active techniques help establish that biometric data was captured from a living person in real time by introducing motion, temporal depth, and randomness.

However, liveness alone is insufficient against modern attacks. Predictable prompts can be learned and replayed, while visually convincing deepfakes can satisfy purely visual-based checks. In controlled deployments, active liveness with enforced randomness can reduce the rate of successful biometric fraud attempts to well below 0.1%, raising the cost and complexity of attacks. As verification systems harden, fraud predictably migrates toward more sophisticated techniques—especially injection-based attacks—making effective defence increasingly reliant on richer, more resilient passive signals to expose anomalies that cannot be spoofed at the source.

Effective defence therefore requires liveness to be combined with capture integrity and non-visual signals, in addition to enforced randomness, to ensure real-time presence rather than replayed or injected content.

5. Measuring effectiveness responsibly

As biometric fraud becomes more sophisticated, organisations, including government agencies and private-sector service providers, must adopt more nuanced performance metrics. Industry guidance converges on three decisive measures for deepfake resilience: False Acceptance Rate (FAR / APCER), False Rejection Rate (FRR), and Missed Fraud Rate (MFR / BPCER).

Optimising a single metric in isolation can distort the balance between FAR, FRR, and MFR, either by excluding legitimate users or by allowing fraud to scale silently. Responsible biometric systems used by government authorities and private-sector organisations alike require balanced optimisation and transparency around trade-offs.

6. Standards and their limits

International standards establish baseline trust. ISO/IEC 30107-3 remains the global benchmark for Presentation Attack Detection, but it was not designed to address injection attacks. Emerging specifications, such as CEN/TS 18099, begin to fill this gap by focusing on capture circumvention and media injection in response to evolving attack vectors.

These frameworks should be treated as minimum foundations rather than complete solutions. Attack techniques evolve faster than certification cycles, making continuous adaptation essential.

This evolution reflects a broader industry shift: deepfakes are now understood not merely as presentation threats, but as system-level risks tied to capture integrity and injection resilience.

7. Best practices for preventing deepfake-enabled fraud

Many effective defenses against deepfake fraud rely on novel capabilities—particularly in the use of passive and integrity-based signals—and on the application of machine learning and automation to detect patterns at scale. However, their impact ultimately depends on disciplined implementation choices that remove unnecessary attack surface. Experience across public- and private-sector identity deployments highlights several priorities:

- prefer secure, native capture over web;
- keep capture components up to date;
- minimise opportunities for injection by disabling uploads and limiting retries;
- harden web-based flows through integrity-aware capture;
- treat fraud prevention as a continuous process through monitoring, automation and adaptation.

8. Conclusion: keeping biometrics “real”

AI succeeds where systems still equate realism with authenticity. Deepfakes exploit weak assumptions about capture, integrity, and trust rather than the limits of human perception. By combining layered controls, metrics, and evolving standards, the biometric ecosystem can deliver security and trust.

Joined in 2016

Organisation: Entrust
Name: Virginia Chiarentin Senior Product Manager;
Samuel Steg, Senior Principal Regulatory Compliance Strategist
Telephone number: +33 6 83 75 0253
Contact details: samuel.steg@entrust.com

11. Facephi: The Last Mile of Seamless Travel: Empowering Passengers with Agent-based Biometric Consent

Almost Seamless

Passenger digital admissibility, biometric touchpoints, and interoperable verifiable credentials are shaping the future of a seamless passenger experience. In October 2024, a PoC within the IATA Strategic Partnership Program demonstrated this. Using verifiable credentials, passengers selectively shared their PII and biometric traits remotely in advance, allowing them to walk through touchpoints using just their face. This success was reinforced in 2025 PoC "Exploring Artificial Intelligence and Digital Identity Use Cases in Aviation". Still, there are different flavours of adoption. Due to the complexity and fragmentation of different regulatory frameworks along the passenger journey, consent for the use of personally identifiable information (PII), and specially for the use of biometric attributes, is probably the most challenging withholder. This article will deep dive into discussing whether leveraging the same technology as decentralised identity and payments could unlock it, and how it will shape the travel industry wallet so consent travels along with the identity attribute and the passenger owns and manages that consent.

The burden of managing the consent

Managing consent in a fragmented regulatory framework of Privacy and Security is the Last Mile to cross for Seamless Travel. A passenger itinerary travelling from one country to another, and sometimes connecting in a third one, goes through a myriad of data privacy regulations that shapes the passenger experience while authenticating at each of the many biometric touchpoints present in their itinerary (e.g. bag drop, security check, VIP lounge, and plane access).

Depending on the regulatory framework, a passenger can walk through just taking a selfie at the biometric touchpoint, compare it with a previously shared biometric reference (1:N scenario), or presenting its Personally Identifiable Information (PII) such as its biometrics traits at the biometric gate (1:1 scenario). This trade-off between convenience (1:N) and privacy (1:1) shapes the passenger experience, making the travel experience a legal one as well.

With so many regulatory frameworks, such as the European GDPR, the US CCPA and BIPA, the Singapore PDPA, or the Dubai PDPL, among many others, the passenger must opt-in as many times as biometric touchpoints are present in the journey, meaning a possible consent fatigue, ambiguity, and many pop-ups forms to read, and terms and conditions to accept.

For carriers such as airlines or cruise companies, centrally managing this consent is a challenge. To offer a seamless travel experience, they must navigate the complexities of a fragmented and jurisdiction specific regulatory framework and therefore, must design complex customer experiences and business rules for engagement, including regulatory updates, consent revocation, accountability, traceability, and auditability.

Agent-based Biometric Consent

To walk through this complex and fragmented regulatory framework, there must be a source of trust. An airline or cruise company must rely on some Regulatory Frameworks aggregator that is updated, available, and reliable. For instance, IATA's Contactless Travel Directory providing the biometric touchpoints available in a passenger's itinerary, can also be widely accepted and used as a source of information about how consent must be compliant in each of the jurisdictions a passenger must go through.

Inspired by the AP2 Agent Payment Protocol used for "*for trusted, verifiable agentic payments*", a carrier or a cruise company's AI Agent (the Operator Agent) connects to this source of trust APIs using the MCP Model Context Protocol. The Agent retrieves the list of biometric touchpoints and their specific privacy requirements to design a custom consent profile compliant for each and all the biometric touchpoints the passenger authenticates. It then issues an Intent Mandate as a Verifiable Credential (VC), detailing the biometric usage, conditions, and locations (e.g., 1:1 vs. 1:N; EU vs. UAE).

The Operator Agent communicates with the Passenger Agent using the A2A Agent 2 Agent protocol. The Intent Mandate is offered to the passenger's agentic wallet. The passenger accepts and signs a Consent Mandate in VC format containing the information provided by the Intent Mandate and the passenger's Personally Identifiable Information (PII) attributes needed to complete the biometric transaction at each of the biometric touchpoints. This Consent Mandate can fully accept the whole itinerary or selectively accept some specific biometric touchpoints in some specific regulatory frameworks or countries.

An Authentication Mandate in VC format is issued at each of the biometric touchpoints. This verifiable credential contains the biometric transaction context, providing tamper-evident, non-repudiable, cryptographically signed proof of intent and consent. This protocol grants passengers' true ownership of their biometrics while offering ecosystem operators, such as airlines and cruise companies, a scheme that guarantees authorisation, authenticity, auditability, and traceability.

The Passenger Experience will be defined by how the Intent Mandate is presented, and how the Consent Mandate is issued and presented. In a 1:N scenario, Consent Mandate will act like the "Human Not Present" scenario in the AP2 Agent Payment Protocol, and therefore the Operator Carrier will know in advance to proceed in each of the biometric touchpoints, while the 1:1 scenario will be more like the "Human Present" scenario where the passenger will be presenting the Consent Mandate at each biometric touch point at the same time the selfie is taken.

Empowering the Passenger for Seamless Travel

Under this agentic Authentication Consent Protocol, and with an Agentic Digital Wallet specific to the Travel Industry, the passenger takes full ownership of their consent. Operators such as airlines, cruise companies, OTAs, and hospitality providers can now offer an agentic solution that automates decentralised consent management. By doing so, they finally cross the Last Mile, enabling a truly interoperable, compliant, and Seamless Travel experience with Biometric Authentication.

Joined in 2018

Organisation: Facephi
Name: Miguel Santos Luparelli Mathieu, Product Innovation Director
Telephone number: +34 965 108 008
Contact details: miguelluparelli@facephi.com

12. FaceTec: Videos Are No Longer Reliable Audit Evidence in the Deepfake Era

Preface

As the shift toward digital services continues, a growing number of institutions have adopted remote user onboarding. To support compliance obligations, many regulators required institutions to record and retain video sessions of remote identity verification as audit evidence.

The rationale for adoption was reasonable: create a durable, reviewable artifact that could later demonstrate compliance with customer due-diligence obligations.

Of critical importance, however, the threat landscape has fundamentally changed. What was once considered to be strong evidence is now untrustworthy, spoofable, and in storage, creates an unnecessary biometric data honeypot.

Despite this shift, video recordings are widely perceived as a reliable proof-point in remote KYC processes.

The Current Model

In many jurisdictions, institutions are expected to demonstrate that a real person was present, followed instructions, and completed onboarding in real time. To meet these expectations, many organisations record full verification sessions and retain video as an audit trail.

This practice rests on several beliefs: that verification videos cannot be convincingly fabricated, that they can be stored safely over time, and that video itself provides durable proof of authenticity. All these assumptions are now outdated.

Structural Challenges

1. Deepfake and Face-Swap Maturity

Generative AI has reached a point where producing highly realistic synthetic video is no longer unusual or cost-prohibitive. Tools for face swapping and deepfakes are now widely accessible. As a result, recorded verification video can no longer be treated as strong proof that a real person was present during onboarding. Visual review, whether human or automated, loses evidentiary weight as synthetic footage becomes increasingly difficult to distinguish from genuine recordings. Over time, stored videos may be challenged or invalidated as unreliable evidence. An audit artifact that can be convincingly fabricated no longer provides durable assurance.

2. Replay and Media Injection Abuse

Many KYC flows still rely on users performing a predefined set of actions in front of a camera. If a system lacks robust defenses against replay and media injection attacks, previously captured video material can be reused to impersonate users. Ironically, the very recordings created "for compliance" can be exploited against the institution if leaked or misused.

3. Creation of a High-Value Honeypot

Retaining media creates a high-value repository of sensitive data. These assets can be reused for impersonation across services, and a single breach may expose large numbers of individuals at once. From a risk management perspective, long-term storage of such content conflicts with regulatory emphasis on data minimisation and on limiting the impact of breaches.

4. Privacy and Proportionality

Storing personally identifiable information is inherently sensitive. Storing data-rich video represents materially higher exposure. A full verification recording may include voice patterns, behavioural traits, environmental context, and sensitive identity document details- all consolidated within a single file. If compromised, such a recording cannot be reset, replaced, or meaningfully revoked, leaving the affected individual exposed to ongoing risk. At the same

time, retaining full-session recordings may exceed what is necessary to demonstrate compliance. Over time, controls introduced to support auditability can expand institutional privacy exposure and liability.

5. Proposed Direction

To move beyond legacy audit practices that rely on easily exploitable media, institutions should transition from storing human-viewable recordings to retaining non-replayable proof. This more resilient approach relies on generating a biometric payload within a secure execution environment that is immune to presentation attacks and media injection.

1. The audit record should be derived from a live capture session but should not itself be usable as input for future verification attempts. It must retain evidentiary value without remaining operationally reusable.
2. It should not be visually interpretable or repurposable as media.
3. Signals used to establish liveness should exist only during the verification process and be discarded afterward, ensuring the retained artifact cannot be replayed or injected into another flow.
4. Data encryption should be mandatory and enforced by default.
5. The artifact should be usable only within its originating system and meaningless outside of that context.
6. By design, such records reduce honeypot risk. Their non-human-readable, non-replayable nature limits both their attractiveness to attackers and the impact of unauthorised access.

Conclusion

Video recordings served as transitional evidence in early remote onboarding models. In today's threat environment, they no longer provide the level of integrity, safety, and long-term reliability required for high-assurance identity processes. Effective compliance is not achieved by retaining data for its own sake. It depends on retaining the right kind of data: records that resist spoofing and replay, cannot be meaningfully interpreted by humans, and that preserve privacy by design.

Looking toward 2026 and beyond, assurance cannot rest on artifacts that attackers can fabricate with greater realism than human reviewers can reliably detect. Durable trust requires audit evidence aligned with modern attack vectors.

Joined in 2017

Organisation: FaceTec, Inc.
Name: Ilya Vlasov, Senior Sales Consultant
Telephone number: +382 68 798 344
Contact details: ilya@facetec.com

13. FACIA: Remote Identity Verification: Best Practices and Proven Solutions

As digital interactions increasingly dominate, the need for secure remote identity verification (IDV) becomes essential. Remote IDV solutions allow businesses to verify identities without physical presence, ensuring secure onboarding. However, with advancements in technology, challenges such as identity fraud, spoofing, and privacy concerns arise. AI-driven biometric verification methods, including facial recognition, document verification, and liveness detection, are key to addressing these risks. This piece of content explains the latest trends, best practices, and operational advantages of remote IDV while highlighting the ethical and privacy considerations organisations must address to foster trust and comply with regulations.

Rising Trends in Remote Identity Verification

The digital transformation of industries has accelerated the adoption of remote identity verification. Organisations across fintech, healthcare, government services, and e-commerce are relying on AI-powered verification systems to securely authenticate users. Technologies such as facial recognition, document verification, liveness detection, and behavioural biometrics are integrated to create seamless onboarding experiences.

Recent data from Goode Intelligence reveals that the global adoption of remote identity verification is rising rapidly, with verification checks projected to reach 3.8 billion. The shift to paperless, remote processes has made real-time, accurate identity verification a crucial element of digital operations, enabling both efficiency and security in user interactions.

Challenges and Threats

While remote identity verification offers efficiency and convenience in user onboarding, it faces growing risks that are increasingly highlighted by regulators. Identity fraud remains a major concern, with criminals exploiting stolen documents, synthetic identities, and AI-generated media to bypass remote verification systems. The U.S. Financial Crimes Enforcement Network (FinCEN) issued an alert in 2024 warning about the rise of generative-AI-powered deepfakes in identity theft and fraud, especially in attempts to defeat remote onboarding and authentication controls.

Spoofing attacks, such as using photographs, masks, or deepfake videos, continue to challenge verification systems like facial recognition and liveness detection. Moreover, technical limitations like poor image quality, inconsistent lighting, and network instability can reduce verification accuracy. At scale, organisations must find a balance between security, accuracy, and user experience, underscoring the need for adaptive and resilient solutions.

Societal and Ethical Implications

Remote identity verification inherently involves handling sensitive personal and biometric data, raising privacy and ethical concerns. Organisations must ensure compliance with data protection regulations, such as GDPR and CCPA, to safeguard users' personal information. AI-driven verification systems must be carefully designed to avoid demographic or racial biases, ensuring fairness in authentication.

Transparency and accountability are essential to building trust with users, who need confidence that their data is secure and used responsibly. Ethical implementation of remote IDV not only protects individuals but also strengthens organisational reputation, promotes regulatory compliance, and reinforces public trust in digital services.

Best Practices and Verification Mechanisms

Effective remote identity verification relies on multiple layers for robust security. Document verification ensures that IDs are authentic, while biometric authentication (including facial recognition and liveness detection) ensures that the legitimate user is accessing a service. AI-driven fraud detection further strengthens protection by analysing user behaviour and device data to detect suspicious activity. Verification solutions must be independently tested to ensure reliability. Certifications like iBeta Level 2 demonstrate effectiveness in Presentation Attack Detection (PAD), providing

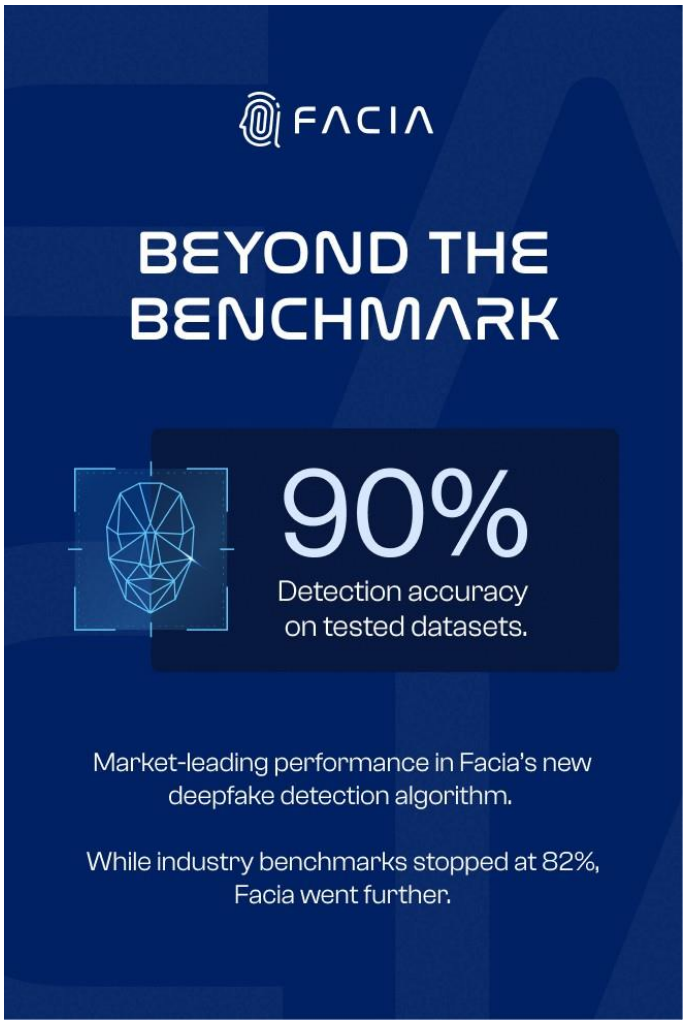
resilience against sophisticated spoofing and fraud attempts while maintaining accurate and secure verification processes. These independent evaluations ensure that the solutions used are robust against evolving security threats.

Financial and Operational Impacts

Implementing effective remote IDV delivers measurable business benefits. Systems streamline onboarding, improve customer conversion rates, and reduce operational costs. Face biometrics with advanced liveness detection provides a higher level of assurance, ensuring that the person presenting the identity is genuine while meeting regulatory standards. By combining robust verification methods with real-time identity checks, organisations can reduce fraud risks, improve user trust, and demonstrate compliance with global data protection and financial regulations.

Future Prospects

The evolution of remote identity verification continues to grow, with face biometrics playing a central role in shaping the way users access services. Today, technologies such as Pay with Face transactions, seamless airport check-ins, wallet authentication, and secure access to remote government services are becoming mainstream.



In the near future, AI-driven verification will ensure these interactions remain secure by detecting subtle signs of fraud and validating identities instantly. Integration with broader digital ID ecosystems will allow cross-platform verification, while continuous authentication will maintain trust throughout the user journey. These innovations promise both enhanced convenience and stronger digital security, making everyday interactions faster, safer, and more reliable.

Governance, Legislation, and Compliance

Governments and regulators are increasingly defining how remote identity verification must operate to ensure security and trust. The European Union Agency for Cybersecurity (ENISA) has published best practices for remote identity proofing, which outline threats and necessary countermeasures for biometric systems.

These practices highlight the importance of anti-spoofing and injection-attack defences. The eIDAS II regulatory framework introduces harmonised requirements for remote identity proofing across the EU, including strong biometric verification under **Article 24**. Additionally, joint guidance on remote identity proofing for European Digital Identity Wallets (EUDI Wallet ARF) further emphasises **biometric genuineness** and **document authenticity** as core elements of secure onboarding.

Securing the Digital Future

Face biometrics have become indispensable for secure remote identity verification, enabling seamless access to digital services while ensuring robust authentication. However, the threat landscape is evolving rapidly, particularly with the rise of generative AI-powered deepfakes. It is therefore essential that verification solutions are equipped with advanced anti-spoofing capabilities, such as liveness detection and fraud pattern analysis, while adhering to strict data privacy standards.

By combining security, compliance, and user convenience, organisations can deliver reliable, efficient onboarding experiences, safeguard digital identities, and maintain trust in an increasingly connected and high-risk digital ecosystem.

Organisation: FACIA
Name: Daniyal Chughtai, CTO
Telephone number: +92 33 34538900
Contact details: daniyal@facia.ai

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

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 multimillion-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 nonexistent 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 categorise 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, organisations 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.

Multifactor 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 behavioural biometrics, which are harder to synthesise 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:

- Enrolment 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.

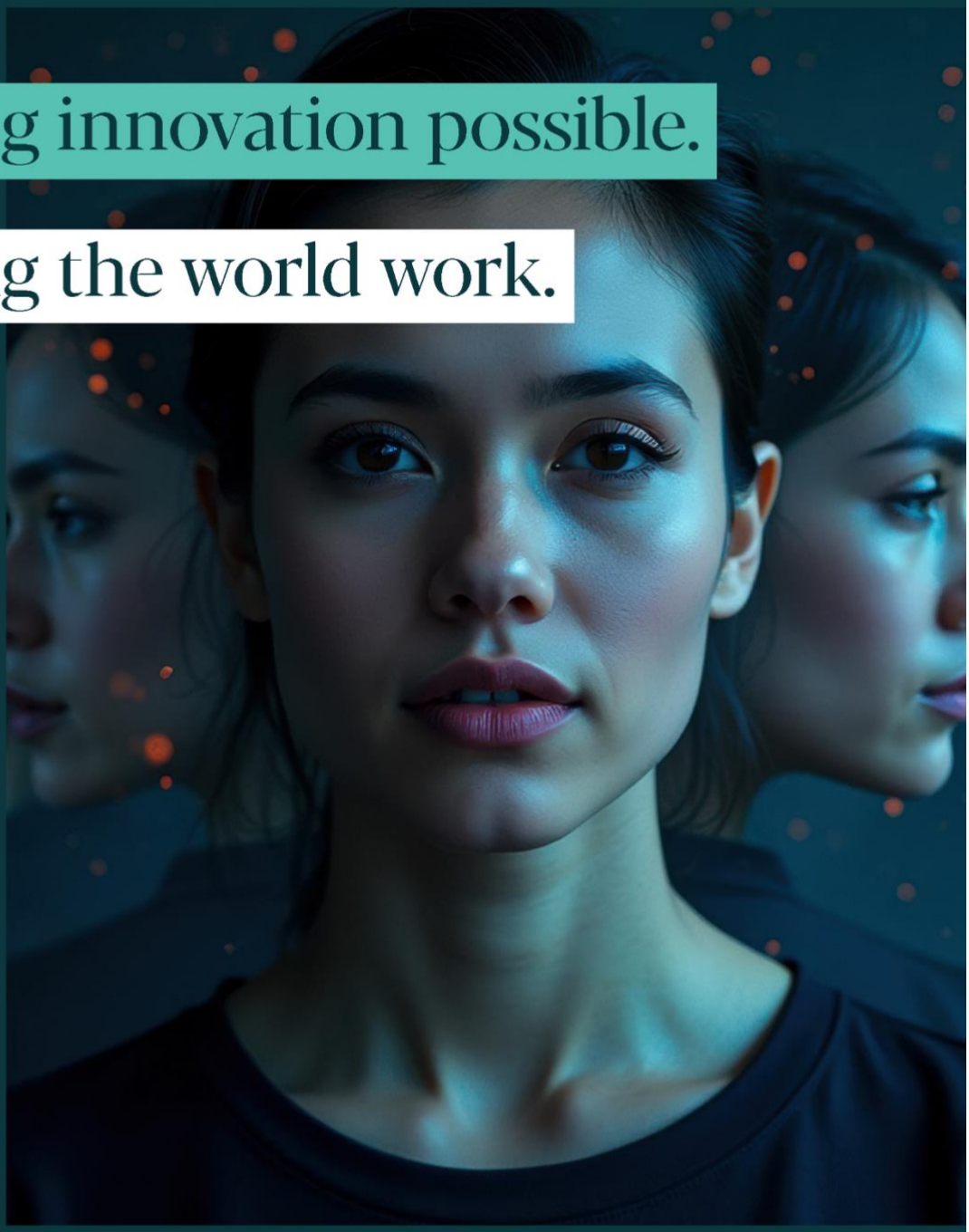
Strengthening governance and reinforcing reliability

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 organisations 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, industrialised 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 recognised standards and regulatory enforcement. By adopting layered defences across the user lifecycle and reinforcing biometric systems with advanced detection and security controls, organisations can stay ahead of increasingly sophisticated deepfake attacks.

Organisation: Fime
Name: Jean Fang, Lead Consultant Digital Identity at Consult Hyperion, consulting by Fime
Telephone number: Stéphanie Pietri +33 1 41 98 4859
Contact details: stephanie.pietri@fime.com

fime × consult hyperion
consulting by fime



Making innovation possible.

Making the world work.

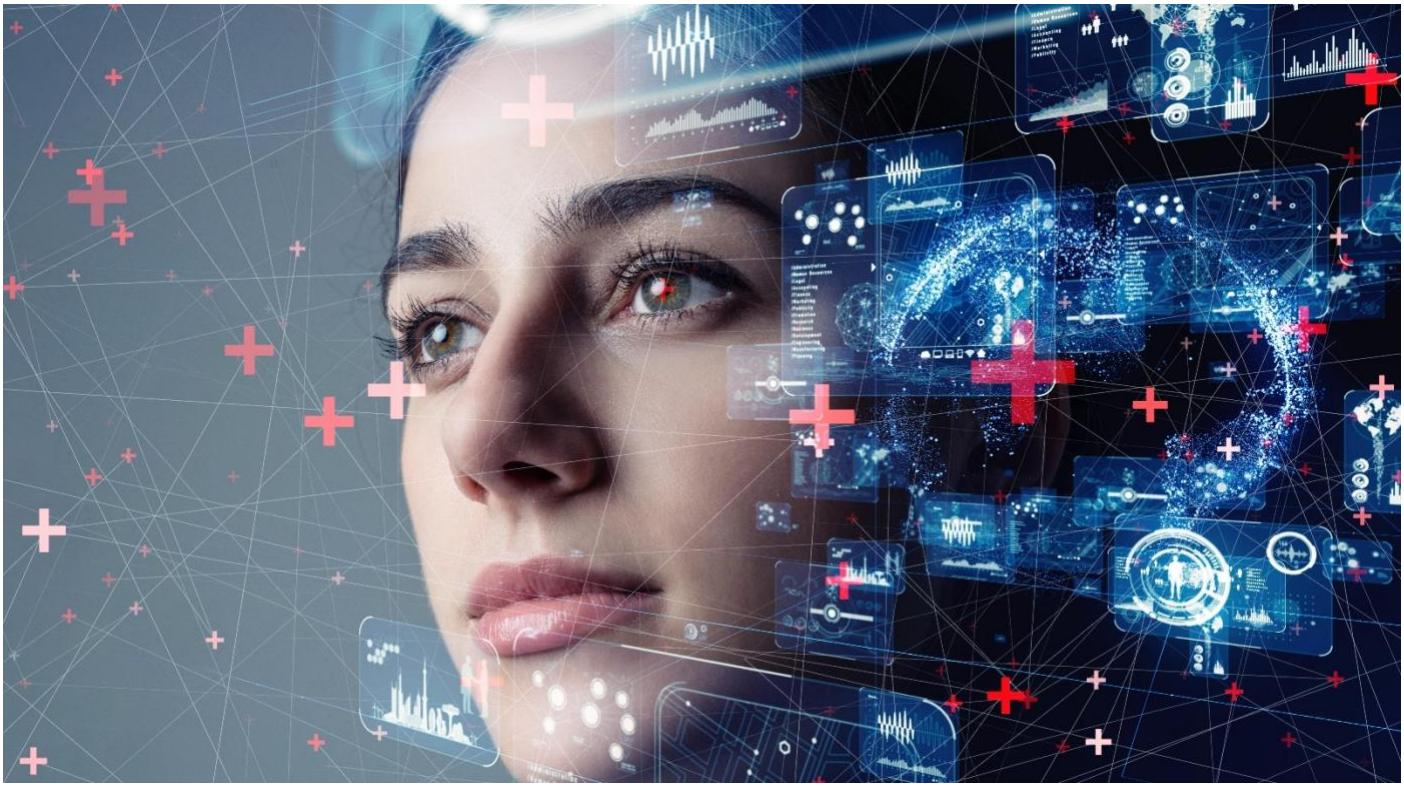
Consulting | Test Platforms | Testing Services

Contact us at fime.com

15. Fujitsu: From recognition to responsibility: strengthening live facial recognition through behavioural analytics

The adoption of live facial recognition (LFR) is accelerating, particularly across Western societies. This once experimental technology is rapidly becoming mainstream, driven by growing challenges like violence, antisocial behaviour, and retail crime. Here in the UK, for example, the Home Office recently announced the country's largest rollout of LFR to date as part of a wider programme of policing reforms[1].

The pace of change here poses its own challenges. The question is no longer "should LFR be deployed?", but "how do we ensure that it is deployed responsibly?". How do we ensure that LFR meets standards around ethics, transparency, and accountability? And what controls are required if those standards are to be met consistently at scale?



Retail as a flashpoint

Before we can answer those questions, we need to take a moment to consider why LFR now finds itself in the spotlight – and it's here that we need to turn back to the subject of retail crime.

Retail may not be unique in facing rising levels of violence, theft, and antisocial behaviour, but it is an industry in which those pressures are highly visible and deeply consequential, impacting everything from staff wellbeing through to profitability and customer experience. It's also an environment in which LFR can play a critical role in defending against those behaviours. Used effectively, LFR can help to identify known (and typically prolific) offenders, link individuals to previous incidents, and support more consistent decision making by security teams.

Put simply, LFR is exceptional as a confirmational tool – one that gives retailers and law enforcement agencies the ability to recognise people of interest and take appropriate action. But as effective as it may be at visual identification, LFR inevitably has shortcomings, too. For instance:

- LFR is heavily reliant on human operators to monitor feeds and interpret alerts. Over long shifts, fatigue can set in – leading to lapses in attention, missed cues, and inconsistent decisions.

[1] UK announces largest ever facial recognition rollout as part of policing reforms – Biometric Update, 26th January 2026

- Across a large building or estate, tracking subjects of interest between cameras is difficult, especially if faces are not visible, deliberately obscured, or affected by viewing angles or lighting conditions. These gaps in continuity can prevent rapid intervention.
- While LFR can identify an individual against a gallery of faces, it cannot tell operators what they have done, are doing, or might do next. Without those behavioural cues, the response can become reactive, rather than preventative and informed.
- Looking for known faces alone does not protect against perpetrators of organised crime who may recruit new individuals to commit planned offences, or detect theft or anti-social behaviour by new and unknown actors.

Combined, these issues have real implications from a responsibility perspective. Decisions may be made based on incomplete or fleeting substantiation. Opportunities for intervention may be missed or prove disproportionate to a person's actual behaviours. Perception that technology 'should have prevented this' may undermine confidence in systems. And actions taken based on facial identification alone may be difficult to explain after the fact.

Without a change in the way that LFR is used, questions about responsibility—about whether it is consistent, proportionate, and accountable at scale, and how effective it can be on its own—are always likely to linger. And it's in that context that the concepts of behavioural analytics and body biometrics need to enter the discussion.

Context matters

If LFR is going to be deployed successfully (and responsibly) at scale, then it needs to go beyond just confirming who someone is; in live environments like stores, transport hubs, and public venues, security decisions need to be shaped as much by context as they do by recognition.

Behavioural analytics (BA) makes that possible. Rather than focusing solely on who someone is, BA focuses on what they're doing—and what they might do *next* —within a specific environment. Analysing actions, patterns, and changing behaviours in real-time, BA can detect even the subtlest signs of intent, such as loitering, agitation, or unusual movements. And, crucially, these insights can be attained regardless of whether a subject is already known.

BA, which looks beyond the face and at things like body shape, posture, and movement, creates a unique and anonymous body identifier that can be tied to behavioural indicators.

In practice, the addition of BA can fundamentally bolster the effectiveness of LFR. LFR retains its value as a confirmational tool, without needing to shoulder the entire risk detection burden.BA can provide the context that operators need to understand *why* an alert matters, not just *who* it relates to. Used effectively, that information can shift the emphasis from in-the-moment response towards prevention, a key distinction when considering proportionality.

Another issue here is continuity. As noted above, when people move around public spaces, tracking them accurately and consistently based on facial recognition alone can be difficult. A unique body identifier can act as a binding mechanism, maintaining continuity across feeds and environments without repeated facial matching.

And that distinction matters. The biometric data delivered by BA doesn't need to be used to identify more people or add them to watchlists. Instead, it can be used to reduce inconsistency, improve understanding, bring forward intervention points, and lower the risk of decisions being made on partial information. It can make decisions more robust, more explainable, and more responsible.

Together, BA and supporting biometric insights can act as controls on LFR, rather than extensions of it. Employed in the right way, they can be a force multiplier for human operators – focusing their attention, helping them remain vigilant, and giving them greater confidence in their decisions. Moreover, it can prevent people from becoming criminalised in the first place, giving retailers the opportunity to shadow—and ultimately deter—a casual opportunist.

Ultimately, this isn't about expanding surveillance but enabling responsibility at scale. As LFR becomes more widespread, questions over its ethics will only become more pointed. And as that happens, LFR's long-term viability will depend on it working consistently, proportionately, and fairly. BA can make that possible.

Organisation: Fujitsu
Name: Peter Sutcliffe, Borders Technology Lead
Telephone number: +44 777 927 3045
Contact details: peter.sutcliffe@fujitsu.com

16. HID: The Future Is You: Biometric Trends That Will Redefine Identity in 2026

We have all heard the question: **What if you *never* had to carry documents or keys, swipe cards or remember passwords again?** In 2026, that reality is closer than ever. Everyday credentials—and their frustrations—are fading away. And *you* will be the only element needed to validate your identity and access to spaces, places and services.

What are top trends driving this shift to shape the biometrics landscape in 2026 — and transforming our daily lives?

The Rise of Vertical Use Cases

One of the most compelling trends is the spread of biometrics into vertical use cases — for faster access, reduced friction and experiences that feel almost invisible.

Travel is the most visible example. Forget long queues at airport immigration or presenting multiple documents at security. In 2026, facial recognition quietly becomes the key that unlocks a truly seamless journey. And this trend is rapidly expanding into other sectors, like banking and finance. Imagine walking into your branch or up to an ATM and having your identity confirmed instantly via a secure fingerprint or facial scan — no physical IDs, no lengthy security questions, no waiting lines. Just immediate, verified access to services and an extraordinary customer experience.

Self-Service and Contactless Dominance

The demand for quick, do-it-yourself interactions is making facial recognition essential. In 2026, self-service kiosks will be everywhere — from air travel and healthcare to venues and banks. Biometric authentication instantly verifies your identity for seamless access to services and loyalty program benefits. Other places biometric-enabled kiosks make life easier:

- Border crossings and immigration
- Retail and restaurants payments
- Hotel check-in and access to amenities
- Hospitality patient check-in

Organisations can maximise efficiency and optimise resources, while ensuring equity for users regardless of age, skin tone or mobility/dexterity challenges.

Multimodal Biometrics: Stronger Together

Multimodal biometric authentication is another significant shift for 2026. Fingerprints will increasingly be combined with facial or voice recognition to create a stronger, multi-layered identity profile. Why settle for one lock when you can have more — and still gain access instantly?

Multimodal biometrics deliver much stronger security and are being embraced worldwide. For example, Brazilian banks are evolving from single-factor biometric authentication, such as fingerprints at ATMs, to **multimodal biometric authentication** that combines fingerprints with facial recognition for enhanced security. Layering technologies can effectively prevent fraud while improving customer experience.

AI-Powered Defense

Fraudsters are more creative than ever, with threats (deepfakes, masks and silicone fingers) evolving quickly. Stay ahead with next-generation biometrics—equipped with AI-powered **Presentation Attack Detection (PAD)**—as the frontline defence against identity fraud. Advanced PAD detects and prevents sophisticated spoofing attempts in real time, helping organisations mitigate fraud while safeguarding their brand reputation.

Innovative biometric systems do not just compare static images — they use sophisticated algorithms:

- **Facial Recognition**: Ensure a living person is present — combating digital and physical spoofs.
- **Fingerprint Biometrics**: Multispectral imaging (MSI) captures the surface and subsurface fingerprint details for superior accuracy and liveness detection — making fake molds ineffective.

Privacy-Preserving Identity

Privacy isn't optional; it's foundational. In 2026, consider ***how safe*** your personal data will be. Security cannot be an add-on but must be engineered into every layer of the biometric system. Three big shifts lead the way:

- **Self-Sovereign Identity (SSI):** Imagine individuals maintain full control of their identity through secure digital wallets and verifiable credentials, eliminating dependence on centralised databases that hackers target. This decentralised approach strengthens privacy and simplifies compliance.
- **Edge Processing:** Instead of sending sensitive biometric data to a central cloud service for verification, the processing happens locally on the device. Edge processing drastically minimises latency and the exposure of private data to external threats.
- **Built-In Protection:** Privacy embedded into every layer of the solution — from secure boot-up processes to strong end-to-end encryption across all data flows, meeting or exceeding regulations and enabling confident operation in any market.

Regulatory Acceleration

The growing wave of regulation continues, primarily emanating from the European Union (EU). Global companies are closely monitoring how these frameworks will redefine their operations. Key legislation driving this shift:

- **GDPR:** Establishes rigorous data privacy mandates
- **EU AI Act:** Sets strict, high-risk thresholds for biometric applications like facial recognition
- **EU Entry/Exit System (EES)**: Mandates and digitises border checks with biometrics

These standards set a high bar and become de facto global standards. Biometric system providers and deployers worldwide can align their technologies with strict privacy and ethical rules to remain competitive.

Scalable, Developer-Friendly, Seamless Integration

Integrating biometrics can be easier than ever, without needing to be a specialised engineer. Integration is becoming effortless:

- Clean, lightweight APIs and SDKs that plug directly into existing apps and infrastructure
- Seamlessly add biometrics to an app, system or kiosk without rebuilding the entire platform
- Ease of integration turns biometrics from a high-cost, specialised security layer into a standard, agile feature

Looking Ahead Yet Keeping It Real

Biometrics in 2026 promise a future where identity is effortless, portable and secure. Facial recognition powers contactless security and makes it much easier to travel, while fingerprint biometrics are evolving into a cornerstone of continuous, multimodal authentication. So, as biometrics reshape the way we live and work, the real question is: Are you ready for what comes next?

Joined in 2019

Organisation: HID
Name: Daniel Asraf, Vice President Innovation and Product Management
Telephone number: +1 612 286 6496
Contact details: daniel.asraf@hidglobal.com

17. IDEMIA Public Security: Biometrics, Borders, and Travel: Is Seamless Travel Becoming a Reality?

Biometrics is rapidly becoming a global standard in border management. From automated gates to large-scale entry and exit programs, biometric identity verification is now embedded in the way travellers are processed across regions and transport modes.

As adoption accelerates, the conversation is evolving. The question is no longer whether borders will use biometrics, but whether biometric technologies can facilitate genuinely seamless travel: journeys that are secure, intuitive, and efficient, without compromising trust.

Seamless travel is emerging through a combination of developments. Progress depends on both the advancement of border operations, through automation, self-service, and frictionless processing, and closer cooperation across the wider travel ecosystem, with interoperability and trusted data governance as critical enablers.

1. From automation to flow: rethinking border clearance

The most visible improvements toward seamless travel are taking place at the operational level. Across airports, land borders, and, increasingly, seaports and rail environments, biometrics supports a shift from manual checkpoints to more automated, flow-based clearance models.

Scaling automation and self-service

The first pillar of this transformation is the expansion of automation and self-service. Biometric eGates and kiosks are now widely deployed, leveraging digital pre-enrolment and contactless capture, to streamline processing. Automation helps authorities to scale throughput while allowing border officers to focus on exceptions, higher-risk cases, and traveler support where human judgment remains essential.

Crucially, automation does not remove border guards from the process. Instead, it reallocates resources to higher-value tasks such as supervision, decision making, and human-centric help. Biometric-enabled self-service is therefore becoming a structural component of border modernisation.

Designing for real-world travel behaviours

Seamlessness also requires systems that reflect real-world travel behaviours, rather than idealised one-by-one processing models. Travel involves families, assisted passengers, and passengers with varying levels of digital familiarity. In response, border agencies are broadening eligibility for automated clearance, through assisted lanes, supervised automation, and family-friendly processes.

Singapore (ICA): Automatic border Clearance for families

At land borders, innovation is also driving approaches such as in-vehicle clearance, recognising the distinct characteristics of road-based crossings. Seamless travel cannot be achieved if automation benefits only a narrow subset of travellers.

Passportless and document-light travel

A further evolution is the emergence of passportless or document-light travel concepts, where biometric identity becomes the primary token for clearance. Singapore, for example, has articulated approaches that enable travellers to move through parts of the journey using biometrics as the core identifier.

As digital identity frameworks mature, biometrics is extending beyond point-of-check verification toward continuity across multiple touch points.

On-the-move clearance: the next operational frontier

The next frontier in seamless operations is on-the-move biometric clearance. Next-generation solutions aim to allow travelers to move naturally, with biometric capture and verification taking place in the background.

These flow-based models have the potential to significantly improve throughput and user experience, moving seamless travel from controlled pilots toward wider operational deployment.

Taken together, these developments demonstrate that seamless travel is increasingly becoming an operational reality.

2. Seamless travel as an ecosystem: interoperability and trust

However, seamless travel cannot be delivered by border technology alone. True end-to-end journeys depend on cooperation and interoperability across the travel ecosystem.

Border authorities, airlines, airports, cruise and rail operators, and technology providers must align processes, data flows, and standards to avoid fragmented traveller experiences. Seamlessness is not simply the automation of a checkpoint; it is the continuity of trusted identity across the journey.

UAE (Abu Dhabi airport): Single Token end-to-end Journey

This requires frameworks that allow identity to be established once and reused appropriately across stakeholders, while respecting governance boundaries. Collaborative approaches, supported by interoperable architectures, will be essential to scaling seamless travel beyond isolated deployments.

Trust, privacy, and fairness as prerequisites

At the core of this ecosystem approach lies trust. Biometrics involves sensitive personal data, and adoption depends on strong safeguards around privacy, transparency, proportional use, and fairness. Travellers must have confidence that biometric systems are deployed responsibly, with secure data handling and consistent performance across populations.

Seamless travel is therefore not only a matter of convenience, but also one of legitimacy and public acceptance.

Seamless travel is emerging—responsibly

Biometrics is already reshaping borders and travel at an unprecedented pace. Automation, expanded eligibility, passportless concepts, and on-the-move clearance are moving from aspiration to operational reality. At the same time, the full promise of seamless travel depends on ecosystem-wide cooperation and trusted governance frameworks that ensure privacy, fairness, and confidence.

In this sense, seamless travel is arriving. Its long-term success will be defined by how responsibly, collaboratively, and transparently the industry delivers it.

Joined in 2001

Organisation: IDEMIA Public Security
Name: Genevieve De Vera, Director, Communications
Telephone number: +1 978 808 7047
Contact details: genevieve.devera@ps-idemia.com

18. IDEMIA Public Security: Deepfakes and Deception: Is AI Outsmarting Us?

Artificial intelligence has reached a point where it can convincingly reproduce human appearance, voice, and behaviour with remarkable realism. Media generated by advanced models, such as generative adversarial networks and diffusion techniques, is no longer confined to experimentation or entertainment. It is increasingly exploited for fraud, impersonation, and social engineering, directly challenging trust in identity systems. The question is not whether deepfakes will emerge, but whether institutions can preserve trust in genuine identities as these techniques evolve.

Deepfakes exploit a basic human vulnerability: We trust what we see and hear. AI-generated content can now capitalise that instinct, creating false yet convincing representations of real people. Research from the US National Institute of Standards and Technology (NIST)[1] shows that human inspection alone is not sufficient when distinguishing genuine images from manipulated or synthetic ones. This has direct consequences for law enforcement, border management, financial services, and remote identity verification.

Addressing the threat of deepfakes requires a layered and evidence-based approach. One line of defence focuses on distinguishing biometric signals that remain difficult to replicate consistently. These include involuntary facial movements, fine-grained skin texture, micro-expressions, and subtle physiological indicators such as blood-flow patterns. NIST's Face Recognition Vendor Test program has demonstrated that not all algorithms perform equally when exposed to morphed or artificial data, reinforcing the importance of independently evaluated technologies.

Liveness detection has become another cornerstone of resilience. Its purpose is to confirm that a biometric sample originates from a live individual who is physically present, rather than from a replayed image, video, or generated artifact. Contemporary methods combine passive analysis with active interaction, assessing depth, motion, texture, and natural responses. When implemented correctly, these measures significantly increase the complexity and cost of deepfake-enabled attacks.

Liveness detection must be combined with device-level cyber defense. Secure devices—such as point-of-sale terminals, professional biometric capture devices, or dedicated enrolment hardware—protect against attempts to inject manipulated or replayed data directly into the system. In Bring Your Own Device scenarios, additional safeguards are required to detect compromised devices and prevent data acquisition attacks while maintaining trusted capture and enrolment processes. This layered approach ensures that both the user and the device contribute to the integrity of biometric authentication.

Prevention is just as important as detection and it begins even earlier, at the point of enrolment. Secure identity creation relies on high-quality capture, controlled conditions, and compliance with recognised standards. Weak enrolment processes allow manipulated data to enter systems, undermining trust throughout the lifecycle of an identity. Conversely, robust initial identity proofing ensures that subsequent checks are anchored to reliable reference data, limiting opportunities for synthetic substitution.

Within this broader ecosystem, organisations such as IDEMIA Public Security contribute through longstanding experience in large-scale identity programs. Working with governments and public authorities worldwide, trusted identity suppliers should support enrolment, verification, and identification systems across border management, law enforcement, and civil identity contexts. Their core focus should include secure capture, algorithmic performance, and system integrity reflects the type of end-to-end strategy required to address sophisticated threats.

Independent evaluation plays a critical role in maintaining trust. Biometric algorithms must be regularly assessed through NIST programs, providing objective insight into accuracy, robustness, and demographic performance. Such testing is

[1] https://www.nist.gov/publications/guardians-forensic-evidence-evaluating-analytic-systems-against-ai-generated-deepfakes

particularly relevant for synthetic media, as it helps decision makers understand how systems perform under difficult conditions, including manipulated or low-quality inputs.

Beyond technology, effective responses to deepfakes depend on governance and collaboration. Public authorities, solution providers, researchers, and standards bodies all have a role in shaping responsible deployment. Practical examples already illustrate the scale of the challenge: fabricated media intended to mislead investigations, AI-driven impersonation during remote onboarding, and attempts to exploit automated border systems using fake identities. Across these scenarios, success depends on strong identity proofing, liveness assurance, continuous monitoring, and solutions validated against recognised benchmarks.

Looking forward, deepfakes will continue to improve in realism and accessibility. Countermeasures must therefore evolve through multimodal approaches, behavioural analysis, and AI models trained specifically to recognise artificial artifacts. The objective is not to remove AI-generated media, but to preserve trust, identity, accountability, and fairness wherever it appears.

AI is not outpacing our ability to respond, but it is redefining expectations. Through independent testing, secure-by-design architecture, and responsible deployment frameworks, organisations can detect manipulation, limit misuse, and sustain confidence in identity systems. Responsible biometrics are not a one-time technological choice, but a continuously governed capability built to uphold societal trust.

Joined in 2001

Organisation: IDEMIA Public Security
Name: Genevieve De Vera, Director, Communications
Telephone number: +1 978 808 7047
Contact details: genevieve.devera@ps-idemia.com

19. Innovatrics: Beyond Face: Strengthening Remote Identity Verification with Palm Recognition

Standard remote identity verification relies heavily on facial biometrics. While effective, this current approach has inherent limitations. The most significant vulnerability is the public availability of high-resolution facial imagery. In the age of social media, finding a clear photo of virtually anyone is trivial, providing attackers with the raw material needed for impersonation.

To mitigate these risks, modern solutions employ various defenses, such as **Injection Attack Detection (IAD)** and **Presentation Attack Detection (PAD)**. However, because these methods rely on probabilistic machine learning models, they are never 100% foolproof. There is always a statistical likelihood that a sophisticated attacker could circumvent these defenses.

The Palm Advantage: A Multi-Layered Approach

Adding palm recognition changes the attacker's starting position. Unlike faces, high-quality images of a person's palms are rarely found online, making it significantly harder for bad actors to harvest biometric data for impersonation.

Furthermore, using palms offers several unique technical advantages:

- **Dual Biometrics:** Most users have two hands, providing two distinct biometric sets.
- **Multi-Sided Verification:** Identification can be performed using both the **palmar** (inner) and **dorsal** (outer) sides of the hand.
- **Natural 3D Mapping:** By asking a user to rotate their hand in front of a camera, the system can reconstruct 3D information from motion. This is often more intuitive and less cumbersome for the user than rotating their entire head or maneuvering the phone for a facial 3D scan.

Our research indicates that single-palm verification accuracy is comparable to facial recognition. However, by combining a face scan with two palm scans, three uncorrelated biometric samples should be utilised. This multimodal approach pushes system accuracy and security significantly further than any single-factor biometric alone.

Transparency and Limitations

While powerful, palm recognition is not a "silver bullet." It carries two primary limitations that must be kept in mind:

1. **Human Verifiability:** Unlike faces, humans cannot easily recognise or verify individuals based on their palms. Therefore, facial photos remain necessary for manual audits or human-in-the-loop verification.
2. **Onboarding Requirements:** Palms are not included in standard identity documents (like passports or ID cards). During the initial onboarding, the system must capture both the face and palms simultaneously to ensure the new palm templates are securely bound to the verified identity on the document.

User Journey: High-Security Transaction Verification

To understand how this looks in practice, consider the following scenario for a user performing a high-value financial transaction.

1. Secure Onboarding

The user begins by scanning their government-issued ID. To prevent "identity decoupling," a system should prompt the user to capture their **face and palms together in a single frame**. This creates a linked identity package where the palm data is permanently tied to the face on the ID.

2. Risk-Based Authentication

When a user initiates an operation, a risk engine should determine the necessary level of friction:

- **Low Risk:** (e.g., checking an account balance from a trusted device) The system requires only a quick **Face Scan**.
- **High Risk:** (e.g., a large wire transfer to a new recipient) The system triggers **Multi-Modal Verification**.

3. Verification Flow

For high-risk scenarios, the user follows a seamless, guided process:

- **Phase A: Face Capture:** A standard facial scan verifies the primary biometric.
- **Phase B: Primary Palm (Palmar & Dorsal):** The user holds up their dominant hand, showing the palm and then rotating it to show the back of the hand. This motion captures the 3D geometry of the hand.
- **Phase C: Secondary Palm (Optional):** For maximum-security environments, the user may be asked to repeat the process with their other hand to provide a third layer of confirmation.

4. Continuous Security Guardrails

Throughout this process, two "invisible" security layers should operate in real-time:

- **PAD (Presentation Attack Detection):** Confirms the hand and face are living tissue, not photos, screens, or masks.
- **IAD (Injection Attack Detection):** Ensures the video stream is coming directly from the physical camera and has not been intercepted or replaced by a software bypass.

A New Model for Trust

The future of remote identity verification may be less about perfecting a single biometric and more about designing adaptive journeys that balance risk, usability, and attack economics. Palms are compelling precisely because they can be introduced without rewriting the entire experience. In low-risk contexts, the system can stay face-first and fast. In high-risk contexts, it can step up to multimodal proof in an intuitive way.

If faces are the world's most public biometric, palms may be among the most practical "private" ones we can capture with today's devices. And in an era where attackers can obtain a face image as easily as a username, that distinction may be exactly what remote identity verification needs next.

Joined in 2019

Organisation: Innovatrics
Name: Jakub Sochor, CTO
Telephone number: +420 724 346 309
Contact details: jakub.sochor@innovatrics.com

20. iProov: Virtual Camera Attacks: The Hidden Threat to Remote Identity Verification

Native virtual cameras represent a critical threat vector in identity fraud – they bypass traditional security measures by operating within standard device permissions, making them effectively undetectable by conventional cybersecurity systems. These sophisticated yet easily accessible tools, some of which are available on mainstream app stores, run on smartphones, intercept the device's camera feed, and seamlessly inject deepfakes or synthetic content that appear as legitimate video streams to identity verification systems. This invisible threat exploded by 2,665% in 2024, transforming from experimental techniques to one of the most dangerous challenges facing remote identity verification worldwide.

The Alarming Rise: From Experimental to Mainstream

The evolution of the native camera attack has been rapid. It was first used in 2023 in a mainly experimental capacity with limited capabilities and few attempts. In early 2024, advances in tools increased, and they reached their peak later that year. The tactics changed yet again in 2025, with fewer but more targeted attacks as threat actors became selective.

What makes this progression particularly concerning is that it reflects the broader expansion and weaponisation of native virtual camera tactics across the threat landscape. Threat actors have moved beyond experimental probing to developing sophisticated, proven methodologies. Having demonstrated the effectiveness of these attacks, criminals have become increasingly strategic in their deployment and execution, systematically targeting organisations with vulnerable identity verification systems while sharing intelligence on successful breach techniques across global networks. Crime-as-a-service is developing alongside these methodologies as criminals share and sell their techniques.

How Native Virtual Cameras Trick the Operating System

Understanding how these attacks work shows why they're so difficult to detect and prevent. The sophistication lies not in complex hacking, but in exploiting the normal way devices handle camera permissions. By requesting legitimate camera access, often through apps available in mainstream app stores, the malicious software positions itself between the physical hardware and the target application at the OS level. This enables seamless system-level interception, allowing synthetic content, such as deepfakes or pre-recorded video, to be injected into the stream. Because the interception occurs deep within the device's video pipeline, the resulting feed retains authentic metadata and device characteristics, delivering fraudulent imagery that appears indistinguishable from a live, genuine camera stream.

Why Traditional Security Measures Fail

The sophistication of native virtual camera attacks poses significant challenges for conventional security approaches, as they operate entirely within the device's foundational blind spots. Unlike legacy injection methods that rely on "jailbreaking" or "rooting" to compromise a device, these attacks utilise legitimate application frameworks to intercept the video pipeline at the operating system (OS) level. Because they function within standard permission structures, they maintain impeccable metadata and device signatures that bypass conventional integrity checks. By the time the video reaches the authentication layer, the identity has been synthetically replaced while the digital signals appear perfectly valid. This shift from physical tampering to software-level mimicry renders traditional mobile security insufficient, as malicious camera apps are increasingly distributed through mainstream channels, turning the very tools we use to establish trust into vectors for impersonation across the consumer and workforce.

Furthermore, the discovery of a malicious camera application in a mainstream app store marks a significant milestone in the evolution of these attacks and has profound implications for security strategies. An app store presence gives these tools a veneer of legitimacy, dramatically increasing their potential for distribution, scalability, and reach.

Beyond Biometrics: A Cybersecurity Challenge

The rise of native camera attacks challenges the traditional categorisation of identity verification threats. These attacks exist at the intersection of biometric security and cybersecurity, requiring integrated defence strategies that address both domains.

Evidence from our threat intelligence clearly shows that robust defence requires both strong biometric liveness detection and cybersecurity measures working in concert. The attack patterns we observed suggest threat actors are actively exploring this dual-pronged approach, targeting weaknesses where these two security domains meet.

How To Defend Against Native Virtual Camera Attacks?

Effective protection against these sophisticated attacks requires a multi-layered approach that starts with visibility; you can't defend against what you can't detect. Identifying suspicious activity in real time is the foundation of any effective biometric defence.

1. Real-Time Managed Detection and Response

Perhaps most critically, organisations need continuous monitoring capabilities that can identify novel attack patterns in real-time. The rapid evolution of these threats means static defences quickly become obsolete. Security measures that can't adapt quickly fall behind the threat, allowing new attack types to slip through unnoticed. That's why managed detection and response, with real-time signals, is essential to keeping identity verification systems resilient.

2. Passive vs Active Liveness Detection

Traditional active liveness detection (based on challenge-response mechanisms like blinking or turning) is vulnerable to native camera attacks because it relies on predictable user actions that can be replicated. Its widespread use has driven demand for native virtual camera attack tools, as they're specifically designed to deliver the precise movements these systems require. On the other hand, passive liveness detection solutions avoid this vulnerability by not providing attackers with a predictable template of behaviours to replicate.

3. Device Integrity Verification

While root detection alone is no longer sufficient, comprehensive device integrity checks remain an important layer of defence. These should examine the entire video processing pipeline rather than just the device's root status.

The speed and sophistication with which native virtual camera attacks have grown represent a fundamental shift in the identity verification threat landscape. Their dramatic rise emphasises the urgent need for organisations to re-evaluate their security strategies and implement multi-layered defences that address this evolving threat.

The future of identity security lies not in any single technology but in comprehensive approaches that integrate biometric security, cybersecurity, and real-time threat intelligence. As these attacks continue to evolve, organisations must remain vigilant and adaptive, implementing security measures that can keep pace with the threats themselves.

Joined in 2018

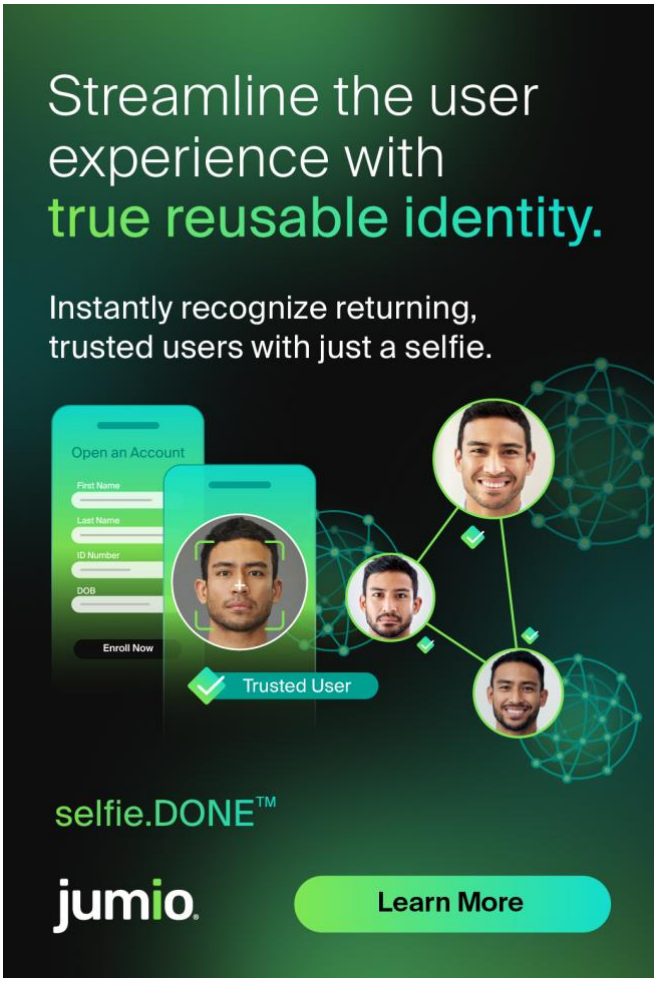
Organisation: iProov
Name: Louise Burke, Global PR Manager
Telephone number: 079 1717 6095
Contact details: louise.burke@iproov.com

21. Jumio: The Next Frontier: Reusable Identity at Scale

The identity verification market is at an inflection point. Five years ago, opening an account online and proving your identity simply by using a webcam or mobile phone to capture your ID and a selfie were still somewhat novel. Today, we not only expect this functionality — we want it to be even faster and involve a lot less friction. After all, if we've already proven our identity, why should we have to do it over and over again?

The Next Frontier of Identity Verification

Enter the concept of **reusable identity**. The purpose of reusable identity is to enable users to go through identity verification once and then be put in the fast lane for instant recognition in the future based on trust. This means that a user who has already onboarded using their selfie and ID at one business could onboard at another business with just a selfie, skipping the ID scan.



While a novel idea, the depth and scale to enable reusable identity in the real world is extremely complex. Implementing a truly effective and seamless reusable identity solution requires an intelligent, connected system that continuously learns, adapts, rewards trust, and defends against sophisticated, AI-driven fraud attacks without additional requirements from legitimate users.

Why Reusable Identity Matters

Reusable identity is a fundamental shift in the way people establish trust online. Traditional identity verification methods force even the legitimate users to repeat the same ID scan steps every time they onboard or need to reverify their identity. This repetition is well known to add the most friction, increase abandonment, and erode confidence.

Reusable identity solves these roadblocks by allowing verified users to skip redundant ID scanning steps while maintaining full fraud controls. The result is faster verifications, much higher conversions, and smarter security that adapts to risk in real time. Businesses that continue to rely on traditional identity verification methods will be left behind as customers grow increasingly intolerant of unnecessary friction.

Defining Reusable Identity (and Why Most Get It Wrong)

Many companies equate reusable identity with prefilled forms, credential wallets, or local or siloed identity systems. But true reusable identity is global, intelligent, dynamic, and rooted in trust signals, not stored credentials. It enables recognition and reverification in the background based on established trust across previously verified transactions rather than requiring new user actions. Governed by user consent and enterprise control, reusable identity is the perfect bridge between security, convenience, and digital trust-at-scale.

The Technology Making It Possible

The foundation of true reusable identity lies in intelligence. It hinges on the ability to connect signals globally across transactions, customers, industries, and time to distinguish between legitimate and fraudulent behaviour. Key enablers include biometrics, advanced liveness detection, global risk intelligence, and real-time trust evaluation and decisioning.

Delivering true, real-time reusable identity also requires fundamental change at the technology layer. It requires a new delivery platform that can address requirements around performance, reliability, connectivity and AI. The platform must be meticulously built using the right graph technology, which takes a highly efficient approach to modelling relationships and interconnected data to provide this intelligence. Because graph technology can unify data from legitimate and fraud interactions across industries and geographies, it creates a continuous learning model of trust. This approach ensures every reuse decision is risk-aware, with built-in seamless fallback to full, high-friction ID verification when risk is detected.

Furthermore, this approach allows businesses to verify users without exposing data or relying on federated networks. Historically, providers could facilitate data reuse between clients, but today's technology enables providers to act as the custodian of verified identities under a single security model. By minimizing data sharing and reuse of personal documents, you can actually reduce exposure and enhance user privacy. Consumers retain transparency and consent, while enterprises gain a trusted, compliant custodian of digital identity.

The Business Impact

The business impact of reusable identity is immediate. When trusted users can skip unnecessary verification steps, they have a much better experience, and businesses see higher conversions and lower abandonment. Additionally, risk and fraud teams gain stronger, data-backed protection through cross-industry intelligence. Industries such as gaming, banking, fintech, and e-commerce are seeing the biggest impact, where speed and trust drive competitive advantage. With stiff competition in these industries, true reusable identity is quickly becoming essential.

The shift to reusable identity also creates a foundation for ongoing customer relationships. With trust established and instantly reasserted every time the customer interacts with your business, you provide an outstanding user experience that increases loyalty and smooths the path for expansion. For example, if a bank allows an existing checking account customer to open a high-yield savings account with a single click, that customer is much less likely to go through a lengthy account-opening process somewhere else.

Looking Ahead

The future of onboarding will belong to companies that treat identity as a living, intelligent signal of trust, not a point-in-time check. Dynamic workflows should remove ID scans and other high-friction checks for trusted users and introduce just the right amount of checks at the right time for everyone else. Trusted users must be instantly recognised and reverified across businesses with just a selfie powered by biometrics and advanced liveness detection, eliminating the need to rescan their ID for every new onboarding or verification. This approach doesn't just revalidate their identity; it intelligently recognises and re-verifies users based on real-time identity intelligence.

When implemented through a secure, intelligent, global and privacy-first solution, reusable identity holds the key to building trust online at scale, without the trade-offs.

Joined in 2019

Organisation: Jumio
Name: Abhijeet Singh, Director of Product Management
Telephone number: +44 747 423 8544
Contact details: abhijeet.singh@jumio.com

22. Paravision: Biometrics, Borders, and Travel: Is Seamless Travel Here?

Introduction

As global passenger volumes continue to rise, airports and border authorities face the dual challenge of maintaining security while ensuring efficiency and traveller convenience. Long lines, manual checks, and document verification can slow operations, frustrate passengers and staff, and increase operational costs. Emerging biometric technologies and digital travel credentials promise a new era of seamless travel. But is it truly here? Evidence from early deployments suggests that the building blocks for frictionless, secure journeys are already in place.

Electronic Travel Authorisations: Pre-Arrival Verification

Electronic Travel Authorisations (ETAs) are reshaping how countries manage entry. By screening travellers before arrival, ETAs enable digital identity verification and risk assessment, reducing reliance on in-person inspections. Travellers submit personal and biometric information online and receive digital authorisation to enter the country.

The UK Home Office's ETA program illustrates the scale and impact of such systems. Over 19.6 million ETAs have been granted, enabling eligible visitors to gain entry with minimal disruption. Applicants use a smartphone or web portal to scan their passport and capture a biometric image, verified against passport data with biometric technology. Manual verification has decreased by more than 50%, and most applicants receive results within days. Other countries, including the United States, Canada, and Australia, have similarly deployed ETA-style programs. The European Union is preparing to launch the European Travel Information and Authorisation System (ETIAS) in 2026, covering travellers from over 60 countries and processing an estimated 30 million applications annually.

ETAs demonstrate how pre-arrival verification improves efficiency and security. By confirming identity before travellers reach borders, authorities can prioritise resources, reduce congestion at checkpoints, and mitigate fraud. Accuracy, inclusivity, and privacy remain essential: effective ETAs must perform consistently across demographics, secure sensitive data, and maintain public trust. When these conditions are met, ETAs form a foundational component for seamless travel.

Airports Leading the Way

While ETAs handle pre-arrival verification, airports are pioneering near real-time, frictionless identity systems such as the Contactless Corridor.

Orlando International Airport has recently started a pilot program for biometric technologies, including a Contactless Corridor. This corridor will allow travellers to pass through without stopping to show passports or tickets. Networked cameras track passengers in motion, combining facial recognition with 3D tracking to verify identities efficiently. Optional participation for domestic travellers and mandatory verification for foreign nationals ensures that both operational efficiency and security requirements are met.

Early observations show the promise for reduced bottlenecks, smoother flow for families or complex itineraries, and minimised friction without compromising safety.

Dubai International Airport provides another instructive example. Its Red Carpet Smart Corridor enables passengers to move through immigration without presenting travel documents, even in a highly diverse passenger population. By integrating facial biometrics with advanced travel systems, the smart corridor can support high throughput flows while maintaining accuracy and oversight. Dubai offers a glimpse of the future of travel: intuitive, frictionless journeys where technology quietly enhances efficiency and security, setting a benchmark worldwide.

Together, these deployments show that frictionless travel is happening now. Automated, on-the-move verification reduces wait times, systems scale to high volumes without major infrastructure changes, opt-in designs maintain privacy, and inclusive performance ensures equitable experiences for all travellers.

Challenges and Considerations

Despite these advances, implementing seamless travel is not without challenges. Accuracy remains paramount: even small error rates can create bottlenecks or undermine public trust. Systems must be robust across age, gender, and ethnic groups to ensure equitable treatment and operational reliability.

Data privacy and security are also critical. Biometric systems collect sensitive personal information, and in-scope travellers must be confident that their data is securely stored, processed, and protected. Transparent governance, regulatory compliance, and ethical frameworks are essential for adoption at scale. Public trust is central. Travellers need clarity on how their data is used, the benefits of participation, and their rights. Inclusive design, clear opt-in processes where legally possible, and transparent communication are critical to ensuring both uptake and equitable outcomes.

Lessons Learned and Emerging Best Practices

Several insights emerge from early ETA and airport deployments:

1. **Pre-arrival verification reduces bottlenecks:** ETAs streamline checkpoints before travellers arrive.
2. **On-the-move biometrics enhance flow:** Contactless corridors demonstrate that real-time, high-throughput verification is feasible.
3. **System integrity must be protected:** Widespread biometric use increases spoofing risks, making PAD and deepfake defences essential to ensuring genuine verification.
4. **Inclusive design is essential:** Accuracy across demographics prevents delays, security gaps, and ethical risks.
5. **Transparency fosters trust:** Clear communication about data use and privacy encourages engagement.
6. **National-scale infrastructure enables consistency:** Centralised biometric services can support multiple ports of entry and exit, enabling consistent verification across travel ecosystems.

These lessons show that seamless travel is achievable when technology is paired with operational design, ethical governance, and public engagement.

Conclusion: Is Seamless Travel Here?

The answer is affirmative. Global deployments for traveller authorisation and in-airport processing show that biometric solutions reduce friction, enhance security, and scale for high volumes. Seamless travel is not a single technology but a system of coordinated processes. When combined thoughtfully, travellers move more quickly, security agencies operate more efficiently, and passenger experience improves. The future of travel lies in expanding these models, refining system accuracy, and maintaining public trust. As early deployments demonstrate, the technology exists, operational lessons are clear, and frictionless travel is already underway.

Joined in 2021

Organisation: Paravision
Name: Ella Nuutinen, Director of Marketing
Contact details: ella@paravision.ai; info@paravision.ai

23. Regula: Making Fraud Near-Impossible: Robust Remote Identity Verification

Remote identity verification often begins with a camera session where a person claims their identity and presents evidence. That same session is also a target: synthetic faces, pre-recorded media, and AI-generated document images are used to push the process toward its weakest step.

Luckily, there are a range of measures organisations can take to make their ID verification truly effective.

Start with liveness

Many teams begin with the document photo. In higher-fraud environments, starting off that way often wastes effort because a pre-recorded clip or deepfake can trigger retries and manual review before anyone has even confirmed there is a live person on the other side. A liveness gate up front filters out many synthetic attempts early on, plus it sets up cleaner binding to the document and, later, to an identity record.

- **Active liveness relies on user interaction.** It asks the user to react to prompts — something that video-replay and mask-based spoofs will struggle to do.
- **Passive liveness relies on analysis of the capture itself.** It looks for red flags without prompts, which can reduce friction but depends heavily on capture quality. Red flags include frame-to-frame consistency cues such as unnatural motion patterns, lighting and shadow behaviour, skin texture detail, and artifacts that often appear in screen replays or synthetic video.

Treat each session as single-use: accept live input inside a short time window, validate server-side consistency signals, and watch for signs of video replay, injection, or synthetic streams.

Confirm the document is physical

Remote verification depends on document authenticity checks and on binding biometrics to the document record. If a flow extracts and validates data before it has confidence that the document is a physical artifact, it can approve clean data that came from a manipulated image.

Document liveness catches printouts and screen replays by checking physical characteristics and security features that are difficult to simulate convincingly, including dynamic elements such as holograms. Glare, low light, and low-end cameras can hide those cues and drive repeated attempts, so it's critical to include quality gates, capture guidance, and a supervised fallback.

Use NFC reading for biometric documents (when available)

A biometric passport or eID card can provide chip-backed evidence that a document photo cannot imitate easily. When NFC reading is available, chip verification can become a high-confidence branch in the decision logic, especially where document images are likely to be attacked by strong forgeries or AI generation.

Chip reading should be cross-checked against what was read visually and in the machine-readable zone, and verified with passive, active, or chip authentication to confirm that the chip has not been cloned or altered. In remote scenarios, a zero-trust stance toward mobile devices helps: re-check key results in a controlled environment, such as a private cloud or a company's on-premises infrastructure.

You should also confirm that all sources agree, including the primary and secondary portrait and the live selfie.

When NFC is not available, define an alternate route, such as supervised capture or agent-assisted review, so "no NFC" does not quietly turn into a lower-security path.

Deepfake resistance through cross-checks

Many IDs carry more than one portrait, and electronic documents may provide both printed and chip portraits, so compare the live selfie to each relevant portrait source and treat disagreements as high-signal events. Weak matching that slips through creates a predictable gap that attackers will probe with synthetic selfies that resemble one portrait but fail against the others.

Where lawful and proportionate, biometric search and external data-source checks can add confidence after the document and selfie have already been bound.

Age verification: Define the claim, then retain the minimum

Age checks fail when they are treated as a single feature rather than a policy-backed decision with routing and safeguards. A useful pattern is a "challenge age" buffer above the legal threshold: users clearly above the buffer take a low-friction path, while users near it move to higher certainty, such as document-based date-of-birth confirmation or a privacy-preserving proof that confirms "over threshold" without exposing a full birth date.

Closing: Build a stable evidence chain

Remote identity verification succeeds when the flow stays stable under attack. Using liveness first reduces synthetic noise early, document and document-liveness checks stop the system from trusting polished artifacts, and NFC chip verification can add a strong anchor when available.

Cross-checking portraits and, where permitted, adding biometric search and external corroboration makes it harder for deepfakes to pass as a single clean signal, while clear fallbacks keep legitimate users moving.

Joined in 2019

Organisation: Regula
Name: Andrey Terekhin, Head of Product
Telephone number: +48 571 447 241
Contact details: andrey.terekhin@regulaforensics.com;
julia.oganova@regulaforensics.com

24. SAIC: A 'Real' Look at Evaluating Biometric and Identity Systems for Remote Identity

The biometrics and identity landscape is rapidly evolving as advances in artificial intelligence make it possible to perform biometric recognition at scale, including to reduce fraud in online transactions. Remote identity systems expand access and convenience, but they also introduce new risks. Even as biometric technologies reach higher performance benchmarks, threats such as deepfakes, digital injection attacks and uneven performance across devices and demographic groups can undermine public trust and real-world effectiveness of biometric systems.

To preserve the security and fraud fighting potential of remote identity systems, they must operate consistently and reliably across diverse environments and user populations. Independent verification of vendor performance claims is essential to maintaining public confidence, confirming security can be maintained while ensuring low user rejection rates.

Why Rigorous Biometric Evaluation Matters

Operational performance in biometric and identity systems, including remote identity systems, must be measured accurately, quickly and consistently to keep pace with technological change. Independent research from government, industry and academic sources highlights persistent performance gaps that can reduce usability and erode trust.

Key findings include:

- **Demographic variation:** A recent General Services Administration study found that the median true accept rate for genuine users was only 85% across five tested systems, with significant differences in performance across demographic groups.[1]
- **High user rejection rates:** The Department of Homeland Security Science and Technology Directorate evaluated 3,024 combinations of presentation attack detection, face recognition and document validation technologies. The median system accepted only 46% of genuine users, and fewer than 1% of combinations met both security and user facilitation targets.[2]
- **Device and environment sensitivity:** Research shows that user devices, document types and testing conditions affect system performance, with direct implications for reliability and public confidence.[3]

Taken together, these findings show that capable technologies do exist. However, success depends on strategic ongoing evaluation and selection of system components. Deployment of a system to meet compliance requirements, absent independent evaluation, does not provide assurance of acceptable performance. Performance verification before deployment and throughout operations is required to ensure systems perform as expected and continue to meet real-world demands.

Barriers to Effective Biometric Testing

Despite its importance, comprehensive testing of biometric and identity systems remains challenging for many organisations due to several barriers, including:

- **Data privacy and access:** Limited availability of sequestered data that reflects real-world conditions makes reliable and repeatable testing hard to achieve.
- **Cost and complexity:** Testing at scale is expensive and requires specialised expertise. Fragmented system architectures further complicate evaluation, particularly when security and user facilitation must be assessed independently.

---

[1] Center for Identification Technology Research. (2024) *"A Large-Scale Study of Performance and Equity of Commercial Remote Identity Verification Technologies Across Demographics."* arXiv preprint, https://arxiv.org/pdf/2409.12318

[2] DHS Science and Technology Directorate. (2025) *"A Quantitative Framework for Evaluating Remote Identity Validation Systems: Technical Demonstration Analysis and Evaluation."* DHS S&T Technical paper series, https://www.dhs.gov/science-and-technology/publication/quantitative-framework-evaluating-remote-identity-validation-systems

[3] SAIC Identity and Data Sciences Laboratory. (2026) "*Robustness of Presentation Attack Detection in Remote Identity Validation Scenarios.* arXiv preprint, https://arxiv.org/abs/2602.00109

- **Reliance on vendor-led testing:** Performance claims provided by vendors may not reflect operational use or are often difficult to compare across solutions.
- **Resource constraints:** Many organisations lack the funding and capacity to build and maintain in-house testing capabilities.

These barriers limit informed decision-making and increase the risk of deploying systems that fall short in operational environments.

A Path Forward: Testing as a Service

Collaborative, independent testing as a service (TaaS) solutions provide a practical way to address challenges and build confidence in biometric and identity systems. Effective test service providers deliver scalable, objective testing that supports operational readiness and informed decision-making. With the right test infrastructure in place, teams can conduct rapid, repeatable evaluations at scale, producing performance metrics trusted by both government and industry organisations.

1. **Continuous testing without disruption:** TaaS enables repeatable testing processes using sequestered data collected in simulated operational environments, without interfering with day-to-day activities. Clients can establish a testing cadence aligned to their needs, while the competent test service provider brings the testing infrastructure, expertise and innovation to bear for the client.
2. **Component-level insights:** By evaluating individual subsystems such as presentation attack detection and face recognition, TaaS provides clearer visibility into what is performing well and where limitations exist, helping decision-makers identify weaknesses, isolate bottlenecks and target improvements.
3. **Standards-based evaluation:** Established biometric standards provide a common framework for understanding performance metrics, allowing clients to assess and compare technologies on equal footing.
4. **Sequestered data testing:** Unlike vendor testing that may rely on reused training data, independent TaaS evaluation uses protected, operationally relevant datasets that better predict real-world performance.
5. **Streamlined procurement:** Regular assessment of commercial solutions outside of a specific acquisition cycle provides early insight into performance trends, helping shorten procurement timelines and adapt technology selection to dynamic threats and innovation.

Test Early. Test Often.

Ongoing testing helps ensure biometric and identity systems continue to meet requirements as technology evolves and attackers introduce new techniques. Changes made after deployment can unintentionally degrade performance if issues are not identified early. A testing as a service framework supports continuous, scalable evaluation to reduce risk and protect mission-critical operations.

Conclusion

Biometric systems for remote identity offer significant promise, but they also face real challenges in delivering accurate, secure and reliable performance. Meeting operational demands and sustaining public trust requires ongoing evaluation. Testing as a service supports informed technology selection and monitoring while reducing risks tied to demographic disparities, environmental variations and emerging threats. Through an agile, standards-driven testing approach, clients are empowered to make data-driven decisions that strengthen identity solutions and user confidence.

Organisation: Science Applications International Corporation (SAIC)
Name: Yevgeniy Sirotin, Technical Director, SAIC Identity and Data Sciences Laboratory (IDSL)
Telephone number: +1 781 710 3472
Contact details: yevgeniy.b.sirotin@saic.com
Name: Jerry Tipton, Executive Director, Integrated Security Technologies and Programs
Telephone number: +1 301 909 9263
Contact details: jerry.l.tipton@saic.com

25. Signicat: From Static Images to Secure Identity: Why Video + NFC Is the Future

Identity fraud is rising—and faster than many onboarding and verification systems can realistically adapt. Advances in artificial intelligence, particularly generative models like DALLE-3 from OpenAI or Nano Banana from Google, have dramatically lowered the cost and complexity of producing convincing fake identities that can bypass optical verification technologies. At the same time, many organisations still rely on photo-only identity verification as a primary trust signal. In today's threat landscape, this approach is increasingly hard to defend, even where regulations require nothing more than a photo. Chasing so-called "bad AI" with "good AI" is an arms race the defending side cannot win, constrained by ethics and regulation while attackers remain unburdened and highly motivated. Fraud techniques that were once niche, expensive, and technically demanding are now cheap and widely accessible.

Why photo-based identity verification is no longer enough

Photo-only verification systems were designed for a very different threat model. They assume that images are costly to forge at scale and that visual inspection—automated or manual—can reliably distinguish between genuine and fraudulent documents. That assumption no longer holds.

Modern deepfake and image-synthesis techniques generate high-resolution facial images, replicate document textures, and simulate lighting, ageing, and wear with alarming accuracy. Even when combined with basic "liveness" checks, static-image workflows remain vulnerable to replay attacks, image injection, and synthetic identity creation.

For fraudsters, the economics are compelling: a single generated identity can be reused, modified, and scaled across multiple platforms. For defenders, each additional image check yields diminishing returns.

The deepfake inflection point: why now is different

What makes the current moment distinct is not merely incremental improvement, but a structural shift. Publicly research and tooling made in 2025 and 2026 show that new generative and diffusion-based models can produce identity documents and facial imagery with minimal human intervention. These models preserve fine-grained details such as shadows, reflections, features traditional detection systems rely on.

Crucially, the skill and cost barrier has collapsed. Tasks that once required expertise can now be performed with pre-trained models and modest computing. This is no longer a game of isolated bad actors it is widespread. Deepfakes are no longer used solely for external fraud; they are increasingly deployed to *infiltrate organisations from within*. Threat-intelligence reporting has documented North Korea–linked actors using **AI-generated synthetic identities to secure remote technical roles at Western companies**. These personas included fabricated photos, tailored CVs, and consistent online histories, allowing candidates to pass screening, background checks, and even live video interviews.

In several cases, attackers successfully gained employment and legitimate system access, which was later used for espionage, financial fraud, or malware deployment. Crucially, these schemes exploited onboarding processes that relied on photo- or video-based verification without cryptographic document validation or authoritative data checks.

This example highlights a fundamental shift: attackers are no longer merely bypassing controls, they are **operating convincingly within them.** When identity verification focuses on visual plausibility rather than authoritative proof, even interactive verification can be deceived.[1]

Video: a necessary but insufficient evolution

Video-based identity verification represents an important step forward. Unlike static images, video introduces temporal signals, motion, depth cues, and behavioural responses — that significantly raise the bar for attackers. Modern video-

[1] *Reference: Palo Alto Networks Unit 42*

based liveness checks can detect inconsistencies that remain invisible in still images and reduce many common presentation attacks.

However, video alone is not a silver bullet. Real-time synthetic video, advanced injection techniques, and replay frameworks continue to improve. While video reduces risk, it still operates within the same fundamental paradigm: analysing what the identity *looks like*. To move beyond this limitation, identity verification must incorporate signals that cannot be convincingly generated.

NFC and cryptographic proof: anchoring trust in reality

This is where NFC-based identity document verification becomes transformative. Modern passports and national identity cards contain signed data issued by trusted authorities. When read via NFC, this data can be validated for authenticity and integrity with certainty, something no image or video can replicate on its own. It adds a layer of cryptographic proof in a digital world.

By combining video-based biometrics with NFC verification, organisations shift from visual plausibility to cryptographic proof. The face captured on video is no longer assessed in isolation; it is matched against data that is mathematically bound to an official identity document.

This layered approach allows for trade-offs to be picked between security and ease of use. Real-world government adoption, such as the **EU Entry/Exit System**, reflecting a broader European move towards combining biometrics with chip-based document verification at scale.

Authoritative data as the third trust layer

Even video biometrics combined with NFC-based document verification answers only part of the identity question: *is the document genuine, and does the person presenting it appear to be the rightful holder?* What they do not fully address is whether the identity itself is *current, valid, and consistent across authoritative sources*.

This is where individual data from national eID schemes and trusted population registries become a critical third layer. Attributes such as legal name, date of birth, address status, document validity, and in some jurisdictions, life-status or residency indicators provide context that biometrics alone cannot supply.

When verified directly against authoritative sources and used as signals rather than copied or stored, these data points significantly reduce the risk of synthetic identities and recycled credentials. Correlating biometric matching, cryptographic document validation, and authoritative data moves onboarding from appearance-based trust to evidence-based assurance.

The future of secure digital onboarding lies in layered approach of combining **video-based biometrics**, **NFC-verified identity documents**, and **authoritative individual data points** from trusted sources. In a world where faces can be fabricated and documents can be visually forged at scale, trust must be rooted not in what an image appears to show, but in what can be cryptographically and authoritatively proven.

For organisations serious about long-term fraud prevention, the transition from static images to layered, evidence-based identity systems are no longer optional. It is inevitable.

Organisation: Signicat
Name: Mite Mitreski, CTO
Telephone number: +46 768 792 122
Contact details: mite.mitreski@signicat.com

26. SITA: Factoring in The Human Factor

If you've ever tried to verify your identity on a mobile app, you know the experience can go either way. Sometimes it works smoothly. Other times you tilt your phone in three different directions, blink twice, and wonder why technology still struggles with a simple photo.

Remote identity verification has become part of everyday life. Banking. Healthcare. Online shopping. And now travel. As smartphones get better and biometric standards mature, governments are turning to mobile solutions to help travellers prove who they are before they even start their journey.

This shift brings huge benefits. It also brings a simple truth: the human experience matters as much as the technology behind it.

What really happens behind the scenes

Modern travel permission apps, including Electronic Travel Authorisation (ETA) apps, use a secure authenticated portrait. It sounds complex, but the idea is straightforward. The app checks that the document is genuine, then checks that the person holding the phone is the same person in the document.

Under the hood, there are NFC chips, international standards from ICAO and ISO, and a series of biometric checks. All of this reduces the risk of someone pretending to be someone else. But even with strong technology, largescale, real world use shows something important: people will judge the whole system based on their experience in those first few minutes.

If the process feels confusing or slow, frustration shows up quickly in app-store reviews and public forums.

Designing for real people

Mobile identity verification works best when the technology and the human experience are designed together. Early biometric systems taught us that success depends not only on accuracy, but on how easy the process feels to the person using it.

That means working closely with designers, engineers, and real users. Watching how different people hold their phones. Seeing where they hesitate. Noticing which steps feel intuitive and which ones don't.

Experience is a powerful teacher. And solutions become stronger when they are shaped by diverse groups of real travellers in real conditions.

Testing that goes beyond the lab

The biometric industry has an important responsibility: to make sure these tools perform well for everyone. Standard testing is necessary, and large independent evaluations, such as those done by NIST, help buyers compare technologies.

But the real test happens outside controlled environments. It happens when thousands of people, using hundreds of device types, try to complete their identity check after a long day of travel or in a country where connectivity is limited.

Largescale, real-world testing is harder and more expensive, but it is where the biggest lessons come from.

Where travellers feel the impact

Reports from across the industry, including the Biometric Institute's 2025 "Concepts and Solutions Report," highlight the fast rise in travel apps offering mobile identity verification. Travellers now use these tools for everything from ETAs to loyalty programs.

The benefit is clear. People can securely verify their identity from wherever they are, choose what personal information they share, and move through parts of the journey with more control and privacy. But there's a challenge too. Many travellers end up juggling multiple apps and repeating similar steps in different places. When the experience becomes too fragmented or too demanding, adoption drops.

This is where thoughtful design matters most.

Putting user experience at the centre

To build solutions people actually want to use, providers need more than strong technology. They need design frameworks that can adapt to different use cases, and test environments that show how these apps behave across many devices and conditions.

Detailed analytics also play a big role. Where do people struggle to take a good photo? Which phone models have trouble reading passports? What causes someone to abandon the process halfway through?

When we understand these moments, we can improve them. And when the design is grounded in real expertise and real experience, the entire ecosystem becomes stronger and more trusted.

Remote identity verification has the potential to make travel smoother, safer, and more personal. But its success will always come back to something simple: how it feels for the person holding the phone.

Joined in 2011

Organisation: SITA
Bill Perry, Senior Manager/Biometric SME
Telephone number: +610499717784
Contact details: Bill.Perry@sita.aero

27. Speed Identity: From Counter to Kiosk: Scaling Live Enrolment with Automation

As governments strengthen identity management frameworks in response to terrorism threats, identity theft, and national security demands, biometrics have become a core component of secure identity document issuance. The trust placed in modern identity documents depends heavily on the integrity of the biometric data. Yet in many countries, enrolment still relies on applicant-submitted photographs, whether digital or printed, which introduces manipulation risks, inconsistent quality, and costly inefficiencies.

The next practical step is not only live enrolment, capturing biometrics in person under issuing-authority control, but making live enrolment as self-service as possible. With the right automation, issuing authorities can strengthen capture integrity while meeting modern expectations: convenient access, minimal waiting, and consistent outcomes at scale.

Why self-service enrolment matters now

Traditional operator-led enrolment is increasingly difficult to scale. It is staff-intensive, appointment-bound, and sensitive to demand spikes caused by renewal cycles, policy changes, or disruptions. Each manual step increases cost and reduces throughput. Meanwhile, applicants increasingly expect public services to work like well-designed digital services; fast, and available beyond office hours. Self-service enrolment via kiosks or 24/7 service points addresses this gap.

Live enrolment is recommended because it reduces manipulation risks by requiring physical presence and giving the issuing authority control over the data chain, from sensor to secure document. In a self-service model, the same control objectives apply, but the system replaces many human tasks with automated controls.

A well-designed self-service enrolment station should function like a closed loop system: it instructs users, measures quality, and only accepts images that meet strict requirements. This matters because the primary threats to biometric trust; image manipulation and poor quality, are best mitigated at the point of capture, not after the fact.

What automation must do in a self-service enrolment system

To support resilient, scalable identity frameworks, automation should make the enrolment process secure by design and easy by default: minimising reliance on staff, minimising rework, and maximising consistency.

Key automation capabilities include:

1. Guided capture with real-time feedback that prevents failure - Self-service must be instructional, not punitive. The system should provide real-time feedback and guide the applicant to a compliant pose. This reduces rejection loops and prevents the cycle of repeated events that undermines quality.
2. Automatic compliance and quality verification - Instead of a staff member judging whether the photo “looks OK”, the system should automatically validate the parameters that drive biometric performance. Only compliant captures should proceed.
3. High-quality, standards-aligned capture hardware - Automation cannot compensate for weak sensors. For self-service to scale, capture hardware must be purpose-built: high optical resolution, low radial distortion, and controlled illumination to ensure consistent facial detail across diverse users.
4. Chain-of-custody controls that reduce manipulation risk- Self-service does not mean “uncontrolled”. The issuing authority still needs confidence in the origin and integrity of the data. Automated systems should secure the path from sensor to backend—so the biometric record is created, verified, and transmitted without opportunities for substitution or tampering.
5. Automated identity verification during enrolment - A major advantage of automation is that verification can happen immediately. The live-captured biometric can be used to verify the person against existing records before the application is processed and before a new document is issued. That reduces downstream fraud, accelerates approvals, and increases confidence in issuance decisions.

Future-proofing means designing for scale, threat evolution, and convenience

Identity management frameworks must withstand two accelerating forces: rapidly improving AI-enabled fraud and rising expectations for seamless digital and physical services. Self-service, automated biometric enrolment is the practical intersection of both needs. It improves security by controlling capture and chain of custody, and it improves service delivery by reducing dependency on counters, staff, and repeated appointments.

The strategic conclusion is clear: the most resilient identity systems will be those that treat enrolment as a high-integrity, automated self-service workflow—capturing biometric data under controlled conditions, validating it instantly, and producing trustworthy records that remain reliable for years of identity verification to come.

Joined in 2019

Organisation: Speed Identity
Name: Tomas Norling, CEO
Telephone number: +46 733 500 823
Contact details: Slakthusgatan 9, SE-121 62 Johanneshov, Sweden,
tomas.norling@speed-identity.com

28. Thales: AI and Biometrics: The pathway to trusted identity in the age of deepfakes

The proliferation of artificial intelligence has unlocked unprecedented benefits but also exposed the global identity ecosystem to complex new threats. Deepfake, those hyper-realistic, AI-generated images, videos, and audio, are being used for misinformation, fraud, and attacks against biometric systems. As synthetic content continues to rise, so too does public concern about the reliability and ethics of digital identity verification and authentication solutions. The biometrics industry must respond by refining technical defences and fostering greater transparency and trust.

Understanding the Challenge: Deepfakes and Synthetic Attacks

Recent studies illustrate an alarming disconnect between the surge in deepfake content and our ability to recognise it. While projections suggest that 8 million deepfakes could be published online in 2025[1], compared to just 500,000 in 2023, and Europol warns that as much as 90% of online content might be synthetically generated by 2026[2], humans are able to correctly identify deepfake videos less than a quarter of the time[3]. This widening gap between the volume of deepfakes and our detection capabilities is further compounded by the fact that phishing campaigns now increasingly leverage AI, raising significant concerns about the future of digital trust.

In identity verification, these trends pose real risks. Morphing attacks, which use generative AI or image processing to blend two faces into a single image, threaten the integrity of border control and document verification systems. A morphed image can match both original subjects, potentially enabling two individuals to use the same passport undetected.

AI's own dual nature is at the heart of this challenge. Generative AI, the technology that enables deepfakes, is also essential for legitimate applications, such as fraud detection, document security, and advanced recognition. However, its misuse for synthetic manipulation, spoofing, or backdoor attacks raises cybersecurity threats connected to broader digital risks.

Responding to an expanding threat landscape

Biometric systems face a variety of sophisticated attacks. These can target every stage of the biometric process, from presenting the image, to feature extraction, to matching, and even to final decision-making. Fraudsters may attempt to override algorithms, tamper with reference databases, or modify comparison scores.

Presentation attacks involve a perpetrator presenting an image or a face, for example a 3D mask, to fool a facial recognition system. Injection attacks occur when manipulated image or video data is fed directly into a system, bypassing the live capture process. Morphing attacks, as described above, facilitate identity fraud, notably at national borders. Backdoor attacks are another threat. The proliferation of open-source models and datasets has heightened the risk of AI backdoor insertion in facial recognition systems as, in the absence of rigorous cybersecurity assessment, attackers may introduce malicious triggers or exploit corrupted training data to compromise identification.

To counter these risks, the biometrics industry has developed layered defences. Presentation Attack Detection (PAD) algorithms, trained to distinguish genuine faces from spoofs or masks, are now integrated into identity document issuance and border control systems, enhancing the detection of inconsistencies between live captures and ID photos. They effectively strengthen remote identity verification processes. Additionally, algorithms for detecting morphing attacks (MAD) and deepfakes are being developed and improved to increase the robustness of biometric systems.

---

[1] Children and deepfakes, Think Tank – European Parliament, NEGREIRO ACHIAGA Maria Del Mar, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf

[2] Facing reality? Law enforcement and the challenge of deepfakes, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

[3] https://deepstrike.io/blog/deepfake-statistics-2025

Recognising the elevated risk of AI backdoors, organisations are prioritising deep integration of robust cybersecurity: encryption, systematic algorithm testing, data integrity verification, and detailed audit trails are standard operating procedures. Ongoing research and collaboration among industry, government, and standards bodies further reinforce these safeguards and strengthen systems against fraud.

With these evolving solutions, the industry is fortifying every stage of biometric processes against tampering and synthetic attacks, building trust and resilience as biometric technologies grow in scale and complexity.

Evolving governance and transparency

Technology alone is not enough. As synthetic threats grow, the biometrics industry is collaborating to establish new governance frameworks and standards. Greater transparency in how biometric solutions work, how data is handled, and how decision-making processes are monitored is essential to securing public trust. Regulatory initiatives are pushing providers to explain and audit their AI models, address bias, and guarantee ethical use.

Industry-wide initiatives now emphasise privacy-by-design, explicit user consent, and minimisation of personal data. Responsible actors are increasingly adopting approaches that foster greater public confidence in biometrics and digital identity. Approaches designed to ensure transparency, understandability and ethical use, help to guarantee that biometric systems are not just secure but also trustworthy and respectful of user rights.

The road ahead

The pathway to trusted identity in the age of deepfakes is a shared journey for the entire biometrics ecosystem, which demands a balanced approach that transcends the boundaries of individual organisations. Facing the accelerating risks of synthetic content and deepfakes, the biometrics industry is responding with a blend of technical innovation, rigorous security, and improved transparency. Tested solutions for morphing and presentation attack detection, backdoor risk analysis, and integrated cybersecurity are already showing their value. Lessons learned from real-world deployments make clear that securing digital identity is not only a challenge of technology, but also of responsible stewardship and global collaboration. By investing in robust detection methods, ongoing education, and transparent governance, the industry can maintain trust in biometric authentication and verification even as AI reshapes the landscape of digital identity.

Joined in 2013

Organisation: Thales
Name: Sandra Cremer, Biometrics Research and Technology Leader
Telephone number: +33 1 55 01 62 58
Contact details: sandra.cremer@thalesgroup.com

300+

programs worldwide

rely on Thales identity and biometric solutions

thalesgroup.com

THALES

Building a future we can all trust

29. Travizory: Biometrics, Borders, and Travel: Is Seamless Travel Here?

For decades, the travel industry has grappled with its vision of a “seamless journey” - where a traveller moves from their home, to the boarding gate, and across an international border with just their face as a passport. Today, this is still being discussed as a futuristic ambition. However, the evidence from the field suggests that the future has not only arrived but is already being operationalised at scale.

Shifting from Checkpoints to Intelligence Hubs

Historically, border security was defined by physical barriers and manual checks. Officers were forced to make security decisions based on limited information and under intense time pressure. Today, the paradigm has shifted. The border has been digitalised and exported, enabling security screening and risk assessment from the moment a traveller plans their trip.

The rapid adoption of “smart border” programmes and electronic travel authorisation systems worldwide is further evidence of this shift. By combining data and insights from carriers and travellers themselves, governments can move the "heavy lifting" of security upstream to ensure that 100% of all arrivals are thoroughly screened and vetted.

Embracing the Power of Biometrics

The true litmus test for seamless travel lies in its implementation. When identity is verified and travellers are risk-assessed days or weeks before arrival, the physical border crossing can be transformed from a bottleneck into a high-speed transit point.

The holy grail of seamless travel has long been a truly secure, non-stop experience, where a face is all that is required to cross international borders. Deployments in the UAE, Singapore, St Kitts and Nevis and the Seychelles are already putting this concept into action – proving that seamless travel has well and truly arrived. Biometric corridors enable a contactless, automated border control alternative, and represent a quantum leap beyond traditional Automated Border Control (ABC) gates.

While eGates often require a "stop-start" motion—placing a passport, standing still for a photo, and waiting for the gate to open—biometric corridors allow for "matching in motion." High-speed cameras capture facial biometrics in real-time, matching them against the pre-cleared digital profile created during pre-travel enrolment.

The UAE launched its AI-powered smart tunnels, which match travellers to a pre-registered profile. Currently, this technology is in use within the First and Business Class lounges of Terminal 3, with plans for wider implementation. Similarly, Singapore’s Changi Airport rolled out biometric corridors for known travellers, like citizens and residents. In the Republic of Seychelles, Africa’s first walk-through biometric corridor-enabling, passport-free entry for citizens.

The success of these deployments reinforces that the technology is ready, and travellers are demanding it (with 73% expressing a preference for biometrics over passports). However, many countries must surmount the challenge of ensuring high-quality, verified databases of travellers before this technology can be responsibly rolled out at scale, beyond limited “trusted traveller” initiatives or citizen-only deployments.

St Kitts and Nevis, which introduced a similar solution in 2025, proves that secure biometric entry for all arrivals—from first-time visitors, foreign nationals, and citizens—is possible. St Kitts and Nevis has reduced immigration processing times to just 3 seconds per passenger at Robert L. Bradshaw International Airport.

Crucially, security is automatically factored in. Low-risk travellers—those who have submitted biometric data and biographical information via a mobile app in advance— enjoy the seamless travel experience of a biometric corridor. Those who present anomalies or appear on watchlists are instantly flagged via colour-coded risk systems for secondary, manual inspection. This allows border agencies to focus 90% of their resources on the 1% of travellers who actually pose a risk.

These live, national-scale deployments prove that a contactless, paperless arrival is no longer a theory.

Addressing the Industry's Challenges: Trust and Ethics

Barriers to the wide-scale adoption of these technologies remain: limited resources and technical expertise, public trust, and privacy.

- **Human Review:** While AI can flag anomalies and automate routine checks, the final authority to permit or deny entry must always rest with a human border officer. AI should empower officers, not replace their judgment.
- **Data Sovereignty:** Governments must maintain 100% ownership and control over traveller data, ensuring no data is sold or shared with third parties and sensitive passenger data is protected.
- **International Standards:** Organisations such as the *Biometrics Institute* and the *ICAO* must ensure that governments are adequately supported through this transition by convening industry experts and creating standards that keep pace with the technology as it develops.

Conclusion

The future of *Seamless Travel* is undoubtedly rooted in *Trusted Travel.* By implementing robust pre-travel screening systems, governments can verify traveller identities before they reach the border and ultimately make the physical passport a secondary backup to the traveller's own face. For BorderTech providers, like Travizory, and Governments alike, the question is no longer *if* seamless travel is possible, but rather how quickly nations can integrate the systems required to make it a universal reality.

Organisation: Travizory Border Security
Name: Ygor Lutz, Chief Revenue Officer & Founder
Telephone number: +248 251 0568
Contact details: partnerships@travizory.com

30. Trust Stamp: Biometric Security Modules: Enabling Proof of Humanness

Many security systems today rely on Hardware Security Modules (HSM) to securely manage cryptographic keys and perform sensitive operations. Digital identities, confidential communications, financial transactions, crypto transactions (including stablecoins), and modern passwordless solutions (e.g., FIDO-based passkeys) all depend on the robust security guarantees provided by HSMs.

Although HSMs offer strong protection against key extraction and tampering, they are not without limitations. When a device containing an HSM is lost, stolen, or simply broken, the user loses access to their credentials and data. Moreover, HSMs do not provide proof of humanness, since anyone who can control the HSM can act on behalf of the owner of the private key. In this context, proof of humanness means cryptographically verifying that a real, live human (not malware, automation, or credential replay) is present at the time of authentication. A **Biometric Security Module** (BSM)[#] addresses these shortcomings.

What is a Biometric Security Module (BSM)?

A Biometric Security Module extends the trust guarantees of hardware security into the human domain, binding cryptographic control not just to devices, but to verified human presence. It is a system that uses biometric data (such as fingerprints, facial recognition, or iris scans) to protect the cryptographic secrets in the same way as an HSM does.

In a BSM, cryptographic keys are recreated from biometric data each time authentication is required. Unlike traditional systems that store keys persistently, BSMs do not retain keys after a session ends; the key exists in an ephemeral state during the authentication process. Instead, only non-sensitive helper data is stored on persistent storage to facilitate key reconstruction. Importantly, this helper data alone cannot be used to recover the key without the genuine biometric sample, ensuring that security is maintained even if the helper data is exposed. In short, whereas traditional security focuses on the "what you have" (the device), while BSM focuses on the "who you are" (the human).

Components of a Biometric Security Module

A BSM has the following key components: 1) a biometric sensor to capture the user's biometric data, hardened against injection attacks; 2) a presentation attack detection (PAD) module to detect spoofed biometric samples (e.g., printed images or replayed videos or 3D face mask of the target user); 3) an injection attack detection (IAD) to detect deepfake or synthetically generated biometric images; 4) a feature extractor to process the biometric data and extract relevant features; 5) a fuzzy extractor to derive cryptographic keys from the biometric features; 6) secure storage to store any helper data for additional security; and 7) an interface for cryptographic operations, such as encryption, decryption, and digital signatures, leveraged on an existing HSM on device.

Security features of BSM

The following features make BSM secure: 1) a proprietary fuzzy extractor known as "stable IT2" that can directly extract 256 bits from a face capture session; 2) a face capture solution that can detect presentation attacks and is designed to resist injection attacks; 3) use of AES256 cryptography to ensure the solution is post-quantum ready; 4) no persistent storage of cryptographic secrets: Unlike conventional HSMs, the cryptographic keys that are bound to the user are reconstructed only during authentication; 5) helper data stored is non-sensitive and cannot be used to recover keys without the genuine biometric sample; 6) protection against device loss or theft, as access requires the user's biometric sample; and 7) proof of humanness, preventing unauthorised access even if the device is compromised.

BSM deployment architecture

In a networked environment, the BSM can run both on the server and a client device, which is typically a smartphone for our purpose. The client device functions as a full Biometric Security Module (BSM), capable of biometric capture,

[#] The Biometric Secure Module (BSM) Project was financed by Xjenza Malta, through the FUSION: R&I Technology Development Programme Lite

feature extraction, fuzzy extraction, and cryptographic operations. However, a server is necessary because a core assumption is that the client device, typically a smartphone, can be lost. The server's primary role is to store or back up registration artifacts. It can also perform all operations, including processing biometric data, should the client device lack sufficient capabilities. Since the server cannot capture biometric data directly from the user, it must rely on the client device to provide biometric samples.

What does a successful user authentication prove?

Combing a BSM with Schnorr Non-interactive Zero-Knowledge (NIZK) Proof, a successful verification proves four aspects: 1) **proof of humanness** – only the live-captured biometric sample of the user; 2) **proof of knowledge** of the private key; 3) **proof of intent** – they are intentionally performing the action, e.g., login, transfer 1 ETC; and 4) **proof of freshness**, e.g., the transaction is valid within 5 minutes.

Applications of BSM

- **Online account recovery**: A cloud BSM allows service providers to perform biometric authentication remotely over the Internet when the user's device is lost. It can be combined with multifactor authentication, thus guarding against Sim swap attacks since the registered user must be present.
- **Social account recovery**: If the primary user cannot provide their biometrics, BSM can also be used by an authorised guardian vouching for the identity of the primary user.
- **Cloud BSM supporting digital identity at scale**: A software-based microservice BSM can emulate a population-scale cloud HSM for citizens, providing a cost-effective alternative to the currently impractical and expensive deployment of cloud-based HSMs at scale.
- **Self-custodial password manager** on device or hosted on cloud storage. The storage contains only encrypted passwords that can only be accessed with proof of humanness. In the form of SDK, BSM can be installed on multiple smartphones of different brands, allowing them to synchronise passwords or passkeys between Android and iOS devices, or even laptops, via the intermediary of a data vault storing only encrypted data.
- **Crypto and digital wallets**: BSM can be used to biometrically bind the private keys associated with crypto wallets and digital wallets to the user, creating a solution that is resistant to phishing and friendly fraud.

Summary

Feature	Hardware Security Module (HSM)	Biometric Security Module (BSM)
Primary Trust Root	The physical hardware/chip.	The verified human biometric presence.
Key Persistence	Keys are stored permanently in the chip.	Keys are **ephemeral**; reconstructed and then deleted.
Loss of Device	Leads to total loss of credentials.	User can recover identity via "Cloud BSM."
Identity Proof	Proves the device is present.	Proves a **live human** is present.
Deepfake Defence	Vulnerable to credential replay/malware.	Built-in detection for synthetic/ injected media.

BSM represents a significant enhancement to HSM in the era of deepfakes, designed to perform the "last mile" of authentication – the human themselves, without mandating them to carry a device with HSM which can be lost, stolen, or broken. It can verify a returning customer by generating a Schnorr proof, which confirms four key aspects without revealing biometric data: proof of humanness, proof of knowledge, proof of intent; and proof of freshness; yet is designed to be tamper proof against presentation and injection attacks.

Joined in 2017

Organisation: Trust Stamp
Name: Norman Poh, Chief Science Officer
Telephone number: +44 739 673 1314
Contact details: npoh@truststamp.net

31. Veridas: Real Identity in the Age of AI: Proving a Real Human on a Real Device

Ten years ago, when we started building identity technology, our ambition was not to become just another vendor in a fast-growing market. We set out to build something more fundamental: trust. Our mission was simple but demanding: **distinguish real from fake, in any channel, using technology designed with privacy at its core**.

Today, trust is under direct attack. Cybercrime is expected to cost the global economy **$9.5 trillion annually**, and identity has become its primary attack surface. Around **41% of cyberattacks now involve some form of AI**.

We are living through what can reasonably be described as an **AI fraud pandemic**. In seconds, anyone can fabricate a face, a voice, or a document that can bypass traditional controls. Most cyberattacks no longer begin with malware; they pivot through compromised identity. At the same time, autonomous AI agents are emerging that can operate at machine speed, without human oversight and, crucially, without identity. Fraud is no longer episodic or manual. It is automated, scalable, and persistent.

The question facing the biometric ecosystem is no longer whether AI is "outsmarting" us. It is whether our assumptions about identity are still fit for purpose.

AI has changed the rules, not the objective

Fraud has always evolved. What generative AI has changed is the economics of deception. Attacks that once required time, expertise, and risk can now be launched cheaply, anonymously, and at scale. This has created a structural imbalance: static, point-in-time controls are expected to defend against adaptive, continuously learning adversaries.

The problem is not intelligence; **it is speed and scale**. Fraud now moves faster than most organisations can detect, investigate, or respond. It targets customers, employees, suppliers, and internal workflows alike. In this environment, renting fragmented defenses or stacking disconnected tools offers diminishing returns. Against an enemy that mutates daily, dependency becomes fragility.

Deepfakes are not the real threat, identity uncertainty is

Deepfakes dominate headlines, but they are only the most visible symptom of a deeper issue: **identity uncertainty.** If a system can be convincingly deceived by something that merely looks real, then the system was never verifying reality in the first place. **Between 1% and 6% of identity verification attempts are already fraudulent**, with a growing share linked to injection attacks that bypass traditional controls entirely.

Seeing is no longer believing. Verifying a face is not the same as verifying a real human being. In a world where synthetic media is increasingly indistinguishable from reality, biometric systems must move beyond appearance toward proof of presence, integrity, and continuity.

This distinction matters. The future of trust does not depend on spotting ever-better fakes alone; it depends on proving that an interaction involves a real person acting in real time through a trusted channel with uncompromised data.

Where reality breaks: from presentation to injection

Historically, biometric fraud focused on **presentation attacks**—photos, videos, masks, or replays shown to a camera. While these threats persist, the more dangerous evolution is happening out of sight.

Injection attacks bypass sensors entirely by inserting pre-recorded or synthetically generated data directly into the digital stream between the device and the server. **1.4% of verification processes** at one major client showed signs of possible injection activity. In these scenarios, even the most sophisticated liveness check is rendered irrelevant. Trust collapses not at the camera, but in the pipeline.

This shift exposes a hard truth: **trusting the device is no longer enough.** Systems designed to control access to personal electronics are not designed to establish or defend legal, financial, or civic identity. When organisations inherit identity signals from opaque, consumer-grade environments, they also inherit their vulnerabilities.

What "keeping it real" actually requires

Keeping it real is not a single control or certification. It is an architectural discipline built on a few non-negotiable principles:

- Proof of a real human, not just a biometric match.
- Proof of real-time interaction, not replayed or injected data.
- Proof of channel and device integrity across the transaction.
- Proof of identity continuity across the lifecycle, not just onboarding.

This requires **layered defenses that work together**: active and passive detection, data-stream protection, systemic intelligence, and continuous risk assessment. Just as importantly, these systems must be explainable, auditable, and proportionate. Ethics and transparency are not constraints on security; they are prerequisites for public trust.

Layered systems give us an opportunity to fight back and be better prepared against new, unknown threats.

This evolution is also reflected in modern biometric standards. ISO-aligned approaches, such as renewable biometric references (RBRs), replace static templates with purpose-specific, non-reusable representations that can be revoked and reissued if needed. By design, they reduce privacy risk, prevent cross-context tracking, and bring biometric security into alignment with legal principles like data minimisation and proportionality. At the same time, newer standards are introducing formal certification frameworks to address emerging fraud vectors **such as injection attacks,** recognising the need for solutions that ensure the integrity of the device and the channel in order to protect biometric systems against advanced threats.

Presumed identity versus real identity

Our discussion highlights that much of today's digital trust **relies on presumed identity.** Signals derived from devices rather than an established, accountable identity. On-device biometrics were designed to protect phones, not to verify people. Their enrolment is unverified, their identities diluted, and their safeguards easily bypassed by shared or stolen passcodes.

Real identity is different. It is established, not assumed. It is anchored to authoritative sources, defended holistically, and monitored systemically. Most importantly, it is owned and governed by the organisations that depend on it.

Conclusion: the future of fraud is not inevitable

The AI fraud pandemic will continue to evolve. So must biometrics. The future is not a contest between humans and machines, nor between AI and privacy. It is a choice about how seriously we take reality as a system requirement. **Biometrics, when designed responsibly, remain one of the strongest tools we have to prove who is real**—without friction, without surveillance, and without sacrificing trust.

Joined in 2019

Organisation: Veridas
Name: Iván Gulina, Head of Antifraud
Telephone number: +34 677 662 408
Contact details: Juan Fernando Campos, Global PR Manager, jfcampos@veridas.com

32. ZwillGen PLLC: All People May Be Created Equal; All Biometrics Are Not

Legislative frameworks are struggling to keep pace with the changing world of “biometrics.” Leaving for another time the problematic creep of definitions to include characterisation and emotion analysis, one of the changes we need to make in current discourse is to recognise the profound ethical and socio-political differences in unlocking a smartphone versus being identified at a protest rally.

With the growing use of biometric technology in more daily applications, we can no longer afford to treat everything based on a similar scan as having the same impacts and harms in the real world. We should start by consistently separating "verification" (one-to-one matching) from "identification" (one-to-many matching) for purposes of most discussion, and especially for legislative protections.

Too many people, policymakers included, have relied on historically consolidated descriptions of “facial recognition,” which led to assumptions that biometric systems are uniformly accurate (or uniformly flawed). Going forward, we must recognise that the same algorithm can have wildly different outputs and consequences depending on how it’s used.

Verification (1:1) asks: "Is this person who they claim to be?" A user presents an input, and the system compares the sample against one pre-registered template. It is a yes/no question. If the match fails, the door doesn't open; the phone doesn't unlock.

Identification (1:N) asks: "Who is this person?" Here, the system generates a biometric record from an unknown individual, often without their awareness, and compares it to a database of N (potentially billions) to find a match. This is an inquisition, not a lock.

The U.S. National Institute of Standards and Technology (NIST) operates on this distinction, with separate performance testing for verification and identification. However, the public and policymakers often miss this nuance. Claims citing NIST results are often applying the results of 1:1 verification (cooperative subjects in good lighting) to use cases involving 1:N identification (uncontrolled environments, grainy video, bad angles).

Many laws also overlook this distinction. Illinois’ Biometric Information Privacy Act (BIPA), one of the most influential biometric laws, defines biometric identifiers without regard to whether they access an account or power a surveillance network. Others follow this pattern. This is problematic because the use cases for biometric identifiers are growing, but the risks have vastly different stakes.

In a verification system, the primary failure mode is a *False Rejection* (the system fails to recognise you). The result is frustration, annoyance, friction. But it is most often an inconvenience, not a civil liberties violation. The corollary *False Acceptance* (letting in the wrong person) is a security risk, but still usually in a bounded environment (one building, one account).

In an identification system, the concerning failure is a False Match, where the system incorrectly identifies someone unknown. The context here is societal, not transactional: who gets stopped, who is investigated, who is tracked. In a database of billions of people, even a "low" false positive rate can generate thousands of false leads. Because of the quality issues for these collected images, error rates are usually higher, yet when public agencies and law enforcement rely on these systems, a technical error can lead to wrongful arrest or other trauma. Also of note, those errors are usually not distributed equally across demographic sub-groups.

A key difference lies in the user's relationship to the technology. Biometric verification is almost exclusively an active, consent-based process. You *choose* to look at your phone or to step up to an airport gate. You are a participant.

Furthermore, verification allows for privacy-preserving architectures. The template can be stored on your device or other local option. There's no need for a massive database of faces; just a "yes/no" signal from your token.

Identification, conversely, is most often passive and frequently non-consensual. It is the tool of surveillance, with cameras scanning a public square or a commercial venue. You cannot opt-out of your face being visible. This creates a "chilling effect" on free speech and association; people act differently when they know they can be identified and tracked. The harm is the surveillance itself: not biometrics per se, but their use for pervasive identification. And this application requires massive databases to function.

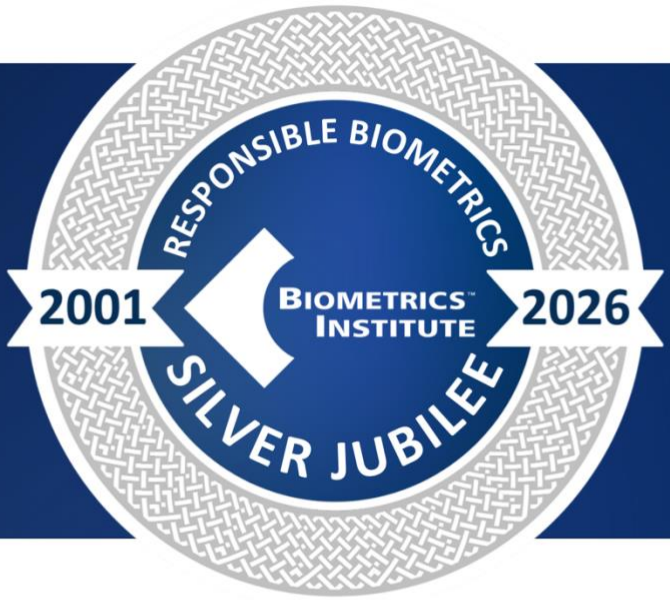
The EU's AI Act acknowledges this distinction by prohibiting real-time remote biometric identification in public spaces and generally prohibiting law enforcement use of such systems, with only tightly defined exceptions. Other forms of remote biometric identification are not outright banned but still classified as high-risk, subject to stringent requirements. This is a values-based approach, recognizing that the same underlying tech may be acceptable in a controlled, consensual context but incompatible with free societies when repurposed at scale.

However, other legislative attempts remain based on the *data type* ("scan of face geometry") rather than the *use case*. This risks the over-regulation of useful access control tools, and the under-regulation of surveillance. We need laws that specifically target the architecture of surveillance such as limiting the size of databases, the retention periods of 1:N query logs, and delineating the specific ways in which identification may be used.

None of this means that identification is never justified or that verification should be given a free pass. An employee asked to "consent" to a biometric time clock, or a traveler offered biometric border control may not have meaningful alternatives. But that is still a very different situation from being identified at a protest by a camera you never even noticed, and protections can be developed and applied with greater individual effect within employment laws, border control, or other regulatory contexts.

Treating "biometrics" as a technical capability that implicates a uniform set of harms, and should be restricted similarly across contexts, will not serve us well in any situation. We should at least accurately categorise identification versus verification, along with a tiered low-medium-high use case approach. This will allow us a way to protect free societies while retaining personal convenience and high-quality security. Moving forward, we should change the way we think and talk about these systems.

Organisation: ZwillGen PLLC
Name: Brenda K. Leong, Director, AI Division
Telephone number: +1 703 587 8429
Contact details: Brenda.leong@zwillgen.com, 1900 M St NW, Suite 250, Washington DC 20036



amadeus · Attain Insight · AURAYA · AWARE · Biometix · BixeLab

iDstation · Cognitec · ENTRUST · facephi · facetec · FACIA

fime · FUJITSU · HID · IDEMIA PUBLIC SECURITY · INNOVATRICS · iProov

jumio · PARAVISION · Regula · SAIC · Signicat · SITA

SPEED IDENTITY · THALES · travizory · TrustStamp · VeriDas · ZwillGen

RESPONSIBLE BIOMETRICS

2001 BIOMETRICS INSTITUTE 2026

SILVER JUBILEE

A global community promoting the **responsible**, **ethical** and **effective** use of biometrics since 2001

biometricsinstitute.org