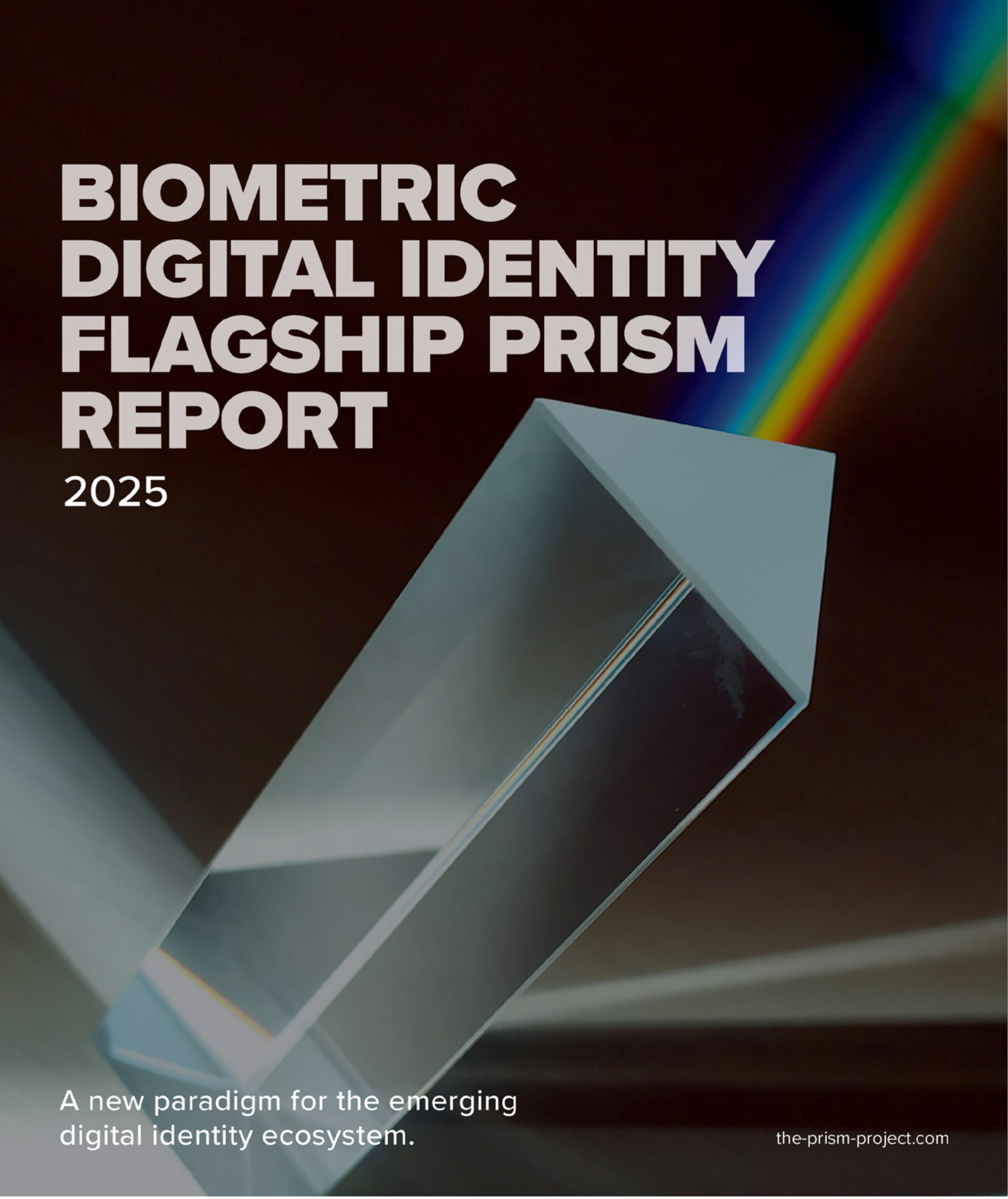
BIOMETRIC DIGITAL IDENTITY FLAGSHIP PRISM REPORT

2025



A new paradigm for the emerging digital identity ecosystem.

the-prism-project.com

THE PRISM PROJECT

ACUITY MARKET INTELLIGENCE

Preface

Welcome to the 2025 Biometric Digital Identity Flagship Prism Report. This is the latest report from The Prism Project—a research, analysis, and market education initiative created by Acuity Market Intelligence to bridge the gap between the identity technology intelligentsia and the private-and-public-sector enterprise professionals evaluating and deploying digital identity solutions to meet the challenges of digital transformation.

Utilizing a holistic framework informed by hundreds of organizations and relying party evaluations, The Prism Project is grounded in a philosophy of digital identity, based on four key pillars:

- Digital identity belongs to the person it describes.
- True identity empowerment relies on government systems of record.
- Identity must be consistently and continuously orchestrated in both physical and online channels to remain secure.
- Biometrics must be at the core of any sustainable, reliable, and secure digital ecosystem, and be implemented with the understanding that identity flows freely between converging virtual and physical worlds.

This report takes a broad view of biometric digital identity. Through its 2024 analysis of biometric digital identity in financial services, government services, and travel and hospitality, as well as its 2025 deep dive analyses of deepfake and synthetic identity threats and privacy and compliance vulnerabilities, The Prism Project identified two core concepts driving identity in a rapidly digitizing world. These are:

- **Trust:** assurance of end-user sovereignty that preserves individual privacy and protects identity elements and ensures their human integrity.
- **Resilience:** fortitude against the AI-powered fraud that poses an existential threat to all concepts of human identity, namely, deepfakes, synthetic identities, and agentic AI.

As relying parties across all market sectors achieve new levels of digitization, identity elements describing the humans interacting with various online entities—including biometrics, Personally Identifiable Information (PII), and contextual data—are at risk of exposure to malicious actors. Once exposed, these identity elements can be used to commit identity theft, mint synthetic identities, perpetrate fraud, and gain unauthorized access to restricted spaces online and in the physical world.

The first Prism report of 2025—the Deepfake and Synthetic Identity Prism Report—identified and categorized the most advanced forms of identity fraud threats powered by AI. The report diagrammed the anatomy of a single digital identity in relation to the processes it undergoes for verification, authentication, and account recovery—categorizing each identity element and placing it within the broader context of the various transactions it enables and the data required at each step along the way. The second report—the Privacy and Compliance Prism Report—leveraged those diagrams, focusing on the identity elements themselves, what can be done to protect them at each step in the process, and how they can be safely managed throughout the entire identity lifecycle. **Here, in the Flagship Report, we bind these ideas together to demonstrate the crucial importance of trust and resilience in the digital identity ecosystem that underpins human transactions.**

The larger mission of The Prism Project is to empower public and private sector influencers and decision-makers by providing the information and analysis they need to understand and effectively evaluate and deploy digital identity technology and solutions. With the 2025 Biometric Digital Identity Flagship Prism Report, we further this mission by presenting a vision of the biometric digital identity ecosystem that enshrines trust and is ready to defend against the most advanced AI-powered fraud threats; a vision that can facilitate constructive engagement among all parties about how identity data should be used in all identity transactions, from opening a bank account to entering a physical data center. **The ultimate goal is to foster a convenient and secure culture of trust built on a shared understanding of inclusive human identity in the digital age.**

In this report, you will find:

- A beginner's crash course in biometric digital identity that:
    - Introduces key concepts and definitions
    - Provides a synopsis of recent critical market dynamics and regulatory evolutions
    - Equips you with the foundation for understanding how trust and resilience factor into the identity ecosystem
- An inventory of identity elements commonly used in digital identity transactions, defined and described in plain language and accessible diagrams, and categorized according to how they impact user privacy and play into the rapidly evolving AI-powered fraud landscape.
- A worldwide trend map, highlighting key biometric digital identity trends around the globe.

Download the 2024 Prism Reports:

- A breakdown of common challenges and vulnerabilities that relying parties face when handling identity data, examined through the proprietary Prism Lens model and across representative markets.
- A guide to technologies and technology-based approaches and solutions that, when deployed appropriately, address the challenges and thwart the vulnerabilities that undermine the resilience of and trust in the biometric digital identity ecosystem.
- The new Prism Resilient Trust Maturity Ladder—a new tool that helps vendors and relying parties align their organizations and products and services with the Prism concepts of resilience and trust.
- The latest Flagship version of the proprietary Biometric Digital Identity Prism market landscape model.
- Evaluations of vendors, relying parties, and infrastructure organizations contributing to the collective effort to enshrine trust and improve resilience.
- Profiles of significant players that prioritize user privacy and anti-fraud innovation.

While it does build on the foundational market knowledge set out in previous Prism Reports, the 2025 Biometric Digital Identity Flagship Prism Report can stand on its own as an independent resource. For further reading and context on the core philosophy that underpins this publication, we recommend supplementing it with our 2024 Flagship Report, the 2025 Deepfake and Synthetic Identity Prism Report, and the 2025 Privacy and Compliance Prism Report, available to download after a brief registration at www.the-prism-project.com/reports.

The Prism Project will publish two Full-Spectrum reports in 2026: a deep dive into the financial services industry and the 2026 Flagship Prism Report, next year's holistic look at the evolving biometric-centric digital identity ecosystem. Those will be complemented by several new Focal Point reports: shorter, sharper reports that laser-focus on flashpoint issues in identity, like airport travel journeys, decentralized identity, and Agentic AI.

As ever, my collaborators and I are evangelists of strong identity and believe that the only way to move forward in our time of digital transformation is to take the ethics of human identity seriously in both the physical and digital realms. As a communi-

Download the 2025 Prism Reports:

ty, the identity industry and its stakeholders are morally obligated to develop and implement powerful digital technologies for the good of humanity. By reading and sharing our vision of a secure, convenient, user-powered identity that ensures trust and resilience, you are helping drive the positive change required to close identity gaps. Together, we can usher in an identity-safe future for all.

Authentically yours,

Maxine Most
Founder
The Prism Project

Thank You to Our Sponsors and Partners

The 2025 Flagship Prism Report is made possible thanks to the participation of our sponsors and partners. The biometric digital identity ecosystem depends on collaboration, and we are grateful to work with the following organizations.

SPONSORS

PARTNERS

The Prism is proudly independent. While participants benefit from increased visibility and vendor profiles in this report, sponsorship does not affect a vendor's evaluation of placement within any aspect of the Prism Project.

Table of Contents

Table of Contents (cont'd)

Introduction

Welcome to the Era of Resilient Trust

As digital identity matures into becoming the essential backbone of global commerce, governance, and daily life, it faces unprecedented challenges. Two forces define this moment: the rise of AI-powered synthetic identity and deepfake fraud, and the escalating urgency of privacy and compliance mandates. Together, these forces create a paradoxical environment, a year of trust under threat, when identity has never been more central to digital transformation, yet never more vulnerable to exploitation and misuse.

The 2025 Flagship Prism Report introduces a dual framework of resilience and trust, built around core principles designed to withstand both current and emerging threats to the identity ecosystem. It frames the current digital identity state of play as a critical turning point, when organizations can no longer simply go through the motions of adoption via pilots, tests, and endless iterations of limited edge deployments. They must move beyond identity silos, archaic Identity and Access Management (IAM) systems—both logical and physical—and minimal regulatory compliance to embrace truly resilient, privacy-first identity ecosystems embedded in the heart of their digital infrastructure.

The Prism Project was founded on a simple but powerful belief: digital identity must be human-centered. It must serve the people it represents, remain anchored in trusted systems of record, flow seamlessly across physical and digital worlds, and be secured with biometrics at its core. The original Prism frameworks of 2023–2024 mapped the biometric digital identity ecosystem through vertical adoption lenses—financial services, travel & hospitality, and government services. These sector-specific maps highlighted market growth, vendor ecosystems, and emerging business cases. Each of these reports revealed both the opportunities and the vulnerabilities that arise as organizations digitize their customer and citizen interactions. Collectively, they showed that while biometrics enable faster, safer, and more inclusive experiences, the underlying identity elements—biometrics, credentials, and contextual personal data—remain fragile and exposed.

As we entered 2025, two forces emerged as defining challenges for the entire digital identity ecosystem:

- **Deepfakes & Synthetic Identity.** Powered by generative AI, synthetic identities and deepfake techniques are destabilizing the very notion of trust in digital transactions. No vertical is immune—from banking and healthcare to telecom, education, and entertainment venues.
- **Privacy & Compliance.** At the same time, escalating regulatory mandates and public expectations are redefining how identity data must be collected, stored, and used. Compliance is no longer a defensive obligation—it is becoming a strategic differentiator.

Synthetic identity and privacy imperatives demanded a different approach. Fraud vectors and compliance pressures cut across every vertical, exposing systemic vulnerabilities and opportunities for transformation. These challenges demand a shift from sector-specific analysis to an issues-first perspective. Where the 2024 reports asked, "How are verticals adopting biometrics?" the 2025 Flagship Prism Report asks, "How can digital identity ecosystems remain trusted and resilient in the face of synthetic fraud and privacy imperatives?"

The 2025 Flagship Prism Report necessarily reframes the ecosystem not by market verticals, but by the dimensions of resilience and trust required to withstand threats and deliver empowerment. The report weaves together insights from both vertical adoption and cross-cutting risks to provide a holistic view of the state of digital identity at the close of 2025.

Identity Under Siege

The same Generative AI advances in artificial intelligence that are transforming creativity, productivity, and human-computer interaction have fueled an unprecedented wave of synthetic identity fraud and deepfake-enabled attacks.

This is not a niche or emerging problem; synthetic fraud represents the defining threat of the AI era. Synthetic identities and deepfakes have weaponized the very elements that once secured trust. Attack vectors now span every stage of the identity lifecycle, from enrollment and authentication to recovery. Vertical markets as diverse as banking, healthcare, education, telecom, and sports & entertainment are facing fraud scenarios that undermine both operational integrity and customer confidence.

As fraudsters industrialize these capabilities, fraud defense requires multi-layered resilience: advanced liveness detection,

multimodal biometrics, forensic AI, and orchestrated defenses across the identity lifecycle. The vendors and relying parties that survive will be those that treat resilience not as a feature, but as a core design principle of their identity ecosystems.

Privacy and Compliance: From Obligation to Differentiation

At the same time, global privacy regulation is evolving from a patchwork of obligations into a de facto competitive battleground. Leaders are moving past checkbox compliance to treat privacy as a core component of digital trust—an asset that differentiates them in markets where customer empowerment and consent are now decisive factors.

Over the last decade, digital identity has outpaced the regulations governing it. From the introduction of consumer biometrics in 2013 to the explosive adoption of remote onboarding during the pandemic, to the latest game-changer—agentic AI—organizations have leveraged biometric and identity technologies faster than policymakers could react. The result is a world in which identity data is both indispensable and insecure.

As biometric and other identity data proliferate across sectors, privacy expectations are increasingly set by users, not regulators. People demand to know how their identity data is captured, stored, and shared. In 2025, privacy is no longer a legal checklist or a defensive necessity. Privacy has evolved beyond a mere compliance requirement, from an obligation into a strategic differentiator—a way for organizations to earn, retain, and monetize customer trust while protecting the most valuable asset in the digital economy: identity data. Organizations that fail to deliver lose not only regulatory standing and potentially significant monetary and digital assets, but also brand equity.

The Convergence Imperative: Resilient Trust

In earlier stages of digital identity adoption, organizations often treated fraud prevention, privacy, and regulatory compliance as distinct—even competing—priorities. Fraud controls were layered on top of compliance programs, and privacy was treated as a checklist of legal requirements.

Today, this siloed approach is no longer viable. Fraud defense, privacy, and compliance can no longer be pursued in isolation, as doing so exposes digital infrastructure to systemic vulnerabilities. These two forces must be addressed simultaneously in an orchestrated identity-first strategy that recognizes that, rather than being

in conflict, these two critical digital identity ecosystem imperatives not only intersect and reference each other, but also build and reinforce each other. **This is the Prism Project's concept of Resilient Trust.**

The Prismatic Future: A Trust-Centered Ecosystem

Within the 2025 Prism Framework, convergence is no longer an abstract goal but an operational necessity that calls for a dual mandate: protect human identity from the accelerating threats of AI misuse and systemic privacy erosion, while empowering individuals with secure, ethical, and user-first digital ecosystems.

- Technology and Solution Vendors must design interoperable systems that integrate fraud defense and privacy controls seamlessly into identity workflows.
- Relying Parties must treat fraud and compliance as a unified Resident Trust investment, not two independent competing budget lines.
- Regulators and Supporting Organizations must align incentives so that vendors and relying parties are rewarded for embedding trust and resilience in digital identity ecosystems, rather than penalized for innovation.

The 2025 Flagship Prism Report is therefore both a warning and a blueprint: a warning that identity is under siege and a blueprint for how resilience, privacy, and user empowerment can converge into a trust-centered identity future.

How to Read This Prism Report

The 2025 Flagship Prism Report is divided into eight sections:

Crash Course

The report opens with a crash course on the identity arms race designed to bring you up to speed on the past decade and a half of innovation and evolution in biometric digital identity, with a focus on how we arrived at the current inflection point of trust and resilience as physical and digital worlds converge. Key terms and concepts are defined in the sidebar, and live links are included as needed to provide **the context and content for the rest of the report.**

Resilient Trust Foundational Primer

Using plain language and supported by intuitive diagrams, the second major section of this report classifies and categorizes the various identity elements collected and processed in digital transactions of all kinds. It is divided into subsections that each define a critical facet of Resilient Trust—the core concept of this report.

- **Biometric Digital Identity Trend World Map:** A map providing a global view of the major biometric digital identity trends as related to privacy and fraud protection.
- **Resilient Trust in the Biometric Digital Identity Ecosystem:** Plain language definitions of privacy, compliance, deepfakes, and synthetic identities, presented in relation to each other and supported with infographics.
- **The Identity Hierarchy:** The Prism Project's proprietary model illustrating the various tiers of biometric digital identity, applied to the Resilient Trust concept.
- **Threats and Vulnerabilities:** A visual breakdown of the identity verification and authentication process, presented with plain language definitions, highlighting threats and vulnerabilities related to Resilient Trust.
- **Countermeasures:** A list of solutions that can be deployed to address the threats and vulnerabilities undermining Resilient Trust in the biometric digital identity ecosystem.

The Resilient Trust Foundational Primer provides the core ideas and lexicon for understanding trust and resilience in biometric digital identity.

The Prism Lens (Challenges and Solutions)

The third section of this report defines the Prism Lens—a proprietary model that identifies the key strategic public and private-sector enterprise C-suite challenges (e.g., pain points) executives face in the age of digital transformation. It then discusses how biometric-centric digital identity technology and solutions can be applied to address them. **The critical pain points highlighted in the Prism Lens serve as the basis for the practical applications of biometric digital identity highlighted in the report profiles.**

Vertical Market Breakdown

To illustrate the broad real-world scope of biometric-centric digital identity opportunities, the fourth section of this report applies the challenges identified in the Prism Lens to representative vertical market sectors. **The Vertical Market Breakdown lays the groundwork for the tools and evaluations in the rest of the report.**

The Resilient Trust Maturity Ladder

New for the 2025 Flagship Prism Report, the fifth section introduces a proprietary tool for mapping organizational alignment with the Prism concept of Resilient Trust. The Resilient Trust Maturity Ladder can be used by vendors for self-assessment and by relying parties that are evaluating vendor capabilities. **The Resilient Trust Maturity Ladder harmonizes the concepts laid out throughout the report into a framework for understanding how organizations can direct their operations and philosophy to support an identity-safe future.**

The Prism

The sixth section is the proprietary biometric digital identity industry ecosystem framework: the Prism. The Prism ecosystem positions market leaders in the center, surrounded by the full range of marketplace contributors, arranged by "Prism Beams," that define their primary contribution to the biometric digital identity ecosystem. This configuration reflects a market dynamic that depends on cross-beam collaboration between foundational and specialized technology and platform providers, integrators and solution providers, and infrastructure players and relying parties (end-user organizations) to enshrine trust and build resilience across all major use cases. **The Prism is a living research program, providing a framework for understanding how these digital**

identity players work together to fight fraud, improve user experience, and empower people in an era where trust and resilience are required for safe transactions.

Evaluations and Profiles

The seventh section lists the organizations depicted in the Prism framework next to their evaluations. Each organization is evaluated in context—based on their capabilities, accomplishments, market performance, and vision and aspirations—and grouped according to their Prism Beam. After each set of evaluations, profiles are presented to illustrate how the solutions offered and market engagement by sponsors of this report address the Resilient Trust challenges defined in the Prism Lens and Vertical Market Breakdown sections. (While many organizations can and do operate across multiple Prism Beams, for the purpose of creating an ecosystem model, each is assigned a primary position within the Prism framework. Sponsor profiles include visualizations called Luminosity Graphs that illustrate their true multibeam positioning.) **The evaluations and profiles provide insight into how organizations are positioned and operate across the Prism landscape, and how they are solving critical strategic problems with biometric digital identity technology and solutions.**

The Prismatic Future of Identity

The eighth and final section of this report contains strategic guidance and recommendations based on this report's research. It also includes author information, an overview of the Prism Project, and information on how to get involved in future Prism reports. **The conclusion lights your way to the next steps on your digital identity roadmap.**

Each section of this report stands on its own, but taken together, the end-to-end report provides a unique, comprehensive view of how biometric-centric digital identity is enabling secure, trustworthy, human-powered identity in an increasingly digital world.

Crash Course: Trust and Resilience in the Identity Arms Race

Deepfakes and synthetic identities pose an existential threat to every organization that operates through digital channels. At the same time, privacy laws, user expectations, and regulatory frameworks are reshaping how personal data can be collected, stored, and used. Together, these forces define the modern challenge of digital identity trust and resilience, where trust comes from privacy, transparency, and compliance, and resilience comes from strong anti-fraud defenses that can withstand AI-powered attacks.

To understand how we got here—where real people and digital facsimiles can be indistinguishable online, and where every **identity transaction** must navigate both regulation and risk—we must review how **biometrics** entered the mainstream, reshaped **PII**, and ignited an arms race between fraudsters and identity vendors. This crash course is designed to familiarize the uninitiated and refresh the well-informed with key digital identity definitions and concepts, and to contextualize them through a rapid journey through the past decade of digital transformation, privacy evolution, and AI-driven fraud. Buckle up.

The Basic Idea Behind Biometrics, Privacy, and Digital Identity

In digital spaces, we don't have bodies, so our interactions are enabled or limited by the identity elements we can provide to prove we are who we claim to be. The same is true of in-person interactions mediated by digital systems—access control, kiosks, remote onboarding, and more. At a fundamental level, we can present three types of identity elements:

- Something we know – **knowledge-based authentication (KBA)** such as passwords, PINs, security questions, or one-time codes.
- Something we have – **token or device-based authentication (DBA**) such as keys, cards, FOBs, USB tokens, cryptographic keys, or smartphones.
- Something we are – biometrics derived from our faces, fingerprints, voices, irises, or behavior.

Key Definitions:

IDENTITY TRANSACTION: An interaction, either online or in a physical space, that requires specific permissions related to an individual's identity. The scope of these transactions is broad-reaching and includes accessing email, making online purchases, verifying your age in person or online, and accessing secure physical spaces.

BIOMETRICS: Technology that uses some kind of sensor (camera, microphone, fingerprint reader, etc.) to measure or capture an image of a user's unique biological trait—most commonly a face, voice, fingerprint, or iris—and represent it via an algorithm as a **biometric template** for the purposes of identification, authentication, or security.

BIOMETRIC TEMPLATE: An algorithmic representation of a captured biological trait, stored as a mathematical value that cannot be reverse-engineered to recreate the original face, fingerprint, or voice.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Data that describes foundational, biographical, and contextual details about an individual—from date and place of birth, to social security number, to address history, and more. PII linked to biometrics creates the foundation for digital identity.

IDENTITY ELEMENT: A component part of identity. In this report, an identity element refers to a biometric, a document, or metadata. An identity element can be authentic or counterfeit.

KNOWLEDGE-BASED AUTHENTICATION (KBA): A form of identity security based on knowable information. Common examples are passwords, PINs, and SMS codes.

TOKEN OR DEVICE-BASED AUTHENTICATION (DBA): A form of identity security that depends on physical possession. Common examples are keys, key cards, FOBs, USB security keys, cryptographic keys, virtual tokens, and mobile devices like smartphones when used for authentication.

KBA can be guessed, shared, stolen, or forgotten. Tokens can be lost, cloned, or stolen. Biometrics, however, when combined with liveness and deepfake detection, stand apart as a stronger factor: your face, fingerprint, voice, or behavior cannot be meaningfully shared or forgotten, and when properly stored as encrypted templates, cannot be "reverse engineered" into the original image.

This is where trust and resilience begin to converge.

- Biometrics and strong authentication tighten the link between a human and their accounts, enabling resilience against fraud and account takeover.
- Privacy-aware storage, consent, and control over biometric-linked PII build trust, ensuring those powerful identity elements are not misused.

By incorporating biological identity elements into online interactions, digital transactions can approach the level of certainty we expect in the physical world. Opening a bank account, renewing a license, or accessing a restricted facility can all be performed remotely if a relying party can trust that a biometric match ties back to an authenticated, compliant digital identity. In short, biometrics give you a body in digital spaces—and that body must be both protected (resilience) and respected (trust via privacy and compliance).

RELYING PARTY: An organization that drives end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

IDENTITY VERIFICATION (IDV): Technology that compares a user's live-captured face to an image on a trusted credential (e.g. passport, national ID, driver's license) and/or a **system of record**. IDV enables **biometric binding** and compliance with **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)** regulations, especially for remote onboarding.

SYSTEM OF RECORD: A trusted database of foundational identity elements maintained by an authority (e.g. a government registry, a university, or a bank's customer database).

BIOMETRIC BINDING: The act of connecting live-captured biometric data to trusted personal information on a trusted identity credential to verify user identity.

KNOW YOUR CUSTOMER (KYC): A set of global guidelines and regulations for the mandatory process of identifying and verifying the identity of a client when opening an account and throughout the customer lifecycle.

ANTI-MONEY LAUNDERING (AML): A set of global laws requiring that regulated entities implement measures to detect and prevent suspicious financial activities.

KY-ABC: An identity concept coined by AWARE CEO Ajay Amlani used to describe the increasingly broad identity demands in the AI-powered era of digital transformation, when relying parties must Know Your Agent, Business, and Customer.

The Biometrics Lifecycle: Where Trust Meets Resilience

To see how biometrics shape both privacy and fraud risk, it's useful to understand the biometrics lifecycle—the three phases where trust (compliance, user rights) and resilience (fraud defense) must be maintained:

Enrollment

A new user submits their biometrics for the first time, creating a biometric template to be used for future comparisons. Enrollment can be strengthened by adding additional identity elements, such as government ID data, through a process known as **identity verification (IDV).** In some cases, as with the biometrics on demand solutions described later in this report, the template generated at this step is not stored, but used to create a stable authentication key.

- Trust: Requires consent, clear data policies, and compliance with privacy laws (GDPR, BIPA, CCPA, etc.).

- Resilience: Proper IDV and biometric binding prevent bad actors from enrolling as someone else or registering synthetic identities.

Authentication

An enrolled user submits their biometrics to match against a template (either stored or generated on demand). A successful match authenticates the transaction.

- Trust: Relying parties should only use data for agreed-upon purposes, log transactions appropriately, and respect user expectations.
- Resilience: **Liveness** detection, multi-factor options, and anti-deepfake measures defend against presentation attacks and account takeovers.

Account Recovery

A user who has lost access attempts to regain it via recovery codes, call centers, in-person visits, or automated device flows.

- Trust: Recovery flows must respect privacy, minimize data exposure, and comply with identity and data regulations.
- Resilience: Call centers and self-service recovery are now prime targets for deepfakes; they need voice liveness, deepfake detection, and risk scoring.

The Mobile Revolution: "Something You Are" Goes Mainstream

Before 2013, online security relied primarily on KBA, occasionally augmented by tokens. These methods were fragile: if a password or card was compromised, whoever possessed it inherited its privileges. There was little assurance that authentication was bound to the right person.

That changed in 2013 with the introduction of iPhone 5S and Touch ID. For the first time, biometrics became a mass-market consumer security feature—a convenient way to unlock a phone. Samsung, LG, and others followed. Soon, fingerprints were touted as a password replacement, and face and voice biometrics started appearing in apps.

This ushered in:

- A new level of resilience, since biometrics made it much harder for casual attackers to impersonate users.
- A new wave of privacy concerns, because biometric data felt uniquely sensitive and irrevocable, demanding stronger

LIVENESS: The quality of authenticity in a biometric. The term is most commonly used in the context of liveness detection software, which is a support technology designed to detect and prevent **presentation attacks** by verifying a live human being is present at the time the biometric is captured. More recently, liveness has been applied to identity documents as well to ensure they are not digital replicas of authentic or counterfeit documents.

PRESENTATION ATTACK (SPOOFING): Presenting **counterfeit identity elements** (like printed photos, masks, or voice recordings) to a sensor to trigger a false positive and wrongfully authenticate.

COUNTERFIET IDENTITY ELEMENTS: Biometrics, documents, and metadata that have been created or modified—by digital or physical means—by a bad actor for the purposes of deception or fraud. This includes (but is not limited to) deepfakes, fake IDs, and misleading or altered metadata.

protections and compliance frameworks.

At the same time, debates emerged over where biometric data should live—**on device** vs. **on server**—which framed early thinking about trust in biometric architectures

Early Privacy Shockwaves and the End of "Security by Illusion"

As biometrics became increasingly mainstream, broader privacy controversies and breaches shifted public perception of identity data:

- NSA PRISM leaks sparked fear that governments might secretly harvest personal data (including, in the public imagination, biometrics).
- The OPM breach (2015) compromised millions of fingerprint records and extensive PII—demonstrating how catastrophic poor data storage practices can be.
- Massive breaches at Yahoo!, Equifax, Facebook, Capital One, LinkedIn, and others revealed that biographical, contextual, and transactional identity data was being leaked at unprecedented scale.

The result:

- **Trust crisis:** Users and regulators recognized that identity elements are highly valuable and often poorly protected.
- **Resilience imperative:** Traditional credentials (passwords, security questions, static data) were clearly no longer enough to withstand modern attacks.

Strong authentication—especially biometrics—began to be seen not only as a convenience, but as a necessary step toward resilience in a perforated security landscape. But this strength had to be balanced with robust privacy and compliance controls.

The Rise of Spoofs: Fraudsters Enter the Biometric Arena

Early biometric systems were relatively primitive and vulnerable to presentation attacks—attempts to fool sensors with fake fingerprints, printed photos, masks, or recordings. Weak spots included:

- Biometric systems reverting to passwords after failed attempts, undermining resilience.

ON-DEVICE BIOMETRICS: Biometric authentication solutions in which enrolled identity elements are stored and matched in a **secure element** and never leave the smartphone, computer, or smart card they're on.

SERVER-SIDE BIOMETRICS: Biometric authentication and verification solutions in which enrolled identity elements are stored and matched on a centralized server. This requires secure transmission of biometric data between the sensor and the server.

SECURE ELEMENT: A cloistered part of a mobile device or computer system that applications or network features cannot access.

- Lack of biometric binding, allowing anyone to enroll their biometrics on someone else's device.
- Sensors that could be fooled by simple artifacts (photos, gummy fingers, audio replays).

Fraudsters quickly realized that if they could imitate or replay a user's biometric, they could bypass "something you are" the same way they bypassed passwords and tokens.

Countermeasures: Building Resilience Without Breaking Trust

In response to these attacks, vendors introduced countermeasures aimed at improving liveness and blocking counterfeit identity elements:

- Sensor fidelity: Higher-resolution and multi-spectral fingerprint sensors, infrared and 3D face capture, and better microphones improved resistance to cheap spoofs.
- Active challenges: Systems asked users to blink, move their face, or repeat random phrases to confirm liveness.
- Multi-factor and multi-modal approaches: Combining biometrics with passwords or tokens, or pairing two biometrics (e.g., face + voice) to increase the cost and complexity for attackers.

These steps dramatically increased resilience against fraud—but they also risked adding friction and complexity. To maintain trust, vendors needed to:

- Not only be transparent about what they collected and why, and...
- Comply with emerging privacy regulations, but also...
- Design user experiences that didn't feel overly intrusive or confusing.

Digital Transformation, Biometric Binding, and Document Risk

As **digital transformation** accelerated—especially around 2020 during pandemic lockdowns—organizations sought to:

- Onboard users remotely,
- Verify identities for higher-risk transactions, and
- Comply with KYC/AML and other regulatory requirements.

This led to widespread adoption of facial recognition plus document capture solutions, combining:

- Live face biometrics,
- **Optical Character Recognition (OCR)** to read credentials

DIGITAL TRANSFORMATION: The organizational process of integrating digital technologies and procedures into daily operations to increase efficiency, enhance accessibility, and boost customer experience.

OPTICAL CHARACTER RECOGNITION (OCR): Computer vision technology that reads text from images, like scanning an ID card via a smartphone camera.

COMPUTER VISION: AI that enables machines to interpret,understand, and identify visual information from images and video.

and

- **Computer vision** to analyze document authenticity and veracity.

This solved the biometric binding problem and improved trust (stronger linkage between identity records and a real person), while enhancing resilience (harder to impersonate someone else without both a face and a valid ID).

But it also created new risks:

- Fake IDs and forged documents became a threat not just to physical venues (bars, borders) but to remote identity systems.
- If a fraudulent document passed IDV at enrollment, it could pollute databases and embed fraudulent synthetic identities that might not be detected for years.

The Regulatory Wave: Privacy as the Backbone of Trust

In parallel with rising adoption of biometrics and booming data collection, regulators around the world began building a legal foundation for trust in digital identity:

- **GDPR** (EU) established strict consent, access, correction, portability, and the "right to be forgotten", with heavy penalties for non-compliance.
- **BIPA** (US State of Illinois) required explicit consent for biometric capture and disclosure, with statutory damages that made ignoring compliance financially dangerous.
- **CCPA** (US State of California) empowered consumers with rights to know, limit, and delete their personal data, influencing many U.S. and global laws.
- **"Children of GDPR" (**LGPD in Brazil, emerging laws in India, UK, Africa, APAC, China, etc.) spread similar principles worldwide.

Collectively, these frameworks:

- Force organizations to treat identity elements—especially biometrics and PII—as sensitive, not just convenient.
- Link trust directly to compliance, making data protection and transparency non-negotiable.
- Push vendors to design privacy-by-default and priva-

GENERAL DATA PROTECTION REGULATION (GDPR): A European privacy law that came into effect in 2018, granting citizens rights over their personal data. The strict nature of GDPR and its focus on empowering end-users have been a strong foundational influence on similar consumer data protection and privacy laws around the world.

BIOMETRIC INFORMATION PRIVACY ACT (BIPA): A 2008 Illinois privacy law concerning the collection of biometric data. Infamous for its heavy penalties, BIPA has led to landmark settlements in the wake of the mobile revolution, as biometrics have become increasingly ubiquitous.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA): One of the first successful privacy laws modeled after GDPR. Like its European counterpart, CCPA formalizes end users' rights to own, control, and delete their personal data.

cy-by-design identity solutions.

In modern digital identity solutions can't be resilient against fraud without being trustworthy under the law—and vice versa.

The Identity Arms Race Enters the AI Era

As enterprise digitalization normalized and biometrics became widespread, **generative AI (gen AI)** arrived. Fraudsters suddenly gained:

- Tools to create high-quality deepfakes (face, voice, full-body video),
- The ability to fabricate realistic identity documents and PII at scale, easily fabricating synthetic identities, and
- A new business model: Fraud as a Service (FaaS), where attackers can buy synthetic identities and ready-made attack kits.

This changed the assumptions behind earlier countermeasures:

- Spoofing no longer required significant skill, expertise, or expensive equipment.
- Deepfakes and synthetic identities could be generated at volume, allowing for sophisticated attacks to be rapidly scaled.

Now, resilience must take into account that:

- Counterfeit identity elements will look and sound extremely convincing.
- Attackers will target every phase—enrollment, authentication, account recovery, support channels, and decisioning systems.

And trust must factor in:

- How systems explain and prove why they accept or reject users.
- What happens to the data they collect in defending against AI-powered attacks.

Next-Generation Privacy and Identity: Aligning Trust and Resilience

With privacy regulations now widespread and AI-powered fraud maturing rapidly, the next generation of identity solutions must

GENERATIVE AI: Artificial intelligence models that can create synthetic content—such as faces, voices, or documents—that can both enhance identity workflows and introduce new deepfake and synthetic-identity risks requiring advanced detection.

MOBILE ID/ MOBILE DRIVER'S LICENSE (MDL): A digital credential securely stored on a smartphone. The best mobile IDs and mDLs are validated against a government system of record, allowing users to control which identity elements they share on a transaction-by-transaction basis.

hardwire trust and resilience into their design. That means:

- **Mobile IDs, mDLs, and Verifiable Credentials** validated against government systems of record, letting users selectively share only the identity elements needed for a transaction.
- Decentralized and hybrid architectures that keep biometric templates on-device when possible, while leveraging trusted systems of record for compliance, KYC/AML, and multi-channel identity.
- **Passkeys** and passwordless flows that use biometrics locally to unlock **cryptographic credentials**—reducing **phishable** secrets and strengthening both security and privacy.
- Advanced liveness detection and deepfake/synthetic identity detection that protect onboarding, authentication, and account recovery from AI-powered attacks.
- Encryption, **anonymization**, and privacy-by-design storage that ensure even in the event of a breach, exposed data is minimized and unusable.

The goal is not just to survive regulation or block a single attack technique—it's to create an identity ecosystem where:

- Trust = compliance, transparency, and user control, and
- Resilience = robust, adaptive anti-fraud defenses that stand up to AI-driven threats.

Where We Are Now

We have arrived at a pivotal moment for digital identity:

- Fraudsters have access to cheap, powerful tools—deepfakes, synthetic identities, scalable botnets, and fraud-as-a-service operations—that can target every digital channel. **Agentic AI** has the potential to scale these threats at an even more unprecedented level.
- Organizations have access to equally powerful tools—biometrics, liveness, provenance, decentralized identity, and advanced privacy-preserving architectures—but must implement them correctly and compliantly.
- Regulators around the globe have made it clear that privacy, user control, and transparency are no longer optional features but mandatory pillars of digital identity.

In other words:

> Digital identity only works if trust and resilience move forward together—trust through privacy-first, compliant

PASSKEY: a passwordless credential based on standards set forth by the FIDO Alliance. Passkeys allow users to sign in to apps and websites using device unlock mechanisms on their computers and smartphones. Because they are device-based, passkeys are privacy-by-design.

CRYPTOGRAPHIC CREDENTIALS: Secure, tamper-evident digital proofs—often tied to government systems of record—that allow users to authenticate or share attributes without exposing underlying identity data.

PHISHING: A deception tactic in which attackers impersonate trusted entities to harvest identity elements or credentials, often serving as a precursor to synthetic-identity creation, account takeover, or deepfake-driven fraud.

ANONYMIZATION: The privacy-preserving process of removing or transforming identity elements so individuals cannot be reidentified, even when their data is used for fraud-detection or system-resilience purposes.

AGENTIC AI: Autonomous AI systems capable of initiating actions, making decisions, and interacting with digital services on a user's behalf, expanding both the opportunity for secure, privacy-preserving automation and the need for continuous verification to prevent misuse or impersonation.

handling of identity elements, and resilience through robust detection and prevention of AI-powered fraud.

Relying parties that succeed in this new landscape will be those who choose vendors and build systems that treat compliance as a core design principle and treat anti-fraud as a continuous, adaptive discipline. Anything less risks not only regulatory penalties and financial losses, but the erosion of user confidence in digital identity itself.

The Prismatic Future: A Trust-Centered Ecosystem

The updated 2025 Prism calls for a fundamental shift in how digital identity ecosystems are measured and managed. No longer is it enough to be a technology vendor, an integrator, or a relying party in isolation. Success is defined by how effectively participants integrate fraud defense, privacy, and customer empowerment into a unified resilience strategy.

The Prismatic Future is one in which:

- Synthetic fraud is anticipated and neutralized.
- Privacy is embedded into every transaction.
- Seamless experiences empower people without eroding trust.

The 2025 Prism is more than a map—it is a blueprint for resilience, a guiding framework for an industry that must now protect and empower at once.

The updated Prism Landscape positions ecosystem participants not simply by function, but by how they perform across the three dimensions:

- **Core Identity Technology Providers** – Anchor resilience through secure biometrics, cryptography, and AI-powered fraud detection.
- **Identity Platforms** – Orchestrate fraud defense, privacy, and user experience across multiple channels and relying parties.
- **Integrators & Solution Providers** – Translate resilience into operational deployments, balancing compliance with seamless flows.
- **Relying Parties** – Banks, governments, healthcare systems, and enterprises that must operationalize resilience at scale.
- **Infrastructure Providers** – Telecom, cloud, and network operators that underpin secure, sovereign, and privacy-compliant identity flows.

2025 Biometric Digital Identity Trend World Map

The 2025 Biometric Digital Identity Trend World Map offers a high-level view of how global regulations are shaping the conditions for trust and resilience in biometric digital identity. In a landscape where privacy expectations, data-protection laws, and AI-driven fraud risks are evolving at unprecedented speed, this snapshot helps relying parties understand the foundational forces influencing how identity elements must be protected, governed, and authenticated.

North America

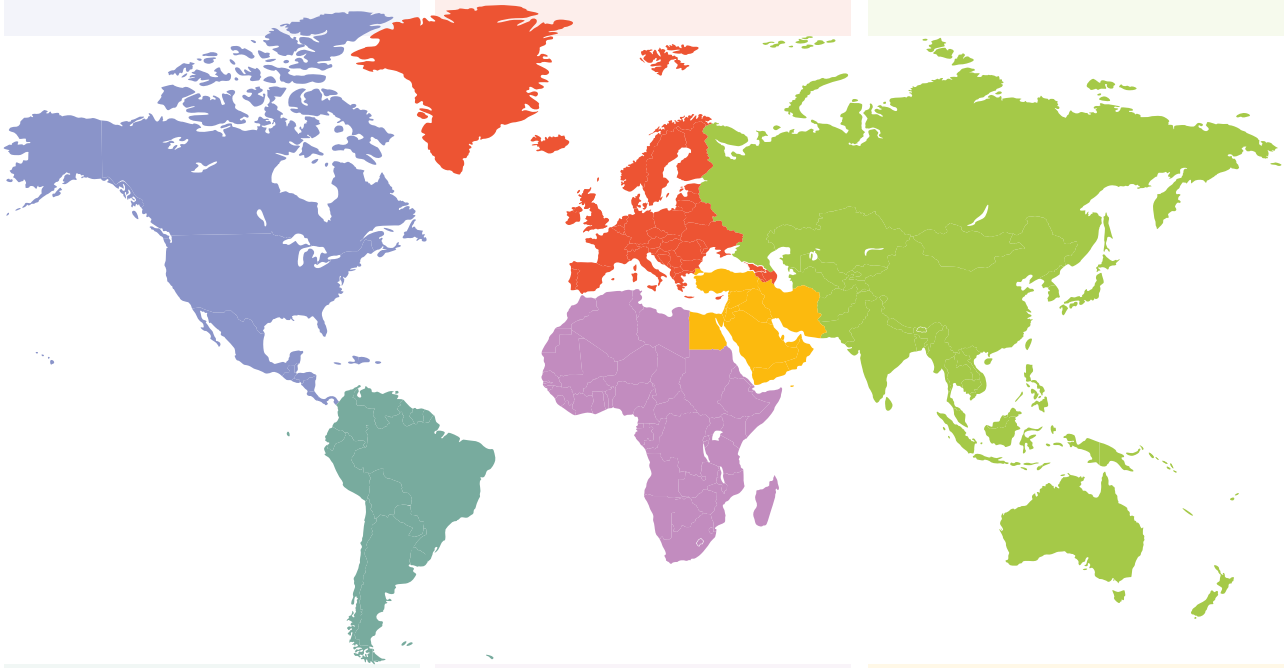
North America is accelerating adoption of mobile IDs and biometric passkey authentication, reinforcing high-assurance digital identity anchored to government systems of record and on-device biometrics. At the same time, enterprises are rapidly upgrading to deepfake-resilient liveness and fraud intelligence as AI-powered identity manipulation becomes a dominant threat.

Europe and the UK

Europe and the UK are shaping global standards through eIDAS 2.0 digital identity wallets and strict GDPR-driven privacy expectations that push biometric systems toward minimization and privacy-by-design. As regulated sectors expand remote onboarding, deepfake-resistant identity proofing is becoming essential to counter rising synthetic and injection-based attacks.

APAC

APAC continues to scale some of the world's largest national digital identity systems, embedding biometrics into payments, government services, and everyday transactions. Rapid fintech growth and heightened fraud pressures are forcing regulators to balance innovation with emerging privacy rules as deepfakes and SIM-swap attacks gain sophistication.



Latin America & South America

Latin America is rapidly embracing face biometrics across banking and government platforms to combat widespread account takeover and synthetic identity fraud. National registries and remote KYC frameworks are expanding, while liveness and document forensics play an increasingly central role in keeping digital channels secure.

Africa

Across Africa, biometric national ID systems are becoming foundational digital infrastructure for inclusion, enabling secure access to banking, SIM registration, and public services. As mobile money scales, countries are adopting selfie biometrics and stronger data-protection rules to counter rising deepfake, impersonation, and data-governance risks.

Middle East

The Middle East is deploying biometric national digital identities and super-app ecosystems that unify government, travel, and financial services under high-assurance authentication. With airport and smart-city biometrics expanding at scale, regulators and financial institutions are tightening anti-fraud controls to address synthetic identities and cross-border financial abuse.

North America

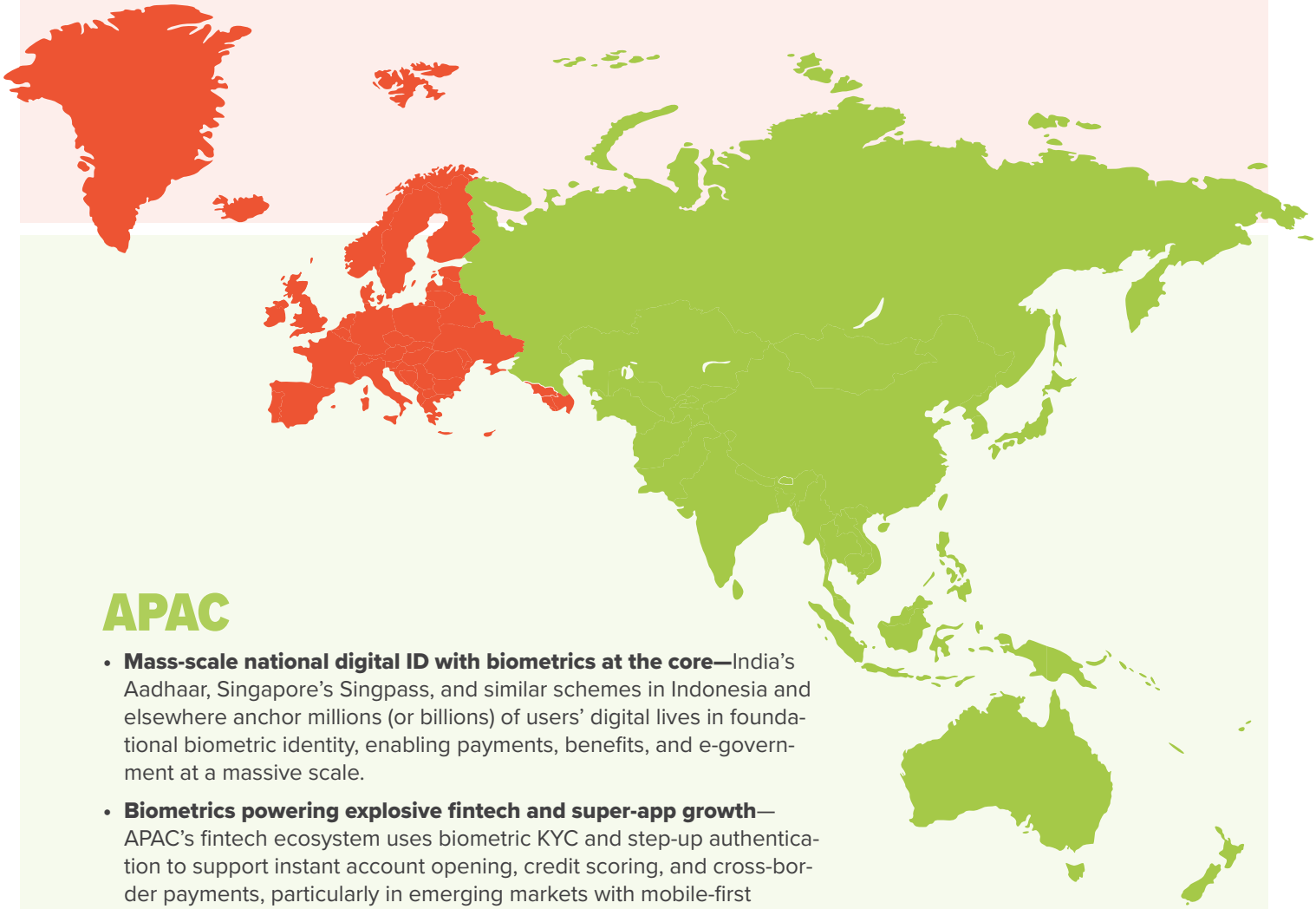
- **Mobile IDs and digital driver's licenses go mainstream**—U.S. states are rolling out mobile IDs and mDLs that tie biometrics to DMV systems of record. These credentials work for airport security, roadside checks, and age verification, creating high-assurance, privacy-aware digital credentials.
- **Passkeys and FIDO-based biometrics replace passwords**—Financial services, technology platforms, and governments are adopting passkeys and FIDO standards so users authenticate with on-device biometrics instead of passwords, cutting phishing risk and strengthening privacy by keeping raw biometric data on user devices.
- **AI-powered fraud drives demand for deepfake-resilient liveness**—Banks and enterprises are upgrading to liveness detection, face/voice matching, and document forensics that explicitly target deepfakes, injection attacks, and synthetic IDs as regulators warn about AI-enabled scams and business email compromise.

Latin America & South America

- **Banking and payments lean hard into face biometrics**—Brazilian and regional banks widely use facial recognition for onboarding and login—around 75% of Brazilian banks already do—making biometrics a primary defense against account takeover and card-not-present fraud.
- **National ID and gov platforms add remote biometric KYC**—Countries like Brazil, Mexico, and Colombia are tying government identity systems to biometric verification and digital channels, enabling remote account opening, welfare distribution, and public-service access with stronger identity assurance.
- **Fighting rampant synthetic identity and social-engineering fraud**—High fraud rates are driving adoption of liveness detection, document forensics, and behavioral risk scoring to detect synthetic identities and deepfake-enabled scams in banking, crypto, and gig platforms.

Europe and the UK

- **EU digital identity wallets under eIDAS 2.0**—The EU is standardizing a cross-border digital identity wallet that will let citizens selectively disclose attributes (like age or license status) using high-assurance biometrics and cryptographic credentials, reshaping public- and private-sector identity flows.
- **GDPR-plus privacy shaping biometric deployments**—Strong data-protection rules (GDPR and incoming AI and data laws) are pushing vendors toward privacy-by-design biometrics—template protection, minimization, and decentralized storage—and driving guidance from groups like EAB and Kantara on safe biometric use.
- **Deepfake-resistant remote onboarding for regulated sectors**—Banks, fintechs, and gambling operators are standardizing remote KYC based on face biometrics, document verification, and liveness tuned to EU AML rules, with growing concern about deepfake identity proofing and injection attacks in video and selfie onboarding.

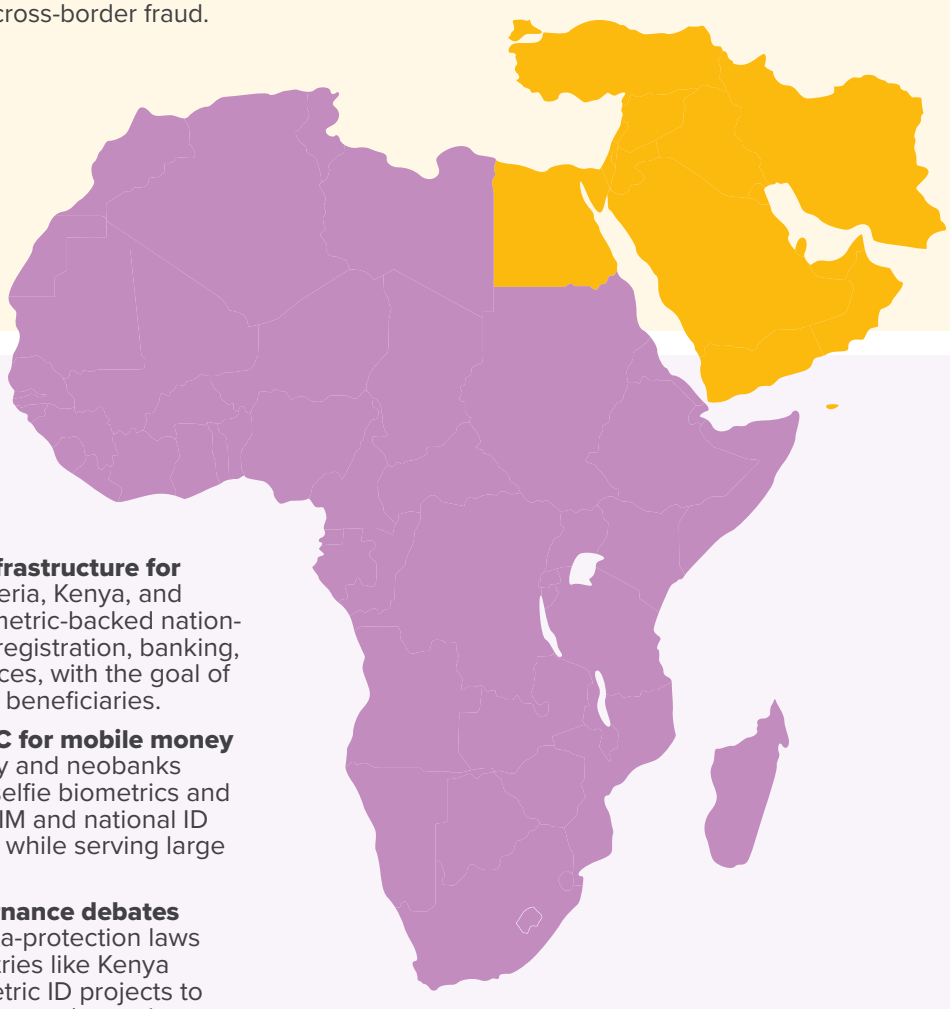


APAC

- **Mass-scale national digital ID with biometrics at the core—**India's Aadhaar, Singapore's Singpass, and similar schemes in Indonesia and elsewhere anchor millions (or billions) of users' digital lives in foundational biometric identity, enabling payments, benefits, and e-government at a massive scale.
- **Biometrics powering explosive fintech and super-app growth**—APAC's fintech ecosystem uses biometric KYC and step-up authentication to support instant account opening, credit scoring, and cross-border payments, particularly in emerging markets with mobile-first populations and thin credit files.
- **Balancing surveillance risks with emerging privacy rules**—Rapid rollout of face recognition in public spaces and financial systems has prompted new data-protection and AI-governance efforts in countries like India and Singapore, as regulators try to keep up with deepfake, SIM-swap, and synthetic-identity fraud.

Middle East

- **Biometric national digital identity and "super app" platform**—Gulf states and others in the region use biometric-backed ID systems such as UAE Pass and Saudi Arabia's Absher as gateways to government and financial services, often integrated into national super apps.
- **Airport, border, and smart-city biometrics at scale**—The region is a testing ground for large-scale face and iris biometrics in airports, borders, and smart-city deployments, aiming for seamless travel and high-security access while raising new privacy and governance questions.
- **Strengthening anti-fraud controls in rapidly digitizing finance**—As digital banking, crypto, and BNPL expand, regulators and financial institutions are tightening biometric KYC, liveness detection, and sanctions screening to counter money laundering, synthetic IDs, and cross-border fraud.



Africa

- **Biometric national IDs as infrastructure for inclusion**—Countries like Nigeria, Kenya, and South Africa are building biometric-backed national ID systems to support SIM registration, banking, voting, and government services, with the goal of reducing exclusion and ghost beneficiaries.
- **Remote onboarding and KYC for mobile money and banks**—As mobile money and neobanks grow, providers are layering selfie biometrics and document checks on top of SIM and national ID data to satisfy KYC/AML rules while serving large underbanked populations.
- **Emerging privacy and governance debates around biometrics**—New data-protection laws and court challenges in countries like Kenya and Nigeria are forcing biometric ID projects to grapple with consent, retention, and security as deepfake and data-breach risks rise.

Trust and Resilience in the Biometric Digital Identity Ecosystem

Protecting identity elements ethically and transparently is the foundation for user confidence, privacy compliance, and continued participation in digital services. At the same time, those identity elements must remain authentic and fraud-resistant in the face of deepfakes, synthetic identities, and AI-driven attacks—allowing digital interactions to remain secure as the threat landscape evolves. This is why it is crucial to understand how trust and resilience interact with the biometric digital identity ecosystem.

To dive deeper into the nuances of AI-powered fraud and privacy in the biometric digital identity ecosystem, download the **Deepfake and Synthetic Identity Prism Report** and the **Privacy and Compliance Prism Report.**

Digital Identity and Identity Elements

At its core, a digital identity is a collection of data that describes a unique human being from the physical world. The Prism Project defines these data points as identity elements. They come in three primary categories that, together, form a fully fleshed-out digital identity: biometric identity elements (templates based on face, voice, fingerprint, or other unique traits), biographical identity elements (PII such as name, address, date of birth, and other life details), and contextual identity elements (metadata like location, device signatures, transaction history, and behavioral patterns). An authentic digital identity is the sum of all these elements, consistently and accurately tied back to a single human being.

Identity elements are not just technical artifacts; they are proxies for a real person's body, history, and behavior. A face template anchors identity to a human body, PII anchors it to their legal and social existence, and contextual data anchors it to time, place, and activity. When these elements are consistent and authentic, relying parties can safely recognize returning users, determine what they are allowed to do, and grant access or privileges. When one or more identity elements are counterfeit, incomplete, or stolen, that trust collapses—creating openings for fraud, abuse, and misuse.

This is where the discussion of trust and resilience begins. Trust arises when identity elements are handled ethically, lawfully, and transparently—meeting privacy and compliance expectations. Resilience emerges when those same identity elements are protected against manipulation, counterfeiting, and misuse—

especially in the face of deepfakes and synthetic identities. Any serious conversation about modern digital identity must start with how we define, own, and safeguard identity elements.

Privacy, Ownership, and Compliance: How Trust Is Built

A digital identity ultimately belongs to the person it describes. Even though organizations receive, process, and store identity elements in the course of providing services—whether banking, healthcare, travel, or social media—the user retains ownership and entrusts those elements to third parties under an implicit and increasingly explicit privacy contract. When identity elements are mishandled, over-collected, sold without consent, breached, or exploited, the individual's privacy is violated, eroding trust not only in a single brand but in digital channels more broadly.

From the user's perspective, this ownership translates into specific entitlements that are now encoded in many privacy regulations: the right to consent (deciding when and how identity elements are shared), the right to access (seeing what is stored about them), the right to maintain (correcting or updating inaccurate PII), the right to deletion, and, increasingly, the right to be forgotten (erasing records and linked transaction histories). These rights define the "trust layer" of identity: users will only continue to participate in digital ecosystems if they believe their identity elements are respected and controllable.

On the organizational side, compliance is how that trust is operationalized. While specific laws vary, best practices converge around seven core principles for handling identity elements:

- **Transparency:** All transactions must be taken with clear notice and consent.
- **Purpose limitation:** Collect identity elements only for legitimate, explained reasons.
- **Specificity:** Collect only what's needed.
- **Accuracy:** Keep biographical elements up to date and user-editable.
- **Temporality:** Store data only for as long as required.
- **Security:** Properly protect identity elements in storage and transit.
- **Good faith:** Act accountably and in line with local regulations.

When organizations uphold these principles, they build durable trust in their treatment of identity elements—setting the stage for resilient anti-fraud measures that users and regulators will

accept.

Deepfakes: Counterfeit Biometric Identity Elements

Deepfake technology weaponizes one of the most powerful categories of identity elements: biometrics. By harvesting images, videos, and audio from public or private sources, machine learning models can fabricate faces and voices that look and sound like real people. These counterfeit biometric identity elements can be used benignly in entertainment, accessibility, and creative applications—but they are increasingly deployed for fraud, impersonation, and identity attacks. Nearly half of organizations report encountering at least one deepfake attack, reflecting how quickly this threat has moved from theoretical to mainstream.

From a digital identity perspective, deepfakes directly target the trust we place in biometric identity elements.

- **Counterfeit image deepfakes** manipulate static photos, undermining legacy "selfie plusID" verification flows by altering the face, the document, or both.
- **Counterfeit video deepfakes** mimic live movement—gestures, blinking, head turns—allowing fraudsters to bypass active liveness detection and even fool humans on video calls.
- **Counterfeit audio deepfakes** use text-to-speech and agentic AI to sound like a target's voice, fooling call-center agents and voice-based biometric systems. In each case, the fraudster isn't stealing identity elements; they are manufacturing new, plausible ones that falsely appear to belong to someone else.

Individually, each deepfake type is dangerous. Combined, face, motion, and voice together can create a full-spectrum biometric doppelganger of a victim, capable of passing many current verification and authentication checks. At that point, organizations face a stark choice: either develop resilient countermeasures that can distinguish authentic from counterfeit biometric identity elements (via liveness, provenance, and specialized detection), or accept that trust in biometric identity will erode to the point where it can no longer serve as a reliable pillar for secure digital interactions.

Synthetic Identities: Counterfeit Collections of Identity Elements

If deepfakes are counterfeit versions of specific biometric identi-

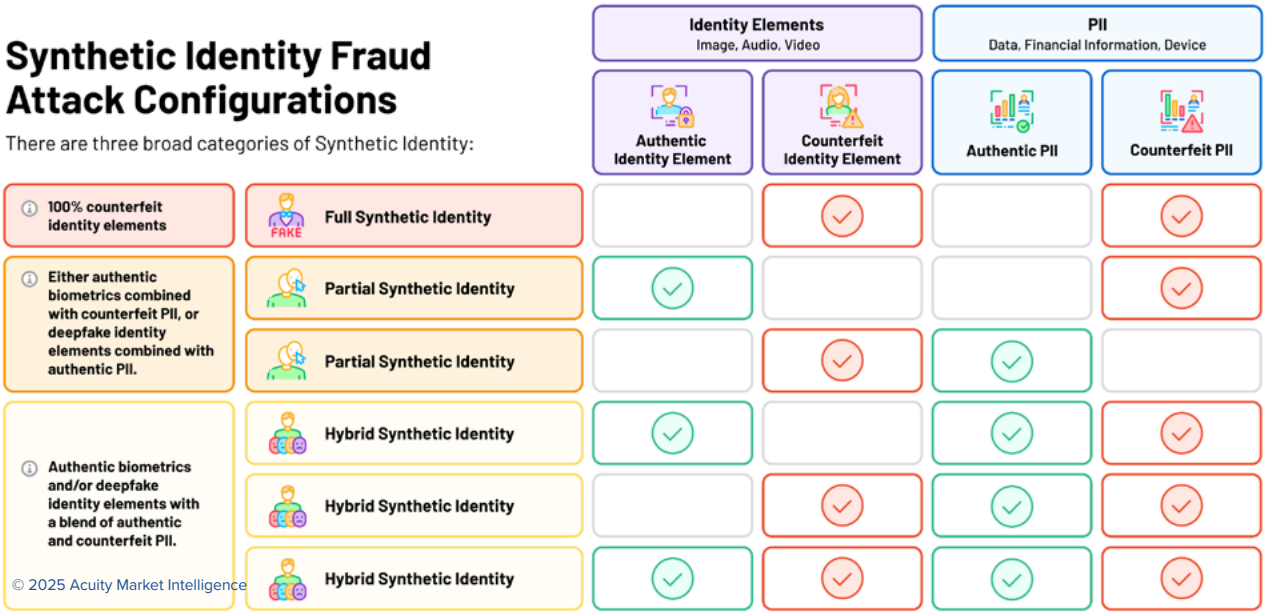
ty elements, synthetic identities are counterfeit collections of identity elements assembled into a plausible digital person. An authentic identity ties biometrics, PII, and contextual data together around a real human being. A synthetic identity, by contrast, is built by forging one or more of those elements—fake faces, fabricated PII, invented histories—until the system accepts it as a legitimate user. Even when some components are real (a genuine face, a real address), one counterfeit element is enough to sever the link to a unique physical person.

Synthetic identities are deceptively powerful because they behave like normal records in a database. They open accounts, pay bills, and slowly build credit or eligibility, often scoring slightly better than average humans. Deloitte estimates that a typical synthetic identity can achieve a credit score around 650, leading to an average pay-off between $81,000 – $98,000. Not bad for for a person who does not exist. Experian reports that synthetic identity fraud may account for up to 20% of loan and credit card charge-offs in the US and is rising sharply in markets like the UK. Because these identities are "born" inside the perimeter—after passing onboarding and IDV tests—they function like an internal fraud vector, slowly draining resources and trust from within.

To better understand and defend against this phenomenon, the Prism Project classifies synthetic identities into three clusters based on their mix of identity elements:

- **Full Synthetic Identities:** entirely fabricated biometrics and PII.
- **Partial Synthetic Identities:** At least one authentic identity element paired with at least one counterfeit element, such as a fake face or fake data configurations.
- **Hybrid Synthetic Identities:** complex blends of authentic and counterfeit biometrics and PII.

The Synthetic Identity Fraud Attack Configuration Chart on the next page illustrates all the ways authentic and counterfeit identity elements can be combined to create these three synthetic identity types.



Despite their differences, they all share the same core problem: databases and decision systems accepting digital identities with no rightful human counterpart—ghosts in the machine that quietly corrode both resilience and trust.

Synthetic Identity: How Identity Elements Are Manipulated

Full Synthetic Identities are built entirely from counterfeit identity elements: a deepfake face, invented PII, fabricated contextual signals. Because they do not reuse stolen images or known data, they often appear unique, making deduplication and simple blacklist approaches ineffective. Only specialized detection systems—capable of analyzing the provenance, structure, and statistical patterns of these identity elements—can reliably surface them. This is one of the clearest examples where human confidence ("we can spot fakes") is dangerously misleading compared to machine-based detection.

Partial Synthetic Identities mix real and fake identity elements, making them especially insidious. "Fake Face Partials" pair authentic PII (like a real person's name and ID number) with a counterfeit face, hijacking the foundational record while replacing the biometric anchor. "Fake Data Partials" do the opposite: they use authentic biometrics bound to fabricated PII, creating entirely new records that appear to be real people but are anchored to a legitimate face. In both cases, some identity elements are valid and can fool systems that only scrutinize one category (just biometrics or just PII) rather than the relationship between them.

Hybrid Synthetic Identities are the Frankenstein monsters of the identity element world: mixtures of authentic biometrics with partial or falsified PII, incomplete data padded with deepfakes, or layered counterfeit PII on top of real people. Each configuration is unique, but the outcome is the same— digital identities with corrupted or ambiguous ties to real humans. Because hybrids live in the gray area between legitimate and outright fake, they demand a layered, identity-element–centric defense: cross-checking biometrics, PII, and contextual histories together, rather than in isolation.

Agentic AI: A New Class of Identity Participant

Agentic AI introduces a transformative shift in the digital identity ecosystem by acting not merely as a tool but as a new category of identity participant—one capable of initiating actions, making decisions, and interacting with services autonomously. In the context of trust, agentic systems must be anchored to authentic human identity elements to ensure that every action they take is authorized, auditable, and attributable to a real person. This requires binding the AI's operational scope to a user's foundational identity, enforcing consent-based delegation, and maintaining strict boundaries around what identity elements an agent may access or use. Much like a human delegate, an AI agent becomes trustworthy only when its permissions, provenance, and behavior remain transparent, controlled, and aligned with the user's privacy expectations.

From the perspective of resilience, agentic AI heightens the need for robust defenses against misuse, impersonation, and manipulation. Because malicious actors can attempt to spoof or hijack these autonomous systems—just as they do with human accounts—agentic AI must operate within identity frameworks that continuously verify authenticity, detect deepfake or synthetic inputs, and validate the integrity of every contextual action the agent performs. Continuous authentication, behavior modeling, and strong provenance checks ensure that AI agents cannot be weaponized as high-speed vectors of fraud. In this emerging paradigm, agentic AI is not a threat to the identity ecosystem but a powerful extension of it—one that, when properly governed and consistently verified, enhances both human trust and systemic resilience in an increasingly automated digital world.

Trust and Resilience: A Layered Approach Around Identity Elements

Taken together, deepfakes and synthetic identities expose a critical reality: identity elements are the battlefield where modern

fraud and privacy risks collide. Fraudsters manipulate biometric, biographical, and contextual identity elements to either impersonate real people or invent entirely new digital personas. Relying parties, in turn, must design systems where every identity element—face templates, PII fields, device fingerprints, behavioral profiles—has its own safeguards, verification checks, and retention rules.

In this landscape, trust comes from treating identity elements in accordance with strong privacy and compliance principles: collecting only what is needed, securing it at every stage of data management, being transparent about its use, and giving users meaningful control. Resilience comes from assuming that any identity element can be forged or blended into a synthetic profile, and building layered defenses that validate authenticity, consistency, and provenance across elements and over time. Synthetic identities and deepfakes can no longer be treated as edge cases; they are systemic threats that emerge precisely where controls are weakest or siloed.

While the fraud landscape is intimidating, the path forward is not to abandon digital identity, but to re-center it on properly governed identity elements. Organizations that succeed will be those that:

- Honor the privacy contract around identity elements to maintain user and regulatory trust.
- Adopt multi-layered, AI-aware defenses that continuously defend those elements against counterfeiting and misuse.

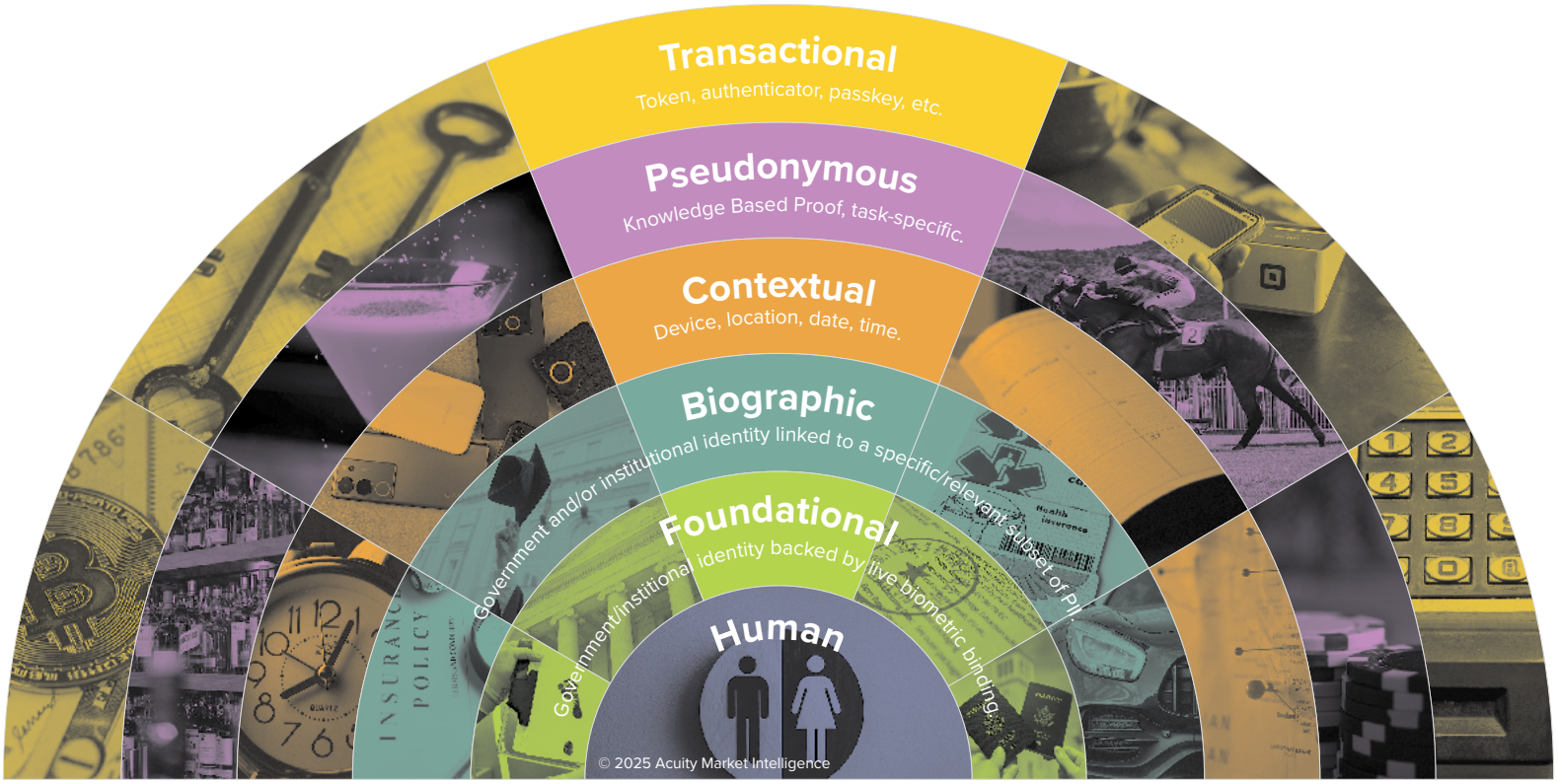
In a world of increasingly convincing digital impostors, trust and resilience are no longer separate goals—they are two sides of the same identity-element coin.

Now that we have a fundamental understanding of Resilient Trust in the biometric digital identity ecosystem, we can examine how these forces tangibly affect end-user identity. For that, we will use the Prism Identity Hierarchy.

Trust, Resilience, and the Identity Hierarchy

The Prism Identity Hierarchy was first introduced in the 2024 Government Services Biometric Digital Identity Prism Report. It represents the five layers of digital identity enabled by the use of biometrics—Foundational, Biographical, Contextual, Pseudonymous, and Transactional.

Deepfake technology and synthetic identities threaten the integrity of user identities at every level of this hierarchy, while privacy and compliance obligations arise wherever identity elements are collected, transmitted, and stored. Taken together, these layers show how trust (built through privacy and regulatory compliance) and resilience (built through robust anti-fraud defenses) must work together for digital identity to function safely at scale.



Foundational Identity

Foundational identity is the core of digital identity and has two components:

- Government-issued identities and physical and/or digital credentials.
- The biometrics that bind those credentials to a real human being.

It is on this foundational layer that all subsequent identity layers can be established with integrity. In a digital world where biometrics, and government-issued identity documents and digital credentials can be compromised or counterfeited, that integrity—and therefore both trust and resilience—are under constant pressure.

Privacy & Compliance (Trust)

From a digital identity standpoint, foundational identity is the most sensitive data an individual possesses, especially when bound to biometrics. This layer should be viewed through the lens of sovereignty and guardianship: foundational identity elements belong to the user they describe, and the relying parties, organizations, or government entities that hold them are responsible for protecting them and preserving the user's rights to access, revision, and deletion. Observing these privacy best practices aligns organizations with strict regulations such as the EU's GDPR, CCPA, and similar global laws, while also supporting compliance with identity-based regulations like KY-ABC and AML that require due diligence in verifying personhood and legitimacy. Foundational identity is therefore both table stakes for digital business and a high-risk compliance zone that must be protected at all costs.

Deepfakes & Synthetic Identities (Resilience)

Deepfakes compromise foundational identity by undermining confidence in the very biometrics and documents that form the base of the hierarchy. If we can't trust that a face, voice, or document is authentic, we can't trust the foundation built upon them. Synthetic identities aspire to infiltrate data stores at this level: if a synthetic identity can be successfully constructed using counterfeit PII or deepfake biometrics, it can enter systems and transact as if it were a real human being. Resilience at this layer requires strong liveness, deepfake detection, provenance, and document-authenticity checks to keep counterfeit identity elements from ever becoming "foundational."

Biographical Identity

Biographical identity is the time-based element of digital identity: where a person was born and lives, what school they attended, their employment history, certifications, and other PII. These details underpin what benefits, rights, and privileges a person can access, and provide a history that can further legitimize a digital identity.

Privacy & Compliance (Trust)

Biographical identity is more fluid than foundational identity—

addresses, jobs, and affiliations change over time—and is often partially public or voluntarily shared. This makes it slightly less sensitive on a per-element basis, but much harder to manage responsibly. Users should be able to control what they want to be public, what they want to be private, and what they want to be deleted or forgotten. For relying parties, this layer demands good "housekeeping": data must be kept up-to-date so licenses, credentials, and benefits remain valid until they expire (at which point they can be revoked); consents must be explicit and understandable, especially when data is used for marketing or research; and users must have easy ways to opt in, opt out, update, or delete their biographical data. Meeting these obligations is essential to sustaining regulatory trust at this layer.

Deepfakes & Synthetic Identities (Resilience)

Deepfakes can be combined with biographical information (e.g., employer, role, history) to make impersonations more convincing—think fake executive videos or fraudulent job applicants that "fit" an expected profile. Synthetic identities use biographical identity in two ways: first, they can borrow or fabricate biographical data to appear legitimate at the outset; second, they can build biographical history over time through fraudulent accounts and transactions, such as carefully managed credit behavior leading up to a large loan scam. Resilience requires detecting subtle inconsistencies, monitoring for abnormal patterns in the evolution of biographical histories, and cross-checking claims against trusted sources.

Contextual Identity

Contextual identity captures how a user typically operates: their usual locations, devices, behaviors, transaction patterns, and the "things they have and know" in real time. It's the behavioral and situational backdrop to identity, describing what a user does typically, where, and with which tools.

Privacy & Compliance (Trust)

From a privacy standpoint, contextual identity is essentially what you do and where you do it at a given moment. Digital identity systems lean heavily on contextual data to confirm that a user is human (and not a bot or AI agent) and detect anomalies that may signal fraud. However, the collection and analysis of this data veers close to surveillance, especially when location, behavioral

analytics, and biometrics are involved. Trust at this layer relies heavily on consent and transparency that grant users the ability to opt in and out of contextual data collection (e.g., location services), review and delete historical data, and have a clear understanding of when, why, and under what conditions this data will be shared. In some jurisdictions, such as under Illinois' BIPA, even biometric-based surveillance for security purposes requires consent and must be managed with strict retention and deletion policies.

Deepfakes & Synthetic Identities (Resilience)

Deepfakes use counterfeit contextual signals to slip past risk-based defenses—appearing to log in from plausible locations, using expected devices, or mimicking typical behavior while the underlying media is forged. Synthetic identities manufacture their own contextual histories through orchestrated transactions and interactions, gradually becoming statistically "normal" in risk engines. At this level, synthetic identities become highly resistant to traditional anomaly-detection systems. Resilience here depends on correlating contextual signals with verified foundational and biographical data, detecting patterns of "too-perfect" normalcy, and employing advanced behavioral analytics that can distinguish genuine human variability from synthetic patterns.

Pseudonymous Identity

Pseudonymous identity is a privacy-empowering transactional layer built on the confidence of strong foundational, biographical, and contextual layers. With an authentic digital identity beneath it, a user can make transactions that rely on their underlying permissions without revealing sensitive details. For example, instead of presenting a driver's license with full name, address, and date of birth to prove age, a pseudonymous transaction simply asserts: "Yes, this user is authorized (e.g., 21+) to purchase alcohol or access age-restricted services."

Privacy & Compliance (Trust)

When implemented correctly, pseudonymous identity is the sweet spot for privacy and compliance. It allows individuals to tightly control which identity elements are shared, minimizing data exposure while still enabling smooth digital experiences. If relying parties can receive trusted pseudonymous assertions—such as "age verified" or "KYC completed"—without storing raw PII or biometrics, they drastically reduce their regulatory

attack surface and liability. Accepting pseudonymous assertions backed by robust lower identity layers becomes a shortcut to compliance: there is no personal data to mishandle.

Deepfakes & Synthetic Identities (Resilience)

Deepfakes threaten this layer by enabling fraudsters to pseudonymously transact using someone else's permissions—for example, leveraging stolen account credentials plus a deepfake voice or face to pass verification and then authorize a transaction "anonymously." Similarly, once a synthetic identity has accumulated enough foundational, biographical, and contextual credibility, it can operate at the pseudonymous level with impunity, enjoying the same privacy protections as real users while executing fraudulent transactions. Resilience here means ensuring pseudonymous tokens and assertions are anchored to authentic, continuously monitored identities, and that detection systems can identify when a supposedly stable pseudonymous identity begins to behave like a fraud vector.

Transactional Identity

Transactional identity is the outermost layer of the hierarchy: payments, logins, and everyday account actions. Many routine authorizations at this level occur without direct reference to foundational, biographical, or contextual identity elements, making this the most lightweight layer—but also the primary surface for attacks and breaches.

Privacy & Compliance (Trust)

Although the identity elements in play at this layer (usernames, masked account numbers, passkeys, tokens) may seem less personal, the systems and data they grant access to often contain highly sensitive foundational, biographical, and contextual information. Historically, some of the most significant data breaches have occurred through compromises at the transactional layer. On the positive side, transactional histories—when properly anonymized—can serve as a privacy-preserving alternative to holding rich PII for marketing and analytics, reducing the liability of managing personal data. To maintain trust and regulatory alignment, organizations must rigorously protect account access, encrypt and minimize stored data, and design analytic practices that rely on pseudonymous or aggregate transactional signals rather than raw identities.

Deepfakes & Synthetic Identities (Resilience)

At the transactional layer, deepfakes are potent tools for impersonation and account takeover—used in call centers, video chats, or voice-based verification to authorize payments, change account details, or initiate scams. Synthetic identities can easily operate here once they've been onboarded, using digital channels to open accounts, make purchases, and execute fraud at scale. Because this layer often interacts with users in "thin" contexts (e.g. a quick login or authorization), it is particularly vulnerable to AI-powered fraud. Resilience requires strong, risk-based authentication; liveness and deepfake detection where biometrics are used; and continuous monitoring for unusual transactional behavior across accounts and channels.

Trust and Resilience Across the Identity Hierarchy

Across the Foundational, Biographical, Contextual, Pseudonymous, and Transactional layers, the Identity Hierarchy makes one thing clear:

- Trust is earned through respecting user sovereignty over identity elements, meeting regulatory obligations, and minimizing exposure.
- Resilience is achieved through anti-fraud defenses—detecting and blocking deepfakes, synthetic identities, and counterfeit identity elements before they can contaminate higher layers or exploit pseudonymous and transactional channels.

Digital identity only works when organizations understand the transactions they conduct at each layer of the Hierarchy, design trusted experiences that honor privacy and regulatory requirements, and deploy a resilient infrastructure that can withstand evolving AI-powered fraud.

Threats and Vulnerabilities to Trust and Resilience

The Identity Hierarchy and the concept of identity elements—biometric, biographical (PII), and contextual—come together in practice through identity verification and authentication processes. These processes capture, transmit, compare, and store identity elements in both remote and in-person contexts. They are also where trust (privacy, transparency, and regulatory compliance) and resilience (protection against deepfakes, synthetic identities, and other fraud) intersect most directly.

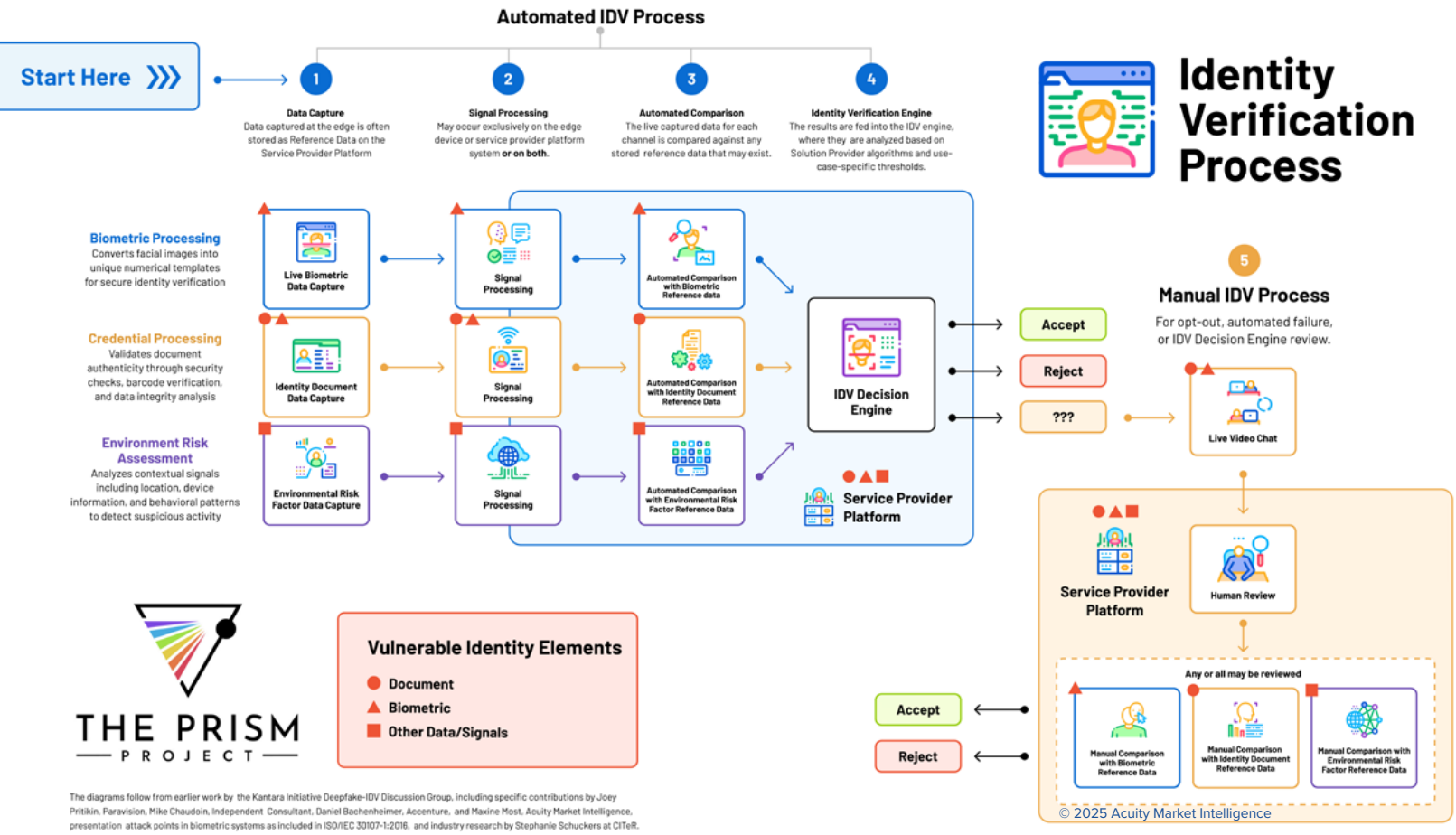
Whether a user is opening a bank account on their phone or passing a biometric gate at an airport, the same basic pattern applies: identity elements are collected, processed, compared with reference data, and used to make a decision about access or authorization. If those identity elements are handled ethically and lawfully, users and regulators can trust the system; if those same elements are rigorously defended against counterfeits and manipulation, the system is resilient against fraud. When either side fails—privacy or security—the entire identity ecosystem becomes fragile.

Understanding how verification and authentication work at a technical and procedural level is therefore essential. It is only by mapping the identity elements as they move through the system that we can see where privacy and compliance vulnerabilities erode trust, and where deepfake and synthetic identity attacks undermine resilience.

The Prism Identity Verification Process diagram on the following page provides this map. The rest of this section describes each step of the process and details the associated vulnerabilities and threats.

How Identity Verification and Authentication Work

Individuals interact with identity systems in two primary ways: automated and manual. In automated flows, users initiate verification themselves by submitting biometric, biographical, and contextual identity elements via edge devices—smartphones, laptops, or kiosks—using sensors such as cameras, microphones, and document scanners. In manual flows, a human reviewer initiates the process, interacting with the user through video, voice, or in-person meetings; this can either stand alone or serve as a backup for users who opt out of or fail automated checks. Both approaches can be used in remote or on-site environments such as bank branches, government offices, or retail locations.



Individuals interact with identity systems in two primary ways: automated and manual. In automated flows, users initiate verification themselves by submitting biometric, biographical, and contextual identity elements via edge devices—smartphones, laptops, or kiosks—using sensors such as cameras, microphones, and document scanners. In manual flows, a human reviewer initiates the process, interacting with the user through video, voice, or in-person meetings; this can either stand alone or serve as a backup for users who opt out of or fail automated checks. Both approaches can be used in remote or on-site environments such as bank branches, government offices, or retail locations.

At the simplest level, identity verification and authentication follow a four-step sequence:

- **Data Capture,** where biometric identity elements (face, voice, etc.), biographical identity elements (Identity documents, credentials, and PII), and contextual identity elements (location, device, behavior, etc.) are collected.
- **Signal Processing,** where these elements are transformed and transmitted for evaluation, either exclusively on the

The Prism Project would like to acknowledge the work of individuals and organizations for their contributions to the analysis in this report. The IDV process diagram, in particular, builds on work by the Kantara Initiative Deepfake-IDV Discussion Group—including specific contributions by Joey Pritikin of Paravision, independent consultant Mike Chaudoin, Daniel Bachenheimer of Accenture, and Acuity Market Intelligence's Maxine Most—as well as presentation attack points in biometric systems as included in ISO/IEC 30107-1:2016, and industry research by Stephanie Schuckers at CITeR.

device, exclusively on the host system, or via a hybrid on-device, server model.

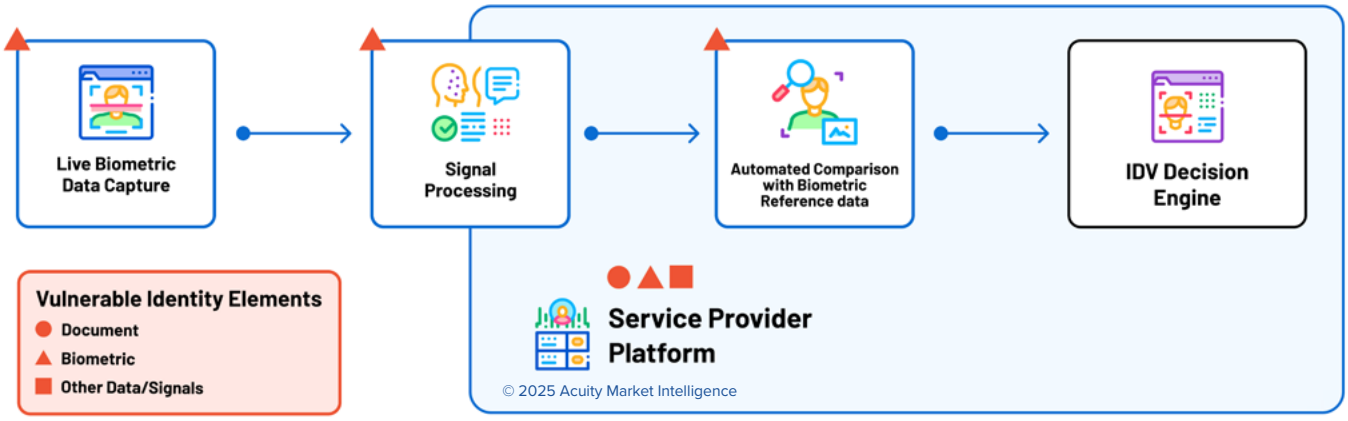
- **Reference Comparison,** where captured identity elements are checked against reference databases, government records, watchlists, and behavioral profiles.
- **Decision,** where the system either grants or denies verification, triggers step-up measures, or routes the user to human review.

This process involves two interconnected systems:

- **End User System (Edge Device),** which captures and sometimes locally processes identity elements.
- **Host System,** which houses IDV software, reference databases, risk engines, and decision logic—often including human reviewers.

Every step and every channel in this pipeline is simultaneously a trust surface (where privacy and compliance must be upheld) and a resilience surface (where deepfake and synthetic identity attacks try to inject counterfeit identity elements). The most trusted and resilient systems encrypt all data in transit and can complete comparison operations with fully encrypted data.

Automated Biometric Processing Channel Vulnerabilities



Trust

In the automated biometric processing channel, trust begins at the biometric capture stage. Users must give explicit, informed consent before their face, voice, or other biometrics are collected; they must know what is being captured, why it is needed, how it will be used, and how long it will be stored. During signal processing, biometric identity elements in transit are particularly

sensitive, requiring strong encryption and clear policies about where processing happens (on-device vs. server) and under what conditions.

At the reference comparison stage, algorithmically derived biometric templates should be used for matching, not the raw images or audio (which are not, by definition, biometric), and comparison should not expose underlying identity elements. After the decision is made—whether to enroll a user, authenticate them, or reject them—any unnecessary data (e.g., biometric or raw images or video) should be purged. If additional biometric evidence (like liveness videos) is retained, for example, to combat high-velocity attacks, that retention must be tightly bound in time, highly secured, and clearly disclosed to users.

HIGH-VELOCITY ATTACKS: High-volume fraud attacks perpetrated in a very short period of time, where the same face may be linked to multiple identities—authentic or synthetic. For more on synthetic identities, download the Deepfake and Synthetic Identity Prism Report.

Handled properly, this channel can sustain trust by demonstrating that biometric identity elements are collected and used only for justified purposes, with minimization, encryption, and controlled retention. That, in turn, creates the regulatory and ethical foundation on which robust anti-fraud controls can operate.

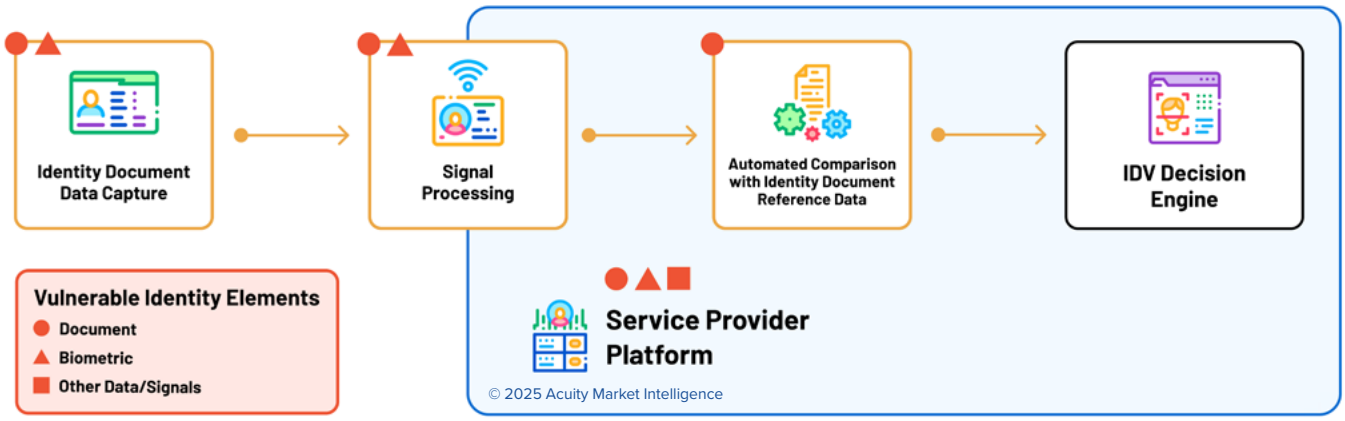
Resilience

The same biometric channel that builds trust is heavily targeted by deepfake attacks designed to compromise resilience. In a deepfake physical presentation attack, a fraudster shows a manipulated face or plays a synthetic voice directly to the sensor during live capture, hoping to generate a false positive match. In a deepfake injection attack, they bypass or simulate the sensor entirely, feeding synthetic biometric data directly into the signal processing or comparison stage so that the host system "sees" fabricated identity elements as if they came from an authentic capture.

A third attack type, the high-velocity synthetic identity attack, typically presents the same face repeatedly (could be the same authentic person or a deepfake), combined with a variety of authentic and counterfeit PII and contextual data, to rapidly test different synthetic identity configurations. This approach aims to slip synthetic profiles through the enrollment pipeline and into the reference database. Once inside, these profiles are treated as valid digital identities, enabling downstream fraud.

Together, these attacks illustrate how combinations of authentic and counterfeit biometric and other identity elements, if allowed to enter or manipulate the verification flow, directly undermine resilience. Effective defenses—advanced liveness detection, deepfake detection, sensor integrity checks, and velocity monitoring—must therefore be built on privacy-respecting biometric pipelines, marrying the trustworthy handling of identity elements with aggressive fraud detection.

Automated Credential Processing Channel PII Vulnerabilities



Trust

The automated credential processing channel focuses on biographical identity elements captured from identity documents, credentials, and forms. At the capture stage, consent is again non-negotiable: users must understand which fields are extracted from identity documents and credentials (passports, driver's licenses, mDLs, etc.), why they are needed, whether the data or images will be retained, and for how long they will be kept. During signal processing PII should be encrypted in transit and organizations must avoid repurposing this data for unrelated uses, such as marketing, without consent.

In the comparison step, stored reference PII should be accurate, up-to-date, and limited to what is required for the stated purpose, such as KYC checks or age verification. Storing unnecessary or duplicative identity elements increases both privacy risk and regulatory exposure. After the verification or authentication decision is made, data not required for ongoing obligations—expired documents, redundant copies, or unused fields—should be purged in accordance with the principles of minimization and temporality.

When these practices are followed, organizations show that they treat biographical identity elements as user-owned assets rather than exploitable slop. That practice underpins regulatory trust, increasing the willingness of users and regulators to accept the strong document checks and watchlist screenings needed to keep bad actors out.

Resilience

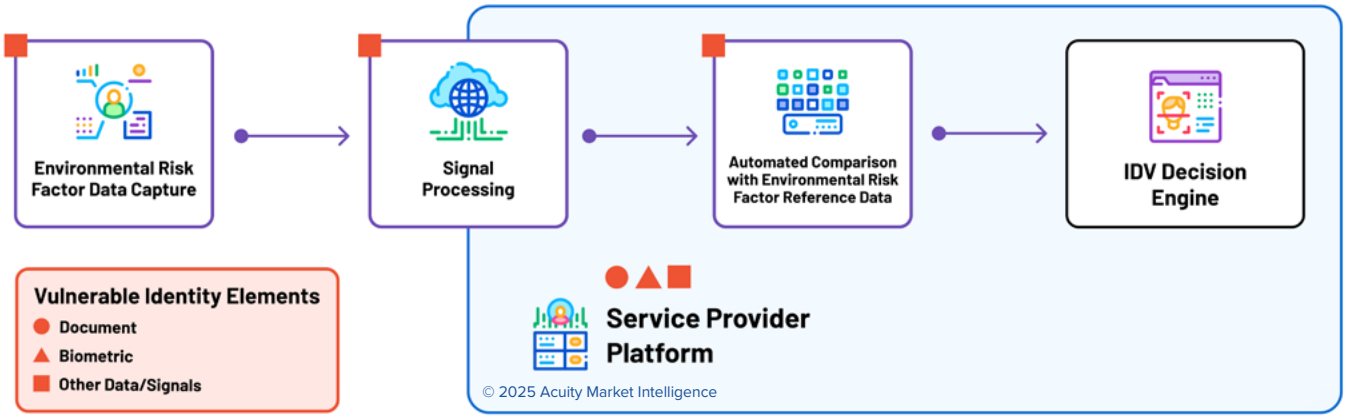
From a resilience standpoint, the credential channel is where bad actors attempt to inject counterfeit biographical identity

elements into the system. In a counterfeit document presentation attack, the fraudster presents fake or altered physical IDs, images, or videos of IDs, or fully AI-generated document deepfakes at the capture stage, hoping they will pass visual or automated checks. In a counterfeit document injection attack, they bypass the capture device entirely, using hardware or software tools to feed manipulated document data directly into the processing or comparison stages.

These techniques support the creation of synthetic identities and the corruption of foundational records. A successful counterfeit document can bind deepfake faces to invented PII or attach authentic biometrics to falsified personal histories, seeding the reference database with identities that have no legitimate real-world counterpart. Once those synthetic profiles are enrolled, they can be used for benefits fraud, credit fraud, or infiltration of controlled environments.

Resilience in this channel depends on robust document authentication (including chip reading where available), cross-checks against trusted sources and watchlists, and analytics that spot patterns of fabricated or impossible PII. Importantly, these anti-fraud controls must coexist with data minimization and user rights to maintain trust while hardening identity verification against synthetic incursions.

Automated Environmental Risk Assessment Channel Contextual Data Vulnerabilities



Trust

The automated environmental risk assessment channel handles contextual identity elements: location, device fingerprints, behavioral patterns, and other metadata. From a privacy perspective, this is the most surveillance-sensitive layer. During risk factor capture organizations must make good faith efforts to clearly inform users what contextual data is being collected (e.g.,

IP address, GPS, device ID), why it is needed, how long it will be retained, how it can be removed or forgotten, and how users can opt out where feasible.

In signal processing, only the metadata necessary for risk evaluation should be transmitted, and it must be protected with strong encryption. For comparison, reference contextual data—historical patterns and known risk indicators—should be tightly scoped and securely stored, avoiding the temptation to indefinitely hoard behavioral data "just in case." Once a decision is made and risk scores or profiles are updated, contextual elements that are no longer needed should be purged in line with stated purposes and retention policies.

Handled this way, contextual identity elements become a trustworthy risk tool rather than a covert tracking mechanism. Users and regulators can see that contextual analysis is being used to protect both them and the system, not to surreptitiously build invasive behavioral dossiers.

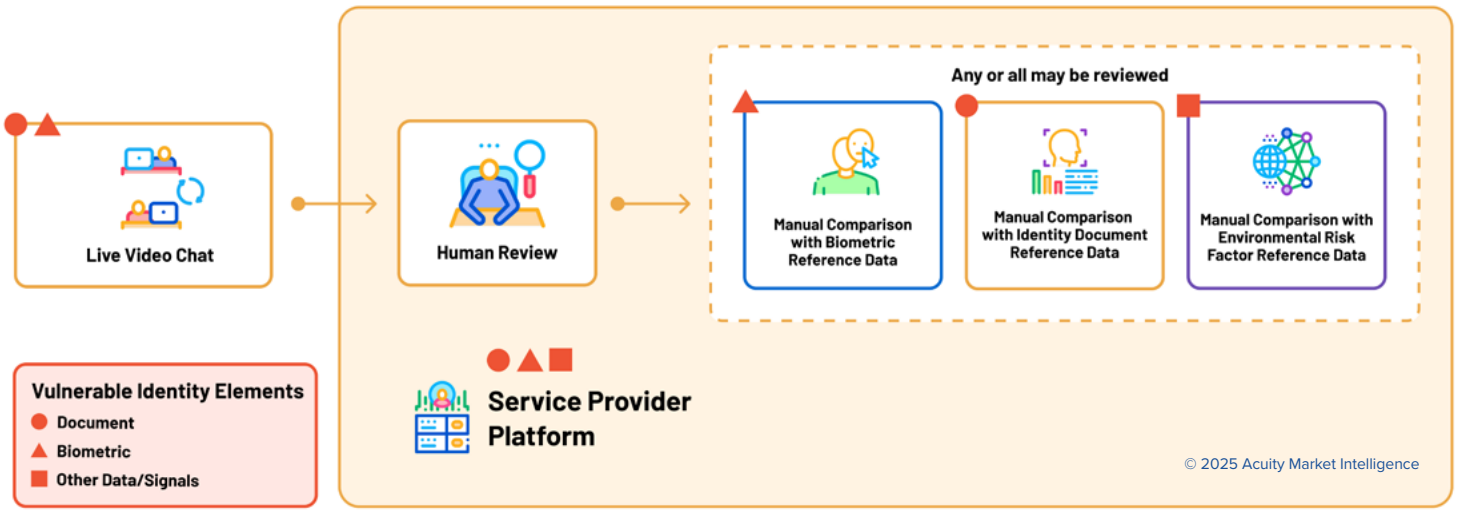
Resilience

Fraudsters target the same contextual channel to defeat risk-based defenses and undermine resilience. In a counterfeit data presentation attack, they manipulate what appears to the system as device behavior or environment: spoofing geolocation, emulating device IDs, intercepting SMS passcodes, or mimicking swipe and typing patterns. The goal is to make risky actions appear consistent with a victim's usual contextual identity so that automated risk engines grant a false sense of normality.

In a counterfeit data injection attack, attackers go further by bypassing the device's real telemetry and feeding fabricated metadata directly into the signal processing or comparison steps. This can make a login from a risky environment appear as if it originates from a trusted network or recognized device, masking account takeover, impersonation, or synthetic identity activity.

Resilience in this layer requires deeper scrutiny of contextual identity elements—cross-correlating them with biometric and PII signals, detecting impossible or conflicting combinations, and monitoring for patterns of "too perfect" normal behavior. As with other channels, these anti-fraud measures depend on—and must not violate—the privacy promises made about contextual data, reinforcing the link between trust and resilience.

Manual Channel Vulnerabilities



The manual channel—live video interviews, voice calls, and in-person review—adds a crucial human element to identity verification and authentication. On the trust side, explicit consent must be part of this process: users need to know when they are being recorded, what identity elements (visual, verbal, document) are being captured, and why. Any physical or digital media created during the session that is not required for audit trails or future verification should be promptly deleted, and human reviewers must be trained not to share, tamper with, or copy identity elements for unauthorized purposes.

However, human review is also vulnerable to live deepfake attacks, where fraudsters combine counterfeit video, audio, documents, and contextual cues to mislead interviewers in real time. Humans are often overconfident in their ability to "spot fakes," even though deepfake quality and sophistication increasingly exceed unaided human perception. This makes manual channels a soft target for attackers who can't easily bypass automated controls but can manipulate human judgment under time pressure.

To maintain resilience, organizations must supplement manual review with technical safeguards—deepfake detection tools, liveness checks, document authentication, and clear escalation paths—while continuing to uphold privacy and consent standards. Manual channels should not be treated as a purely trust-based exception to digital controls; they are another identity element touchpoint where trust and resilience must be jointly deployed.

Host System Threats and Attack Outcomes

Beyond the edge channels, the host system—where reference identity elements are stored and decisions are made—is itself a critical junction of trust and resilience. A reference data attack occurs when authentic biometric, document, or contextual records in the database are replaced with counterfeit identity elements. Once this happens, a fraudster can submit "authentic" data from the edge and still pass, because the system now expects the counterfeit as truth. Insider threats pose a similar risk: compromised staff with access to IDV workflows can inject counterfeit identity elements, override decisions, or approve fraudulent sessions.

All the attacks described across channels—deepfake presentations, injections, counterfeit documents, synthetic context, live deepfakes, reference data manipulation, and insider abuse—serve three main fraud objectives: account takeover (stealing access to an existing identity), user impersonation (wrongfully asserting another user's permissions), and synthetic identity creation (enrolling new digital identities with no legitimate human owner). Each outcome directly weaponizes corrupted identity elements against the verification and authentication processes that are supposed to protect them.

Designing for trust and resilience, therefore, means hardening the host system with strong access controls, auditing, anomaly detection, and provenance tracking for identity elements—while continuing to respect user rights over their data. The more clearly organizations can show that reference identity elements are both well-governed and well-defended, the more confidence users and regulators can have in the decisions those systems make.

Trust and Resilience in Identity Processes

Across every channel and step of identity verification and authentication—data capture, signal processing, reference comparison, decision—the same pattern emerges: identity elements are both the asset to be protected and the target of attack. Trust is earned when organizations collect, use, and retain biometric, biographical, and contextual identity elements in line with clear privacy principles and regulatory requirements. Resilience is achieved when those same elements are safeguarded against deepfake and synthetic identity manipulation at every touchpoint in the process.

The two cannot be separated. A system that focuses solely on fraud prevention while ignoring consent, minimization, and trans-

parency will lose user and regulatory trust. A system that focuses solely on privacy while neglecting deepfake and synthetic identity defenses will become a magnet for fraud. The real challenge—and opportunity—is to design identity verification and authentication processes in which compliant, privacy-respecting treatment of identity elements serves as the foundation for on which effective anti-fraud controls are built.

In an era where attackers can spoof faces, voices, documents, and context with alarming ease, the organizations that succeed will be those that treat identity elements as both sacred and contested: owned by the user, protected by regulation, and defended by layered, adaptive security. That is what it means to build identity systems grounded in Resilient Trust.

Resilient Trust Countermeasures

With global data protection standards converging around GDPR-style principles, trust and resilience are no longer separate tracks—they are mutually reinforcing requirements for any serious biometric digital identity system. The same technologies that minimize data exposure, empower user consent, and reduce regulatory risk also make it harder for fraudsters to weaponize counterfeit identity elements.

What follows is a combined view of proposed privacy solutions and deepfake/synthetic identity countermeasures, framed as a single, holistic toolkit. Each control helps ensure that biometric, biographical (PII), and contextual identity elements are handled in ways that both protect user rights and block AI-powered fraud across the identity hierarchy.

Secure Architecture: Keeping Identity Elements Local, Limited, and Safe

Secure Elements

This countermeasure thwarts:

- Reference Data Attacks

Secure elements are cloistered storage and processing spaces on edge devices—smartphones, wearables, Internet of Things (IoT) objects—where identity elements can be stored, matched, and processed without leaving the device. This decentralized, on-device model is already common for screen unlock and mobile payments. By minimizing the transfer of raw biometrics and PII, secure elements reduce regulatory exposure, shrink the attack surface, and make injection attacks harder to pull off.

Public Key Infrastructure (PKI)

This countermeasure thwarts:

- Reference Data Attacks
- Phishing

PKI protocols enable pseudonymous, transaction-level trust between secure elements and relying parties. When a biometric match is made on-device, the secure element generates a cryptographic key that can authorize a transaction or grant access—without ever transmitting the underlying identity elements. This directly supports privacy and compliance (no unnecessary data sharing) while also hardening against replay and credential-stuffing attacks.

Biometrics On Demand

Biometrics On Demand is an emerging model where biometric checks generate ephemeral public keys that exist only during

the authentication session. Raw biometric data is never stored on devices or servers, nor transferred between systems. This dramatically reduces long-term breach risk while still enabling strong, fraud-resistant authentication—demonstrating that minimizing data retention can simultaneously boost trust and resilience.

This countermeasure thwarts:

- Deepfake Presentation Attacks
- Deepfake Injection Attacks
- Live Deepfake Attacks
- Reference Data Attacks
- Insider Threats

Biometric Templates

Biometric templates are algorithmic representations, stored as mathematical values, derived from the live capture of human characteristics or biological traits, e.g., a face, fingerprint, iris, or voice. They are not stored images. High-quality templates cannot be reverse-engineered into raw image data, meaning that even if compromised, they are not useful for deepfake generation or replay attacks.

This countermeasure thwarts:

- Reference Data Attacks

Encryption & Secure Servers

Encryption transforms legible identity elements into unreadable code, protecting them at rest and in transit across networks and storage. Secure servers—whether in the cloud or on-premises—must be protected physically and virtually, often using privacy enhancing techniques (PET) like breaking up or sharding encrypted data and distributing it across multiple locations so there is no single honeypot of PII to breach. Strong cryptography and hardened server infrastructure are essential for regulatory compliance and for preventing injection and reference data attacks.

This countermeasure thwarts:

- All Injection Attacks
- Reference Data Attacks

Biometric Matching, Liveness, and Deepfake Detection

Biometric Matching / Comparison

Biometric matching is the baseline defense in digital identity, answering the question “who are you really?” by linking a human body to the biometric identity elements stored in a system. At enrollment, biometric matching verifies a user against trusted credentials and/or centralized identity records; during authentication, it ensures that the same person is returning.

This countermeasure thwarts:

- Reference Data Attacks
- Insider Threats
- **High Velocity Synthetic Identity Attack**

Within the host system, biometric search and comparison can also be used to clean reference databases, detecting partial or hybrid synthetic identities that reuse the same or similar face across multiple profiles. This strengthens resilience against synthetic identity clusters while preserving trust, because a clean, deduplicated reference set reduces both fraud and

regulatory scrutiny over bad data quality.

Biometric Liveness & Deepfake Detection

Biometric liveness is a support technology for matching—tuned to detect photos, videos, masks, audio replays, and AI-generated deepfakes in presentation attacks. By passively analyzing micromovements, skin patterns, texture, lighting, and acoustic signatures, modern liveness checks are evolving into deepfake-aware detectors, trained to spot AI tampering artifacts.

This countermeasure thwarts:

- Deepfake Presentation Attacks
- Deepfake Injection Attacks
- Live Deepfake Attacks
- Reference Data Attacks
- Insider Threats

Liveness provides frontline resilience against deepfakes presented to cameras or microphones at enrollment and authentication. When combined with biometric comparison inside the host system, it can also help identify previously enrolled synthetic identities based on deepfaked biometrics. At the same time, liveness allows organizations to continue using high-assurance biometrics without resorting to invasive or excessive data collection, reinforcing trust that biometrics are used strictly for security, not surveillance.

Document and PII Defenses: Privacy-Aware, Fraud-Resistant KYC

OCR and Identity Document Validation

Optical Character Recognition (OCR) uses computer vision to read PII from identity documents presented for verification (e.g. passports, IDs, licenses). This is paired with document validation, which inspects security features, formatting, and other attributes for signs of forgery or tampering. Together, they ensure that the biographical identity elements captured at enrollment are both accurate and authentic.

This countermeasure thwarts:

- Counterfeit Document Presentation Attack
- Counterfeit Document Injection Attack
- Reference Data Attacks

By confirming that PII used in KYC and AML checks is not counterfeit, OCR and validation bolster resilience against document-based synthetic identity attacks while supporting compliance obligations to verify identity using reliable sources.

Chip-based Identity Document Validation & NFC Reading

Chip-enabled identity documents store high-assurance identity elements (including biometrics and PII) protected by private–public key certificates. Real-time chip reading via NFC on edge devices:

This countermeasure thwarts:

- Deepfake Presentation Attacks
- Counterfeit Document Presentation Attack
- Counterfeit Document Injection Attack
- Reference Data Attacks

- Confirms data originated from a legitimate issuer,
- Provides document liveness (the credential is present in a

specific time and place), and

- Eliminates many environmental and integrity issues associated with manual image capture.

By processing chip-side identity elements locally, chip validation and NFC reading minimize reliance on image-based data that can be deepfaked, reducing fraud risk while also limiting unnecessary transmission of PII—an ideal blend of trust and resilience.

Identity Document Liveness & Counterfeit Detection

This countermeasure thwarts:

- Counterfeit Document Presentation Attacks
- Counterfeit Document Injection Attacks
- Reference Data Attacks

Identity document liveness checks verify that a document is a genuine physical credential rather than a screenshot, a printed copy, or a cleverly forged AI-manipulated artifact. Machine vision analyzes lighting, depth, reflections, and signs of image tampering to flag suspicious submissions.

This prevents stolen or synthetic document images from being enrolled alongside authentic biometrics—reducing the risk of synthetic identities hijacking valid foundational identity elements. In doing so, document liveness both protects authentic users' privacy (by blocking the reuse of their stolen IDs) and defends systems against document-based fraud, supporting KYC and AML compliance.

Contextual and System-Level Controls

Data Signature Analysis

This countermeasure thwarts:

- Counterfeit Data Presentation Attacks
- Counterfeit Data Injection Attacks

Contextual identity elements—IP, geolocation, device fingerprints, behavioral patterns—are invaluable for risk scoring but can also be spoofed. Data signature analysis looks for inconsistencies, impossible combinations, or signs of tampering in this contextual data. If something looks off, the transaction can be escalated for step-up verification or human review.

This approach defends against attacks where fraudsters attempt to make malicious sessions appear contextually "normal," and it respects privacy by focusing on limited, purpose-specific risk signals rather than open-ended tracking.

Cryptographic Systems & Secure Servers

This countermeasure thwarts:

- All Injection Attacks
- Reference Data Attacks

As described earlier, strong cryptography and secure server design protect identity elements end-to-end, ensuring that only genuine, untampered data flows through the system. This prevents attackers from inserting counterfeit biometrics, documents, or metadata during transit or at rest.

Beyond improving resilience against injection and reference data attacks, cryptographic rigor helps organizations demon-

strate compliance with stringent data protection and biometric privacy regulations—directly reinforcing trust with regulators and users.

Input Isolation and Control

Protecting capture paths is another key pillar. Input isolation and control techniques physically or logically isolate sensors (cameras, microphones, document readers) from untrusted software and networks, making it much harder for attackers to bypass them and inject fake identity elements. In high-risk scenarios, specialized secured capture devices or supervised in-person enrollment can be mandated.

This countermeasure thwarts:

- All Presentation Attacks
- All Injection Attacks

While this can add friction, it significantly strengthens resilience in critical flows (e.g., high-value onboarding, privileged access) and demonstrates to regulators and users that sensitive identity elements are not being exposed unnecessarily to the broader attack surface—again aligning privacy and anti-fraud goals.

Injection Attack Detection (IAD)

IAD operates during signal processing, scanning data flows for indicators that submissions were injected, replayed, or synthetically generated rather than genuinely captured. It is essentially "liveness for the pipeline," verifying data integrity between capture and comparison.

This countermeasure thwarts:

- All Injection Attacks

By checking the integrity of biometric, PII, and contextual identity elements at every step, IAD reinforces resilience against all injection attack types while supporting trust by enforcing strict, transparent handling rules for identity elements.

Reference Data Comparison

Continuous reference data comparison audits the integrity of the identity database itself—looking for duplicate biometrics bound to multiple records, overlapping or near-identical PII across different profiles, and other synthetic identity signatures.

This countermeasure thwarts:

- Reference Data Attacks

This ongoing hygiene ensures that reference identity elements remain reliable, which is vital for both accurate fraud detection and regulatory-grade due diligence. A clean, well-governed reference set underpins trust in the system's decisions and resilience against the persistence of synthetic identities.

Security Information and Event Management (SIEM)

SIEM systems aggregate logs and events from end-user devices, servers, network infrastructure, and IDV components, applying rules and machine learning to flag anomalies. This gives organizations a real-time, 360-degree view of threats that might

This countermeasure thwarts:

- All Deepfake and Synthetic Identity Threats

compromise identity verification and authentication—from coordinated deepfake campaigns to insider abuse.

By monitoring the broader environment in which identity elements are captured and processed, SIEM tools enhance resilience and demonstrate a mature security posture that regulatory bodies increasingly expect—bolstering trust at an organizational level.

User-Centric Credentials and Hybrid Identity Models

Mobile ID, mDL, Digital Wallets, and Verifiable Credentials (VCs)

Next-generation biometric digital identity solutions—mobile IDs, mDLs, digital wallets, and VCs—embody a hybrid physical–digital paradigm. They combine the privacy benefits of device-based controls with the assurance of government systems of record, giving users direct control over their identity elements.

- **Digital Wallets** securely store and manage digital credentials (mobile IDs, mDLs, VCs) on consumer devices.
- **Mobile IDs** digitize foundational documents (driver's licenses, student IDs, health cards) for both online and in-person use.
- **mDLs** are biometrically bound, government-issued digital driver's license credentials that give users granular control over what elements they share.
- **Verifiable Credentials (VCs)** are cryptographically signed assertions of attributes (age, qualifications, certifications, education, travel eligibility, etc.) that can be shared selectively and are often time-bound (e.g., Digital Travel Credentials for border crossings).

Rather than thwarting specific categories of attack, these technologies heavily limit data exposure, allowing users to disclose only the minimum necessary identity elements per transaction, aligning perfectly with privacy-by-design and minimization principles, while leveraging cryptography and biometrics for fraud-resistant, high-assurance identity proofing.

Governance, Policy, and Hybrid Centralized–Decentralized Models

Policy and Training

Even in an increasingly automated ecosystem, manual identity verification and human review remain critical. Clear internal

This countermeasure thwarts:

- All Deepfake and Synthetic Identity Threats

policies and training ensure that staff handle identity elements properly, understand the risks of deepfakes and synthetic identities, and know when and how to escalate suspicious cases.

By educating reviewers about deepfake techniques, safe interview configurations, and limits on back-to-back sessions, organizations reduce the risk of human error in the face of sophisticated AI attacks. This narrows the gap for live deepfake resilience while reinforcing trust that human handlers are bound by well-defined privacy and security rules.

Hybrid Centralized–Decentralized Identity Models

Modern architectures increasingly blend centralized systems of record (for foundational identity and regulatory assurance) with decentralized, device-based controls (secure elements, biometrics on demand, mobile IDs and wallets). Encryption advances, new standards, and innovation in biometric capture and storage have made it feasible to create hybrid ecosystems where:

- Foundational identity is anchored in trusted, digitally signed, auditable centralized registries.
- Day-to-day transactions rely on pseudonymous, minimal data pulled from user-controlled devices and credentials.

This hybrid approach maximizes privacy, consent, and user control, while giving relying parties the confidence and resilience they need to meet KYC/AML and fraud-prevention obligations. Protecting privacy and defending against fraud stop being competing goals and instead become two sides of the same identity strategy.

Defense in Depth: Privacy as a Security Control, Security as a Privacy Enabler

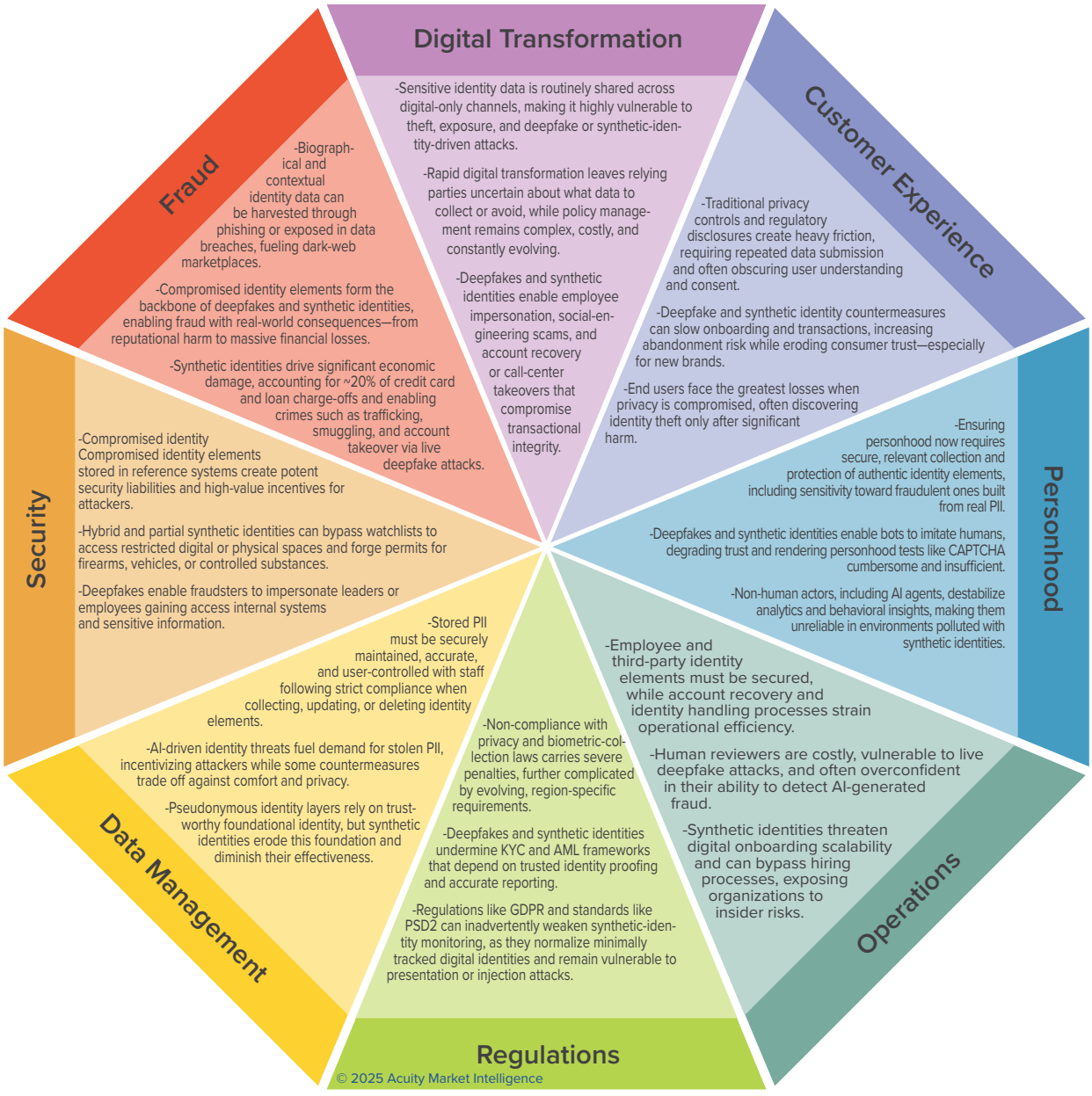
Single-point deepfake and synthetic identity countermeasures are no match for the scope and speed of AI-powered fraud. **But when privacy-preserving technologies (secure elements, templates, wallets, minimization, encryption) are combined with fraud-focused controls (liveness, document validation, IAD, SIEM, reference data comparison), they form an identity-secure ecosystem with live human biometrics at the core.**

In this ecosystem, protecting privacy and defending against fraud reinforce each other. Minimizing and decentralizing identity elements reduces what can be stolen or spoofed; stronger anti-fraud analytics and controls, in turn, protect those elements from misuse or counterfeiting. **The result is a digital identity environment where trust (compliance, transparency, user control) and resilience (robust, adaptive anti-fraud) move**

forward in lockstep—exactly what is needed to withstand the tidal wave of artificial impostors. But what does this technical theory mean for stakeholders with real pain points stemming from digital transformation? For that, we will turn to the Prism Lens.

The Prism Lens

The Prism Lens is a knowledge framework that presents the most critical market challenges facing relying party executives, either within well-defined market sectors, or, in the case of the 2025 Prism Reports, within the context of consequential issues with broad potential disruptive impact across all market sectors—deepfakes and synthetic Identity fraud, and privacy and compliance demands. This version of the Prism Lens shows how converging market demands pose identity-related threats to relying parties and their end users, as trust and anti-fraud resilience become integral to a digitized society.



Solutions

When we break the Prism Lens into its component parts, we examine each challenge individually to see how the application of biometrics and strong identity verification controls can help build Resilient Trust.

Digital Transformation

-Pseudonymous identity transactions Identity transactions enabled by mobile IDs, mDLs, VCs, and passkeys reduce data sharing while maintaining trust, especially when paired with privacy-first pseudonymous biometric identity systems that future-proof compliance.

-Biometric digital identity creates a common language for identity transactions and provides end-to-end protection against deepfakes and synthetic incursions through liveness checks at every authentication point.

-Real-time risk assessment and liveness verification strengthen human review sessions and ensure that all users are genuine humans, not digital impostors.

Customer Experience

-Privacy-first biometric digital identity improves user experience, boosts confidence, and protects users from data breaches through decentralized storage.

-Compliance-forward technologies simplify privacy controls, making consent clearer while preserving seamless, low-friction transactions even in the face of deepfake threats.

-End-to-end biometric identity orchestration, supported by liveness detection and risk assessment, defends against synthetic identities and deepfakes without overwhelming users with friction.

Personhood

-Biometric digital identity can prove personhood without transmitting identity elements, while privacy-first liveness detection anonymizes deepfake-detection data, rendering compromised data useless.

-Deepfake and synthetic-identity detection at onboarding prevents fraudulent identity elements from entering systems, with biometric search/match catching hybrid or partial synthetic identities.

-Persistent liveness detection in face and voice authentication ensures passive, seamless protection against deepfakes and restores trust in digital channels.

Operations

-Biometric digital identity strengthens enterprise operations—from physical access control to time and attendance and digital security—using privacy-by-design principles that reduce exposure to sensitive data.

-Automated, biometric-secured account recovery and liveness-based identity verification prevent synthetic or deepfaked users from creating accounts and reduce malicious bot or agentic agent activity in low-regulation environments.

-Platforms fortified with deepfake and synthetic-ID countermeasures and Agentic AI authentication/verification produce reliable analytics and maintain secure digital operations.

Regulations

-Decentralized biometric digital identity minimizes or eliminates the transfer of identity elements to relying parties, easing compliance and supporting diverse regulatory requirements.

-Biometric identity proofing, authentication, and liveness detection protect remote channels, empower reviewers to detect live deepfakes, and help identify synthetic identities through database matching.

-Organizations adopting privacy-first biometric identity are better positioned to stay ahead of regulatory evolution rather than reacting to it.

Data Management

-Mobile IDs, mDLs, and verifiable credentials can be updated, revised, and revoked on-demand, while decentralized biometric identity gives users secure 24/7 control over their identity elements.

-Minimizing employee contact with biometric identity data strengthens KYC/AML and reduces exposure, while pseudonymous-layer countermeasures limit synthetic-identity threats without sacrificing privacy.

-Deepfake detection protects strong authentication measures, including PSD2-aligned requirements, ensuring data integrity and regulatory compliance.

Security

-Decentralized or hybrid centralized/decentralized identity architectures prevent large-scale identity-element breaches and limit exposure in daily transactions while ensuring system-of-record verification when needed.

-Techniques such as unreversible templates, encryption, anonymization, and fragmentation make stolen biometric data useless, while device-bound biometrics and passkeys ensure identity elements never travel in transit.

-Synthetic-identity countermeasures, liveness detection, and risk-assessment platforms protect watchlists, physical spaces, and official communication channels while resisting phishing—even deepfake-based.

Fraud

-Binding PII and contextual data to biometrics with strong liveness controls makes them unphishable, while decentralized identity prevents large-scale data leaks..

-Deepfake detection, synthetic-ID countermeasures, and biometric search/match reinforce data accuracy, enabling early detection of synthetic identities before they mature into fraud vectors.

-Biometric authentication with liveness detection thwarts account takeover attempts, detects reused biometric data in scalable attacks, and preserves the integrity of authentic digital identities.

Looking Through the Prism Lens

Let's take a closer look at each fragment of the Prism Lens, connecting the challenges and solutions in the context of Resilient Trust. For details and definitions of specific technologies or methods described in the challenges and solutions sections below, see the previous report section, Resilient Trust Countermeasures

Digital Transformation

Resilient Trust Challenges

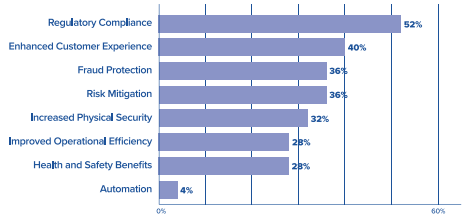
Modern digital transformation has pushed vast amounts of sensitive identity elements into web portals, mobile apps, and remote support channels, making them increasingly vulnerable to theft, manipulation, and AI-enabled exploitation. Organizations must navigate an expanding ecosystem of privacy requirements while determining which identity elements are essential for verification versus which introduce unnecessary liability—an uncertainty amplified by rising deepfake and synthetic-identity attacks. Criminals now use AI-generated voice and video impersonation to breach account-recovery workflows, perform social-engineering scams, and target financial institutions with convincingly forged identity artifacts, prompting warnings from regulators such as FinCEN. This evolving threat environment underscores how deeply transactional integrity depends on the authenticity and protection of identity elements across digital channels.

Resilient Trust Solutions

A privacy-first ecosystem of high-assurance digital identity tools is emerging to mitigate these risks while strengthening both trust and resilience. Mobile IDs, mDLs, verifiable credentials (VCs), and passkeys allow individuals to selectively disclose only the minimal attributes needed for a transaction, reducing exposure of sensitive identity elements in accordance with global data-minimization standards. When paired with pseudonymous biometric identity systems, these technologies support authentication without transmitting raw PII or biometrics, reinforcing trust through user-controlled privacy. Liveness-enabled biometric verification and deepfake-resistant AI enhance resilience by ensuring the entity on the other side of a transaction is a real person rather than an artificial impostor, or unauthorized or

The Prism Project surveyed vertical market stakeholders on their digital technology adoption motivators:

Which benefits of digital transformation motivate your organization to adopt new digital technologies?



malicious AI Agent. Real-time risk assessment adds adaptive defenses that correlate device, behavioral, and environmental signals to route suspicious sessions to enhanced review. **Together, these layers demonstrate that minimizing the flow of identity elements builds trust, while verifying their authenticity at every touchpoint builds resilience against deepfake-driven fraud.**

Customer Experience

Resilient Trust Challenges

Traditional privacy processes—repetitive data submissions, cumbersome disclosures, and inconsistent consent mechanisms—generate friction that undermines digital onboarding and ongoing transactions. Research shows that many users abandon sign-up flows when asked to repeatedly submit the same identity elements, and privacy notices themselves are often too complex for meaningful user understanding (or just too long to bother to read). As organizations introduce additional checks to combat deepfakes and synthetic-identity fraud, abandonment risk rises further—particularly for emerging brands that lack strong trust signals. When privacy protections break down, the consequences fall disproportionately on users: identity-theft complaints continue to be among the fastest-growing categories reported to the FTC, often discovered only after significant personal harm.

68% of consumers are either somewhat concerned or very concerned about their online privacy, according to IAPP's survey of nearly 5000 individuals across 19 countries.

Deepfakes reduce consumer confidence in online commerce. More than half (56%) of UK consumers are worried they could be scammed by deepfakes.

Resilient Trust Solutions

Privacy-first biometric identity systems directly address these challenges by making authentication seamless while reducing data exposure. Decentralized approaches—such as passkeys, mobile IDs, and verifiable credentials—enable users to authenticate without transmitting raw identity elements, lowering breach risk and strengthening trust by keeping sensitive information under user control. Selective disclosure, cryptographically verifiable claims, and simplified consent interfaces streamline experience while ensuring regulatory alignment. Meanwhile, template-based biometrics, passive liveness, and adaptive risk scoring maintain resilience by preventing synthetic identities and deepfake impersonations from entering or abusing digital ecosystems. **This combination proves that strong privacy and strong security enhance customer experience: minimizing identity-element sharing builds trust, while layered biometric assurance delivers resilience against AI-driven attacks.**

Personhood

Resilient Trust Challenges

The emergence of agentic AI—autonomous AI systems capable of executing multistep tasks, interacting with APIs, and adapting to real-time feedback—has intensified longstanding challenges around proving personhood online. Deepfakes and synthetic identities already mimic human faces and voices with high fidelity, but agentic AI enables these inauthentic entities to interactively and persistently perform end-to-end fraud operations. Research shows that such AI systems can bypass or fool basic tests of personhood like CAPTCHA, imitate human browsing patterns, and conduct convincing social-engineering conversations. Simultaneously, non-human traffic is polluting analytics and behavioral baselines: bots now represent a significant share of global activity, making behavioral detection increasingly unreliable. Adding to the complexity, many synthetic identities incorporate fragments of authentic PII, blurring the distinction between genuine individuals and AI-generated impostors.

Learn more about how biometrics protect personhood in the Deepfake and Synthetic Identity Prism Report.

API (APPLICATION PROGRAMMING INTERFACE): A set of rules that allows different software programs to communicate with each other and exchange information in a safe, structured way.

88% of total detected deepfakes target crypto platforms, with Elon Musk impersonations driving 32% of phishing attacks.

Resilient Trust Solutions

Privacy-preserving biometric identity restores personhood assurance by confirming the presence of a live human without exposing raw identity elements. Modern biometric systems rely on on-device templates and privacy-first liveness detection that analyze micro-expressions, vocal dynamics, or movement patterns while discarding sensitive imagery—meaning even intercepted data cannot be reverse-engineered into a usable identity. At onboarding, deepfake and synthetic-identity detection systems prevent manipulated or agentic-AI-generated profiles from entering identity ecosystems, while biometric search/match tools identify duplicates or inconsistencies across datasets. During authentication, continuous passive liveness checks ensure that the user interacting with the system is a human—not a bot or autonomous AI agent. **These measures enhance trust by limiting the number of identity elements organizations see, while delivering resilience by preventing automated, scalable fraud attempts powered by agentic AI.**

KYC and AML fines increased 417% year over year, globally, for the first half of 2025, amounting to $1.23 billion across 118 fines, according to Fenegro.

Operations

Resilient Trust Challenges

Enterprise operations are increasingly strained as agentic AI systems become capable of harvesting employee identity elements, imitating internal communication patterns, and

performing deepfake-driven impersonation during onboarding or account recovery. In a 2025 IRONSCALES survey, 85% of the 500 IT and cybersecurity professionals questioned reported their organizations experienced one or more deepfake-related incident in the past 12 months. **Human reviewers—once a key fallback for identity verification—are increasingly outmatched; studies show that humans perform no better than random guessing when distinguishing AI-generated faces from real ones.** At the same time, synthetic identities, many of which are enhanced by agentic AI, can infiltrate hiring pipelines or credential-issuing processes, creating insider threats that are extremely difficult to detect. Operational bottlenecks, such as manual identity handling and high-touch account-recovery workflows, further increase exposure, cost, and risk.

In the healthcare industry, deepfake technology can be used to impersonate staff, enabling the fraudulent extraction of patient medical records, which can sell for hundreds of dollars a piece on the dark web, or to redirect prescriptions.

Resilient Trust Solutions

Privacy-by-design biometric identity systems help restore operational stability by strengthening authentication processes while reducing the exposure of sensitive data. Encrypted biometric templates, on-device matching, and robust liveness detection ensure that employees and third-party contractors can authenticate securely without transferring raw identity elements. Automated, biometric-secured account recovery reduces operational burden while preventing synthetic or deepfake-driven impersonators from escalating privileges or creating fraudulent accounts. Deepfake detection and synthetic-ID countermeasures reinforce verification workflows, while agentic-AI-aware authentication pipelines help maintain clean, trustworthy analytics and system logs. **Together, these capabilities enhance trust by upholding strict privacy principles and controlling exposure of identity elements, while reinforcing resilience by making it far more difficult for AI-enabled impostors to compromise enterprise operations.**

Deepfakes and synthetic identities undermine Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, which carry non-compliance fees—banks paid over $3.2 billion in AML fines alone in 2024.

Regulations

Resilient Trust Challenges

Organizations face growing regulatory scrutiny as global privacy and biometric laws—such as GDPR, CCPA, and BIPA—impose strict requirements around consent, minimization, and secure handling of identity elements. Penalties for violations have reached multimillion-dollar levels across sectors. Meanwhile, KYC and AML regimes are being challenged by deepfake-enabled impersonation and synthetic identities, which undermine remote onboarding and distort identity-verification datasets.

PSD2: A European Union regulation that modernizes payment security by requiring strong customer authentication, enhancing consumer protection, and enabling secure open-banking data sharing between financial institutions and third-party providers.

Regulators like FinCEN warn that deepfakes are now actively exploited to falsify customer interactions and impersonate employees. Standards like **PSD2**, while intended to strengthen authentication, remain susceptible to presentation and injection attacks, and GDPR-style minimization can inadvertently make synthetic-identity monitoring more difficult by reducing behavioral history.

Resilient Trust Solutions

Decentralized and privacy-first biometric identity solves these tensions by reducing regulatory exposure while hardening fraud defenses. Technologies such as mobile IDs, mDLs and verifiable credentials allow users to store, and control identity elements locally on their own devices, minimizing the data collected or retained by organizations and aligning naturally with global privacy expectations. Liveness-enabled biometric verification and deepfake-resistant authentication strengthen resilience by filtering out AI-generated impostors before they enter KYC/AML pipelines, while biometric database matching helps identify hybrid or partial synthetic identities early. Organizations that adopt these privacy-forward systems position themselves to stay ahead of regulatory evolution rather than reacting to it. **By uniting strict privacy controls with advanced anti-fraud capabilities, decentralized biometric ecosystems simultaneously reinforce trust in how identity elements are handled and build resilience against AI-powered impersonation and financial-crime risks.**

Data Management

Resilient Trust Challenges

Organizations now store unprecedented volumes of identity elements—PII, biometrics, and contextual metadata—and must maintain them securely, accurately, and in alignment with user-control requirements. Yet, identity-related data remains the most frequently compromised category in breaches, driving regulatory penalties and significant remediation costs. Attackers continue to harvest stolen identity elements for creating synthetic identities, exploiting incomplete or outdated datasets to slip through onboarding and poison foundational identity layers. Synthetic identities can undermine pseudonymous identity frameworks that rely on trustworthy underlying data, destabilizing authorization and degrading the effectiveness of selective-disclosure systems. Meanwhile, some security practices—like persistent behavioral tracking—risk conflicting with GDPR-style privacy expectations, highlighting the delicate balance organizations must strike.

Physical data centers are vulnerable to insider threats, which cost companies an average of $4.92 million per incident, according to IBM.

Resilient Trust Solutions

Privacy-first, decentralized identity systems strengthen both trust and resilience by reducing the amount of sensitive identity data organizations must store while improving the assurance of the data that remains. Mobile IDs, mDLs, and verifiable credentials let users update, revoke, or refresh attributes on demand, keeping identity data accurate without exposing raw PII to relying parties. On-device biometric matching minimizes employee contact with sensitive identity elements, supporting stronger KYC/AML compliance and reducing insider risk exposure. Deepfake detection, passive liveness, and robust biometric authentication ensure that only legitimate human users can perform high-assurance transactions, reinforcing PSD2-aligned authentication protections and safeguarding data integrity. **By preserving user control, limiting stored identity elements, and validating authenticity at every interaction, these systems advance trust through privacy, and resilience through fraud resistance.**

Security

Resilient Trust Challenges

Compromised identity elements stored in reference systems remain high-value targets for attackers, contributing to some of the most damaging breaches across industries. Criminal groups now exploit hybrid and partial synthetic identities—blending real and fabricated identity elements—to bypass watchlists, enter restricted locations, or fraudulently obtain access to regulated resources. Deepfake-driven impersonation of executives and employees adds another layer of risk, with regulators warning that AI-generated voice and video impersonation is increasingly used in account-takeover, wire fraud, and internal system manipulation schemes. These converging risks make traditional authentication insufficient, particularly when identity elements can be intercepted, replayed, or forged.

When a partial or hybrid synthetic identity is successfully established in the reference data of a biometrically enabled expedited fan or employee access system—through remote enrollment or injection attacks—bad actors, including banned fans, known criminals, or terrorists, can pass through security at stadiums, arenas, and event venues.

Resilient Trust Solutions

Modern identity-security architectures mitigate these threats by combining privacy-preserving decentralization with strong cryptographic and biometric assurance. Decentralized and hybrid identity models—using verifiable credentials, device-bound biometrics, and selective disclosure—minimize the transmission and storage of identity elements, reducing breach incentives and exposure while ensuring high-assurance verification when needed. Even if attackers obtain biometric or contextual data, templating, encryption, anonymization, and fragmentation techniques render it useless. Passkeys built on the FIDO standard keep biometrics local to the device and eliminate reusable authentication secrets, making phishing—including deepfake-enhanced phishing—ineffective. Liveness checks, synthetic identity detection, and real-time risk assessment further ensure that only legitimate human users—not bots,

not deepfakes, not composite synthetic identities—can authenticate or transact. **These combined measures reinforce trust by limiting identity element exposure and strengthen resilience by creating a deepfake-resistant security perimeter.**

Fraud

Resilient Trust Challenges

Fraud operations increasingly rely on stolen identity elements harvested through phishing, malware, and large-scale breaches, fueling extensive underground markets for PII. Synthetic identities—often assembled from fragments of real identity data—enable fraudsters to impersonate individuals, bypass onboarding controls, and conduct scalable financial crimes. Once embedded, these identities can support downstream abuses such as account takeover, organized criminal activity, and cross-border smuggling. The growing sophistication of deepfake voice and video tools has enabled fraudsters to manipulate call centers, exploit recovery workflows, and deceive employees into releasing sensitive access or information. With traditional controls increasingly ineffective, organizations must find ways to secure identity elements while ensuring they remain accurate, high-integrity, and resistant to manipulation.

With traditional controls increasingly ineffective, organizations must find ways to secure identity elements while ensuring they remain accurate, high-integrity, and resistant to manipulation.

Resilient Trust Solutions

Biometric identity systems strengthened with privacy-preserving liveness detection and device-bound verification technologies help prevent these fraud vectors by ensuring identity elements cannot be phished, stolen, or replayed. Decentralized identity models reduce reliance on centralized data stores, limiting the raw material available for synthetic identity creation and reducing breach impact. While sophisticated data management techniques like decentralized storage of sharded data and **homomorphic and quantum-resistant encryption** can eliminate the susceptibility of centralized data "honey pots" altogether, advanced detection tools—deepfake analysis, biometric search/match, and synthetic-ID countermeasures—improve the accuracy of identity ecosystems and allow early identification of suspicious or duplicated identity elements. Persistent liveness-enabled biometric authentication thwarts account takeover attempts, catches reused data in scalable attacks, and preserves the integrity of authentic digital identities. **By ensuring that identity elements remain private, verifiable, and human-anchored, these systems reinforce trust and establish resilience against AI-powered fraud.**

HOMOMORPHIC AND QUANTUM RESISTANT ENCRYPTION: Cryptographic methods that allow data to remain encrypted even while being processed, and are designed to withstand attacks from both classical and future quantum computers.

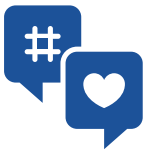
With these eight pain points broadly understood, we are now equipped to take a closer look at how they manifest specifically in the vertical markets most affected by accelerating digital transformation trends.

Trust and Fraud Resilience Vulnerabilities by Vertical Market

Deepfakes, synthetic identities, and escalating privacy and compliance demands collectively define a new era of digital identity trust and resilience. As AI-powered fraud is projected to drive $40 billion in annual global losses by 2027, organizations must recognize that both identity manipulation and inadequate data governance pose equal threats to transactional integrity across all sectors. To clarify the breadth of these challenges, the Prism Project has aggregated research and conducted original analysis to reveal how representative verticals are simultaneously exposed to deepfake- and synthetic-identity risks as well as privacy and compliance vulnerabilities. Protecting authentic identity elements is no longer just good practice—it is a foundational requirement for maintaining trust, meeting regulatory obligations, and safeguarding long-term reputational and financial stability. As digital transformation accelerates, relying parties must adopt privacy and compliance-first identity strategies with the same urgency they apply to detecting and mitigating deepfake and synthetic-identity fraud.

The following table illustrates how these interconnected vulnerabilities impact relying parties and their customers across key vertical markets:

Vertical Market	Trust and Fraud Resilience Vulnerabilities
Financial Services 	• High-impact breaches and costs: Major financial institutions like JPMorgan Chase, Equifax, and Capital One have suffered large-scale data breaches, with the average incident in this sector costing $6.08 million. • Evolving AI-driven threats: Deepfakes and synthetic identities enable fraud, market manipulation,Deepfakes and synthetic identities enable fraud, market manipulation, and identity theft—undermining KY-ABC and AML safeguards, and contributing to 20% of credit and loan charge-offs. • Regulatory and trust challenges: The financial sector faces strict compliance demands (KYC, AML, PSD2) amid growing AI-powered fraud and eroding customer confidence, resulting in billions in AML fines in 2024.
Healthcare 	• Deepfake-enabled medical fraud: Voice cloning and impersonation allow attackers to steal or redirect patient records and prescriptions, with medical data selling for hundreds of dollars on the dark web. • Synthetic identity exploitation: Stolen health records can train AI to create fake PII, enabling synthetic identities to be used to obtain controlled substances—opioids account for 80% of drug-related deaths globally. • Rising regulatory and ransomware risks: Despite strict laws like HIPAA, healthcare organizations remain prime ransomware targets, with 69% of all compromised patient records in 2024 linked to such attacks.
Insurance 	• Deepfakes and synthetic identities: AI-generated identities can infiltrate insurance databases to falsify customer records and submit fraudulent claims, distorting premiums. • Identity amplification: Fraudulent insurance accounts help synthetic identities appear legitimate, enabling larger and riskier financial transactions over time. • High-value data targets: Insurers store vast amounts of sensitive personal data, making them prime targets for cyberattacks seeking PII "jackpots."

Vertical Market	Trust and Fraud Resilience Vulnerabilities
Government Services 	• Deepfake-enabled identity fraud: AI-generated media can be used to create counterfeit foundational identities, enabling bad actors or synthetic personas to obtain official physical and digital credentials, like licenses, passports, mDLs, or other VCs. • Exploitation of public funds: Synthetic identities can fraudulently access government payments such as pensions, benefits, and grants intended for genuine citizens • High-value government data targets: As custodians of citizen identity systems, governments face persistent cyber threats and have suffered major breaches worldwide—including in India, Ethiopia, Iran, the USA, and China.
Retail & eCommerce 	• Deepfake-driven retail fraud: Counterfeit PII enables synthetic identities to exploit in-store application processes for loyalty fraud—estimated at $1–3 billion globally. • Eroding consumer trust and privacy: Over half of UK consumers fear deepfake scams or image misuse, while strict privacy laws like GDPR constrain data collection and marketing practices. • Cyber and compliance pressures: Major 2025 retailer breaches (e.g., Adidas, Harrods, Marks & Spencer) underscore vulnerabilities, driving a shift toward pseudonymous, transaction-based profiling as a compliant alternative.
Travel 	• Supply chain vulnerabilities: Breaches at Southwest and American Airlines in 2023 exposed pilot data, showing how third-party weaknesses can compromise identity security and privacy. • Biometric travel risks: Widespread use of facial recognition to expedite travel demands both strict consent and data policies to protect the privacy of legitimate travelers, and extensive liveness and deepfake countermeasures to detect synthetic or hybrid identities submitted via remote enrollment. • Deepfake-driven threats: AI-generated media can facilitate loyalty fraud, trafficking, and smuggling.
Hospitality 	• AI-enabled access and fraud: Counterfeit identity elements such as deepfakes and device spoofs can bypass digital room security, while synthetic identities enable loyalty program fraud. • High-profile data breaches: Marriott's 2018 breach exposed personal data of over 500 million guests, resulting in significant reputational harm and $52 million in penalties. • Compliance and verification risks: Hospitality providers must handle sensitive identity data and credentials, placing them in high-risk regulatory and privacy positions. Decentralized identity solutions like VCs can limit customer exposure and service provider liability.
Social Media 	• The three foundational social media platforms all suffered major data Widespread data breaches: In 2021, major social media platforms were compromised— 533M Facebook users, 221.5M Twitter users, and 700M LinkedIn users affected. • Identity-focused scams: Social platforms serve as key vectors for stealing passwords, financial data, and PII, often through deepfake-enabled deception. • Synthetic identity and bot amplification: Fake accounts and bots—responsible for 37% of internet traffic—fuel misinformation, exploit users, and erode trust in online communication. Agentic AI is poised to rapidly accelerate the magnitude of this problem.
Gaming 	• Fraud and regulatory breaches: Deepfakes and synthetic identities enable underage or ineligible users to bypass KYC and AML controls in online gaming and gambling. • Strict compliance requirements: The gambling industry is heavily regulated, requiring adherence to KYC, AML, and regional age-verification policies. • Gaming sector vulnerabilities: Video game companies, including Ubisoft, Blizzard, and Nintendo, store sensitive identity data and have experienced notable data breaches.

Vertical Market	Trust and Fraud Resilience Vulnerabilities
Controlled Substances, Products & Content 	• Deepfake-enabled age fraud: Counterfeit videos and images can defeat online age-verification systems, giving minors access to illicit substances and adult content. • Synthetic IDs in the physical world: Partial or hybrid synthetic identities can generate convincing fake IDs, enabling underage access to restricted goods such as drugs, firearms, and pornography. • Privacy-preserving alternatives: Traditional age checks expose excessive personal data, while pseudonymous verification reduces data sharing and strengthens authentication assurance.
Fan Experience 	• Security risks from synthetic identities: Partial or hybrid synthetic identities inserted into biometric access systems can allow banned individuals, such as fans, criminals, or terrorists, to bypass stadium and arena security; they can also be used to coordinate large-scale ticket-buying for scalping operations worth millions. • Major data exposure incidents: The 2024 Ticketmaster breach compromised data for 560 million customers, resulting in litigation, reputational harm, and substantial credit-monitoring costs. • Growing biometric adoption and compliance needs: As venues expand biometric systems for ticketing, entry, concessions, and staff access, they must secure explicit consent and maintain strong privacy and data-management policies—47% of stadiums report biometrics on their 2024 roadmaps.
Digital Entertainment 	• Privacy and consent requirements: Growing personalization and hands-free features in digital entertainment require strong consent mechanisms and the ability for users to update or delete identity-linked data. • Synthetic identity misuse: Fake or synthetic identities can enable account sharing, unauthorized access, and large-scale content piracy. • Deepfake-driven IP violations: AI-generated video, image, and audio deepfakes can be used to infringe on creators' and studios' intellectual property rights.
Border Control and Immigration 	• High-stakes identity handling: Citizenship and visa processes require the transmission of foundational and biographical identity data across borders, while automated border-control systems must follow strict global standards for data collection, management, consent, and user control. • Synthetic identity exploitation: Partial or hybrid synthetic identities can be used to fraudulently obtain visas, work permits, or passports. • Security and criminal risks: These synthetic identities can enable banned individuals, criminals, or terrorists to cross borders and facilitate human trafficking, drug trafficking, and smuggling.
National Security 	• Growing identity-targeted threat landscape: As more sectors digitize, state and non-state actors increasingly seek the identity elements of foreign nationals, creating an online "warscape." • Synthetic identity–enabled infiltration: Reference-data injection and synthetic identities can give adversaries physical access to restricted areas or logical access to secure systems. • Severe national-security risks: These tactics enable espionage, sabotage, and terrorism by allowing bad actors to bypass traditional security controls.

This table is far from exhaustive, but the diversity of impacted sectors underscores the ubiquity of the collection, transmission, and storage of identity elements across our increasingly digitized world. The good news is that identity vendors and infrastructure organizations are working together to enshrine user privacy and data provenance, while investing in innova-

tive deepfake and synthetic identity detection. By building the prismatic vision of a converged digital/physical future together, each stakeholder is helping ensure our interactions retain an aura of human trust. **And the good news is that the Resilient Trust required for this new paradigm can be measured, evaluated, and assessed. For that, we will turn to a new tool: The Resilient Trust Maturity Ladder.**

The Prism Resilient Trust Maturity Ladder

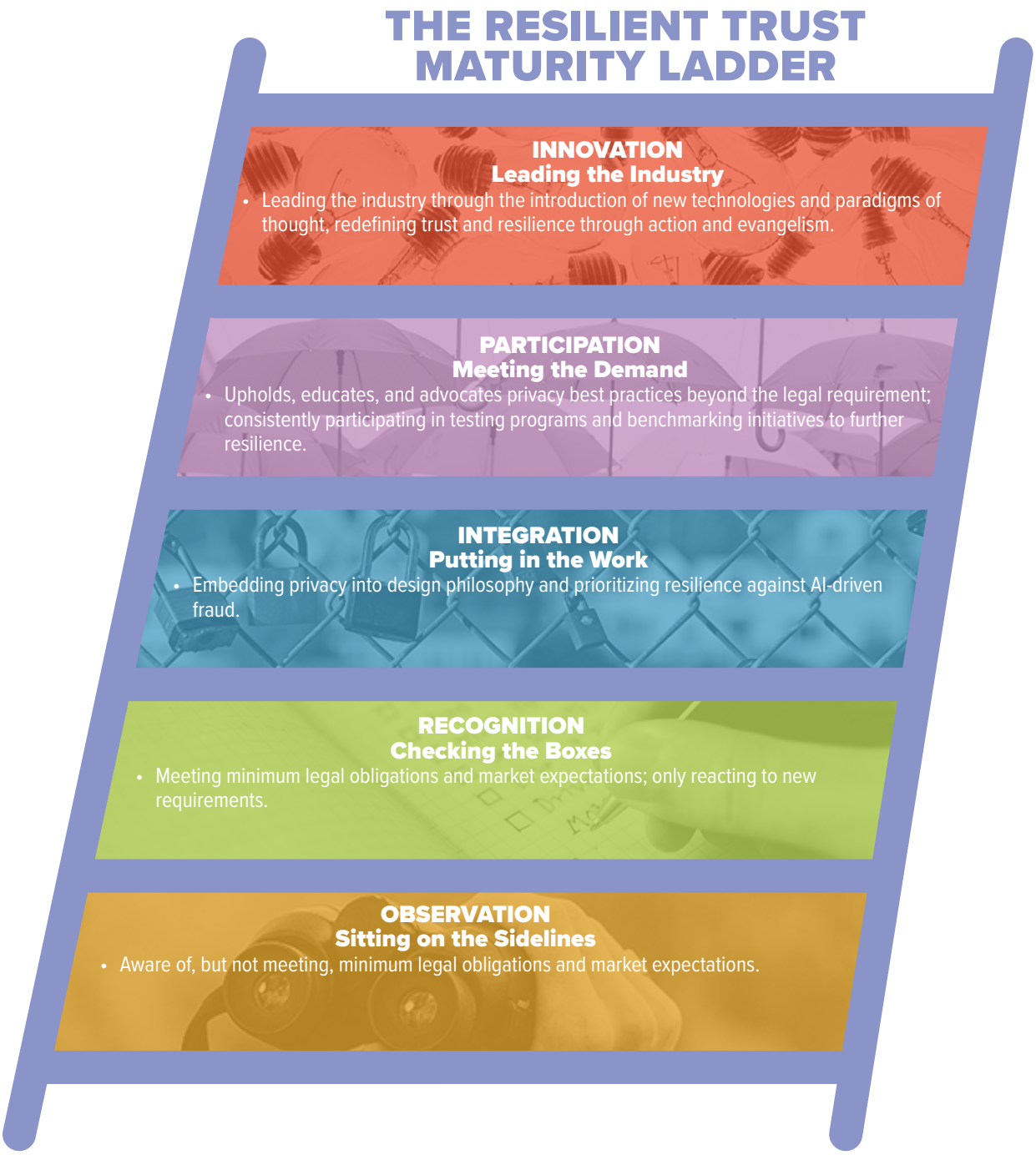
We have seen that the digital identity ecosystem is driven by two primary forces: fraud resilience, and privacy assurance and compliance (trust). Just as deepfakes and synthetic identity reshape the fraud landscape, privacy and compliance imperatives redefine how digital identity systems must be built, governed, and controlled. Together, they form essential infrastructure for digital trust, defining the new Resilient Trust paradigm: embed AI-driven fraud detection and privacy into the very fabric of digital identity ecosystems.

The Resilient Trust Maturity Ladder

The Prism introduces the Resilient Trust Maturity Ladder (see below), mapping organizational Resilient Trust postures along five ascending levels: Observation, Recognition, Integration, Participation, and Innovation.

This model helps public and private sector enterprises in two specific ways.

- The first—to assess their own trust and resilience maturity and chart a path toward resilient trust leadership.
- The second—as a tool to evaluate digital identity technology and solution providers and their offerings as enablers of Resilient Trust.



Cross-Sector Impacts

The Resilient Trust Maturity Ladder provides a means to evaluate technology and solution approaches to the identity threats and vulnerabilities facing every vertical market. In our current era of rapid digital transformation and AI-powered fraud, only the organizations reaching for the top rung of the ladder are fit for the high-stakes tasks of protecting privacy and defending identi-

ty, both online and in the physical world.

As we saw in the Trust and Fraud Resilience Vulnerabilities by Vertical Market section, resilience and trust pressure every vertical market — though the context varies with sector-specific dynamics shaping adoption:

- **Financial Services** – AML/KYC obligations intersect with consent and secure PII storage. Banks are moving toward privacy-preserving identity verification to balance fraud prevention with regulatory scrutiny and customer trust.
- **Travel & Hospitality** – Managing cross-border passenger data sharing while preserving seamless CX. Airlines, airports, and hotels are caught between global data-sharing requirements and customer consent for seamless journeys.
- **Government Services** – Foundational ID programs must balance efficiency and inclusion with civil liberties and citizen trust.
- **Healthcare** – Patient records, biometric health data, and insurance information are privacy-critical. Patient consent, secure storage of health biometrics, and regulatory alignment under HIPAA/GDPR-H are required. Compliance with HIPAA, GDPR-H, and local laws is non-negotiable.
- **Telecom** – Subscriber metadata, lawful intercept obligations, and location tracking sit at the core of privacy debates.
- **Retail & eCommerce** – Loyalty programs, personalization engines, and biometric checkout systems are redefining customer consent.
- **Education** – Student data and biometric proctoring tools spark debates about surveillance vs. integrity.
- **Workplace & Employment** – Biometric time clocks, employee monitoring, and remote work tools challenge labor rights and privacy. Ensuring ethical handling of employee biometrics in monitoring and timekeeping.
- **Sports & Entertainment Venues** – Deploying biometrics for ticketing and access must balance convenience with explicit, transparent consent.
- **Transportation & Mobility** – Balancing regulatory compliance, rider privacy, and biometric driver verification.

Resilient Trust as a Strategic Differentiator

The Trust and Resilience Maturity Ladder emphasizes that basic

fraud prevention and compliance are the floor, not the ceiling, for creating a secure biometric-centric digital identity ecosystem. They are the core pillars of an approach to Resilient Trust that bolsters, not constrains, innovation, providing a roadmap for organizations seeking to achieve or sustain market leadership.

A clear, forward-looking vision that champions Resilient Trust as a competitive strategy and key differentiator includes:

- Embedding resilient trust into product development and customer experience.
- Using certifications, transparency, dashboards, and privacy-first architecture as competitive resilient trust signals. This is true for vendors providing technology and solutions, as well as for relying parties deploying them.
- Positioning resilience and trust as differentiators that create loyalty and accelerate adoption.

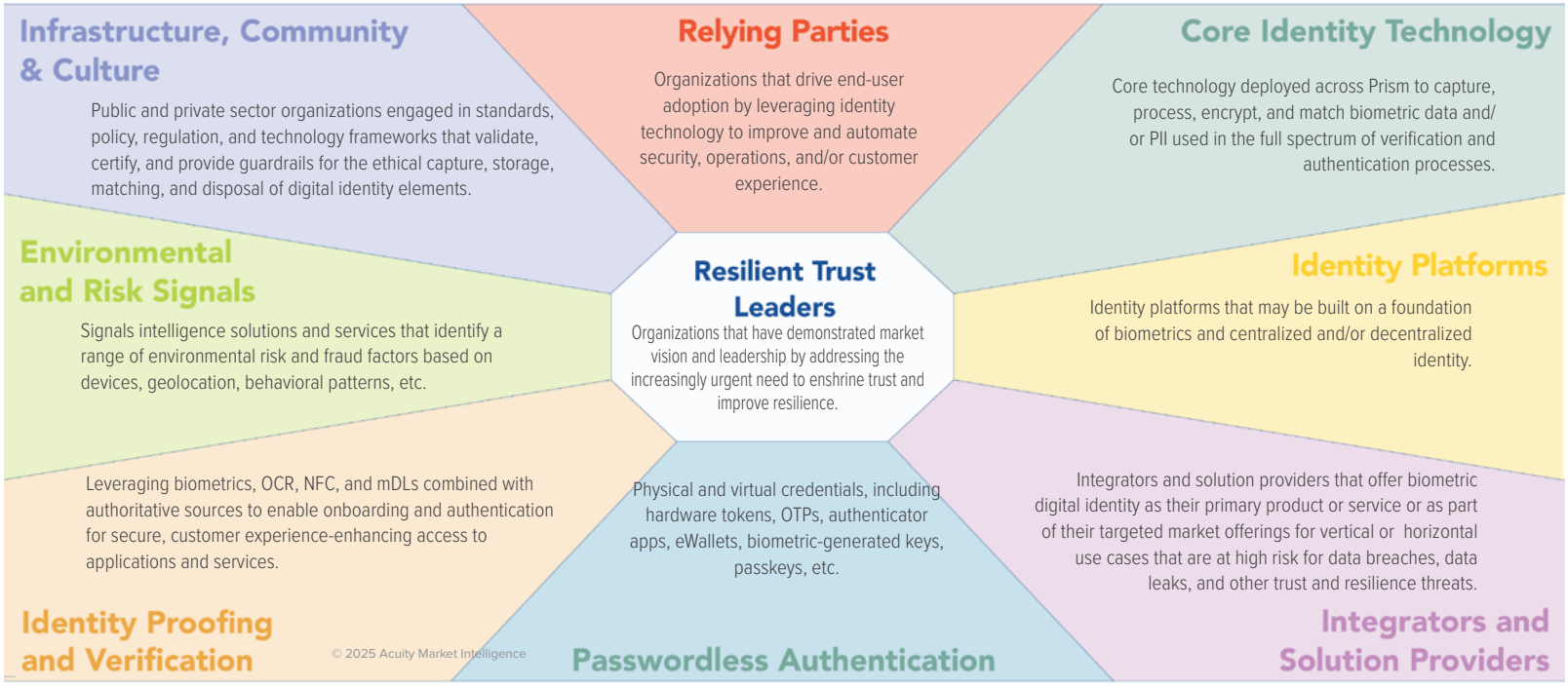
As digital transformation continues to accelerate at the pace of AI innovation, organizations that elevate resilient trust from obligation to critical strategy will thrive. Those who relegate it to the cost of doing business will fall behind.

To shift from obligation to strategy, requires integrating digital identity technologies and solutions designed to meet the challenges of Resilient Trust. And so we turn to the 2025 Biometric Digital Identity Flagship Prism.

The Biometric Digital Identity Prism

Just as a beam of light contains all colors, the biometric digital identity ecosystem is comprised of many organizations contributing to the grand idea of digital identity. The Prism Project conceptualizes this relationship through the Prism: a proprietary market landscape model intended to help reflect the components of the emerging reality of identity in a digitized world.

2025 Biometric Digital Identity Flagship Prism



Organizations are positioned in one of nine Prism Beams. Each beam representing a critical component of the biometric digital identity landscape. For some organizations, it can be challenging to select one beam that represents their singular position in the marketplace. Many appear to span multiple beams. In these cases, we have chosen the beam that most accurately reflects the breadth and depth of their product and service offerings and is most closely aligned with their unique differentiators. Organizations with profiles will see their penetration across multiple beams represented in our Luminosity Graphs (see more below).

How to Read the Prism

Within each beam, there are three evaluation categories: Pulsars, Catalysts, and Luminaries.

Pulsar

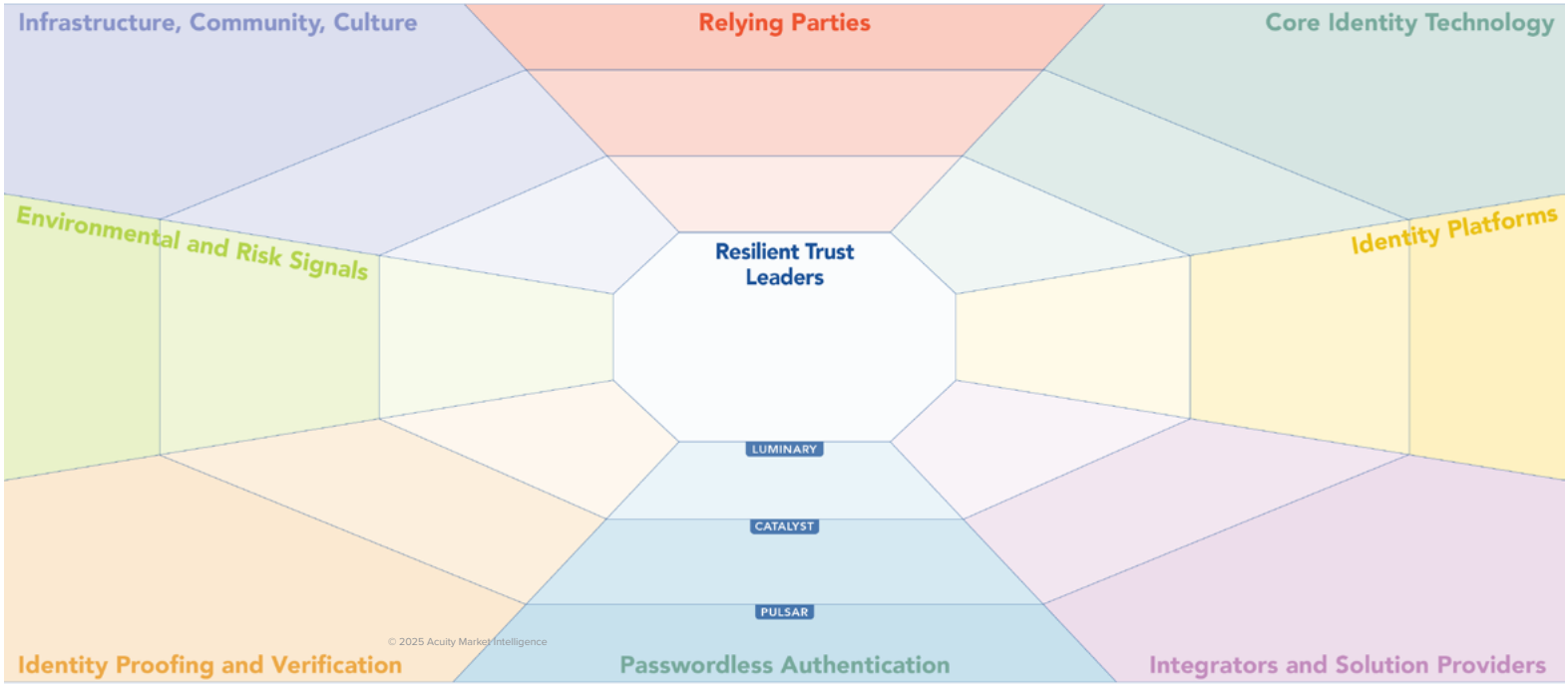
Pulsars are the bright upstarts and pivoting legacy vendors prioritizing the crucial elements of biometric digital identity. Startups with promising technology or established names with a proven aptitude for adapting to the new identity ecosystem, Pulsars have strong potential to influence the Prism landscape.

Catalyst

Catalysts are established disruptors, innovators, and agents of acceleration. With high proficiency in certain areas of assessment, Catalysts are often one step away from ascending to Luminary status, whether through an acquisition, a technological innovation, or an injection of resources.

Luminary

Luminaries are the guiding lights of their industry segment. They show the highest level of proficiency in their beam and are often responsible for setting trends in their fields.

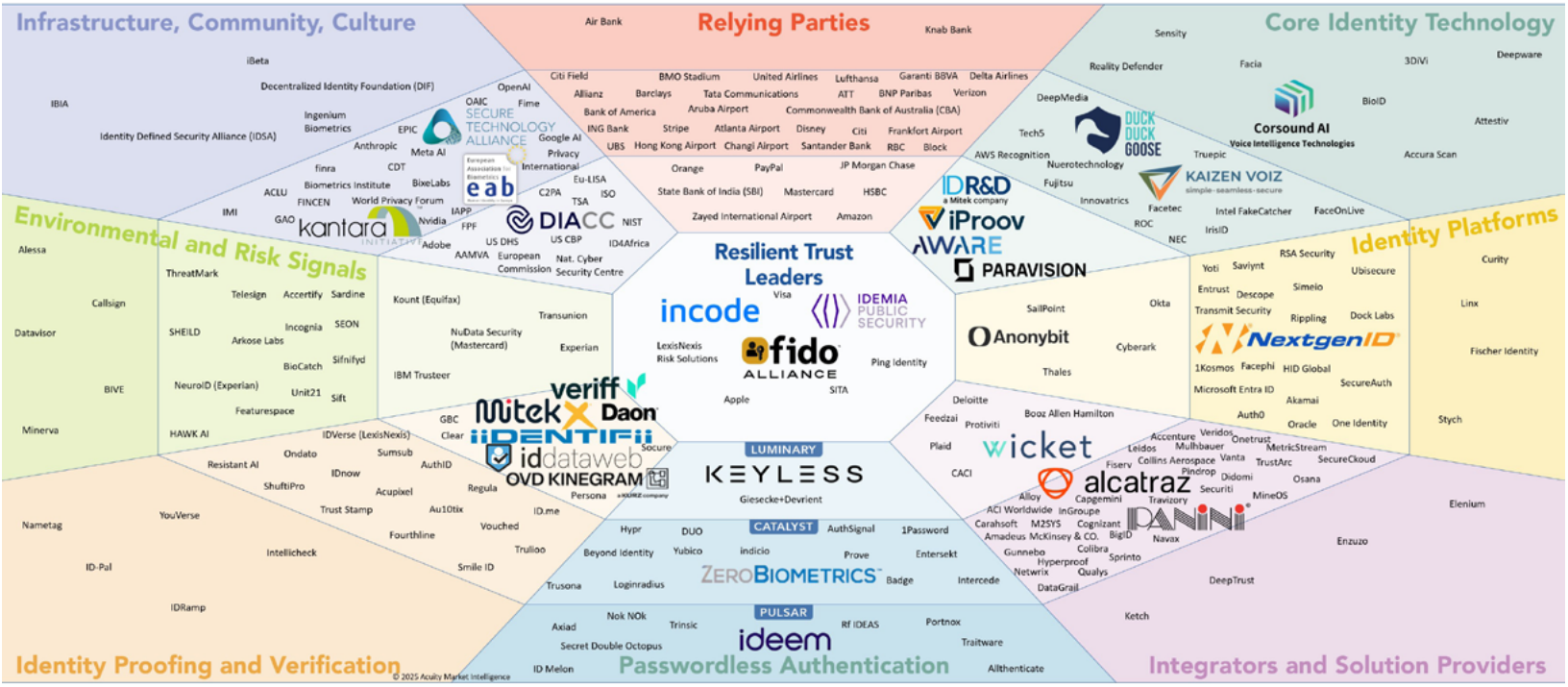


Refractors and Leaders

A special category anchors the center of the Prism—Refractors. In previous Prism reports, Refractor status was based on an organization's proven expertise, market impact, vision and leadership, technological or solutions innovation, or other x-factor impact. These attributes gave them outsized influence on the dynamics and evolution of the biometric digital identity market landscape. This role was defined as a Refractor, as it is through their initiatives that the industry is viewed.

For the 2025 Flagship Prism, this definition has shifted somewhat. The Refractor role has been assigned to the highest scoring Luminary in each of the eight Prism Beams—distinguishing them as Resilient Trust Leaders.

The 2025 Biometric Digital Identity Flagship Prism Ecosystem



Important Note on Prism Beams:

The Prism Beams and the classifications within represent important components of the emerging biometric digital identity landscape as it contends with the demands of Resilient Trust, and group organizations by the role they play therein. It is modality agnostic. Because of the broad nature of Prism Beams, many companies in the same areas are not direct competitors but represent the leading providers of their given solutions.

Evaluations & Profiles

In order to place organizations on the Biometric Digital Identity Prism, we assess the leading companies in each Prism Beam based on a proprietary evaluation scheme that includes six broad criteria.

- **Growth & Resources** – Current revenue, year-on-year growth, financial stability, and resources available to sustain and support ongoing growth.
- **Market Presence** – Overall geographic footprint and market sector penetration, as well as specific geographic regions and markets where a level of dominance has been achieved.
- **Proof Points** – Profile and size of the overall and market-sector customer base, and key customers. Also includes 3rd-party testing results, certifications, and implementation speed..
- **Unique Positioning** – Unique Value Proposition (UVP) along with differentiable technology and market innovation generally, and within their market sector.
- **Business Model & Strategy** – Overall marketing and sales positioning, messaging, and strategy, as well as channel scope and quality, and range of partnerships, thought leadership, market presence and engagement generally, and within select market sectors.
- **Biometrics and Document Authentication Capabilities**– Depending on the market, solutions(s), specific beam, may be rated higher as proprietary or integrated technology.
- **Resilient Trust Leadership** – Demonstrated vision, action, and commitment to thought leadership concerning the urgent matter of enshrining trust and bolstering resilience.

For the Infrastructure Beam, because of the special, critical-market-supporting nature of these organizations, we replace Proof Points with Impact and Influence, and replace Biometric and Document Authentication Capabilities with Commitment to Biometrics.

- **Impact and Influence—**Effectiveness of an organization's ability to guide standards, regulations, policy, and industry best practices through its initiatives and thought leadership.
- **Commitment to Biometrics—**Evidence of long-term financial and cultural investment in biometrics as a core identity technology, not only within a product portfolio, but conceptually at an industry level.

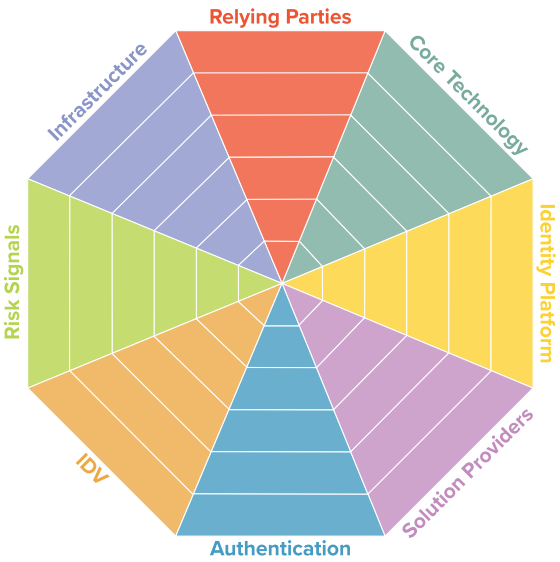
We visualize this assessment as a Prism Evaluation Chart: an easy-to read graphic representation of an organization's current activity, resources, and abilities.

In 2025, the Prism Project introduced a granular evaluation system represented by number grades on a scale of 0-6.

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Deepfakes & Synthetic Identity Leadership	Total	Average
VENDOR LOGO	5.50	5.33	5.17	5.50	5.33	3.00	6.00	35.83	5.12

Luminosity Graphs

New for 2025, Prism organization profiles include a Luminosity Graph—an illustration of the organization's penetration across all Prism Beams. The number of colored segments represents the proportional presence the organization has in the given segment of the overall biometric digital identity ecosystem (ie. the more teal colored segments an organization has, the more proof points it has in the Core Identity Technology Beam).



For reasons of spatial economy, we have abbreviated some of the corresponding beam titles as follows:

- Relying Parties = Relying Parties
- Core Identity Technology = Core Technology
- Identity Platforms = Identity Platforms
- Integrators & Solution Providers = Solution Providers
- Passwordless Authentication = Authentication
- Identity Proofing & Verification = IDV
- Environmental Risk Signals = Risk Signals
- Infrastructure, Community, Culture = Infrastructure

Important Note on Evaluations and Prism Placement:

The evaluation metrics in this report are based on publicly available data, survey data, interviews, and confidential briefings. It is presented in good faith as a representation of the biometric digital identity ecosystem, in accordance with the values stated previously in this report. If you see your company here and have questions about your evaluation or placement within the Prism, please contact: info@the-prism-project.com.

Resilient Trust Leaders

Organizations that have demonstrated market vision and leadership by addressing the increasingly urgent need to enshrine trust and improve resilience. The Refractor role has been assigned to the highest scoring Luminary in each of the eight Prism Beams (indicated in parentheses)—distinguishing them as Resilient Trust Leaders.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Apple (Passwordless Authenticators)	5.67	5.83	5.17	5.83	5.67	4.67	5.58	38.42	5.49	Refractor
IDEMIA PUBLIC SECURITY (Core Identity Technology)	5.33	5.67	5.33	4.00	5.17	5.67	5.25	36.42	5.20	Refractor
incode (Identity Proofing & Verification)	5.17	4.00	5.67	5.17	5.67	5.67	5.83	37.17	5.31	Refractor
LexisNexis Risk Solutions (Environmental Risk Signals)	5.33	5.50	5.33	5.17	5.67	5.00	5.67	37.67	5.38	Refractor
Ping Identity (Identity Platforms)	5.00	5.50	5.50	5.00	5.83	5.00	5.83	37.67	5.38	Refractor
SITA (Integrators & Solution Providers)	5.50	5.83	5.33	5.17	5.50	5.50	5.92	38.75	5.54	Refractor
Visa (Relying Parties)	5.83	6.00	5.33	5.50	5.50	4.67	4.75	37.58	5.37	Refractor

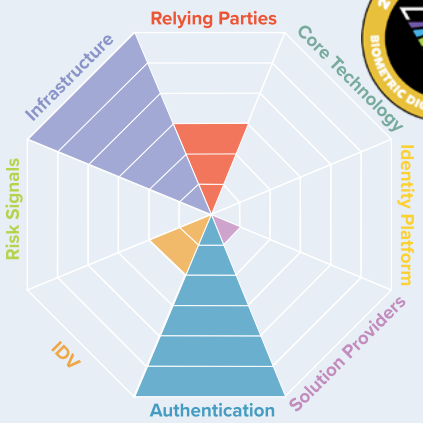
	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
fido ALLIANCE (Infrastructure, Community, Culture)	5.75	5.50	5.83	5.67	5.50	5.83	6.00	40.08	5.73	Refractor

fidoalliance.org

BEAM: **Resilient Trust Leaders** CLASSIFICATION: **Refractor**

(Infrastructure, Community, Culture Luminary)

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average
5.75	5.50	5.83	5.67	5.50	5.83	6.00	40.08	5.73



The FIDO Alliance is one of the most transformative forces in global digital identity, driving the shift from vulnerable, password-based systems to phishing-resistant, privacy-preserving authentication standards that now anchor the modern trust ecosystem. Founded in 2013 and headquartered in the United States, FIDO has grown into the world's leading authority on passwordless authentication, shaping adoption across enterprise security, consumer technology, financial services, public-sector programs, and digital government services. Remarkably, the Alliance anticipated the mobile-biometrics revolution even before Apple launched Touch ID—turning that early insight into a global standard now deployed by major technology platforms, public agencies, and enterprises worldwide. By advancing a mobile-first, public-key-based authentication paradigm, FIDO has established the benchmark for strong, privacy-centric digital identity assurance.

No More Secrets

FIDO advances trust—the foundation of the biometric digital identity ecosystem—by eliminating shared secrets and minimizing exposure of sensitive identity elements. Its flagship innovation, passkeys, enables users to authenticate using device-bound, cryptographically protected credentials stored in secure hardware elements. Under this model, biometrics and cryptographic keys never leave the user's device, never transit the network, and are never stored by relying parties. This aligns directly with the Prism's privacy-first principles: data minimization, user control, and the elimination of centralized identity repositories. FIDO reinforces this trust through rigorous certification programs, including its Biometric Component Certification and Face Verification Certification, which validate accuracy, fairness, demographic performance, and liveness detection. These programs ensure that the biometric systems powering passkey flows remain privacy-protecting and technically resilient—establishing a global floor for responsible biometric use. By promoting universal, interoperable authentication standards that keep identity elements secure even from relying parties, FIDO provides a structural foundation for regulatory compliance, global privacy protection, and user empowerment.

Killing the Password in the Name of Resilience

FIDO's ecosystem strengthens resilience—the anti-fraud backbone of digital identity—by removing the most commonly exploited attack vector in modern cybersecurity: the password. With more than two-thirds of hacking-related breaches originating from stolen or compromised credentials, password-based authentication has become a systemic liability, especially in a world of AI-accelerated phishing, deepfake-assisted social engineering, and automated synthetic-identity campaigns. Passkeys counter these threats by being inherently phishing-resistant and non-replayable: no static credentials exist to steal, no secrets can be intercepted, and authentication cannot be coerced or redirected. FIDO's 2025 Passkey Pledge, signed by major technology companies, universities, public agencies, and multiple Prism Luminaries, represents a coordinated global effort to accelerate adoption of these fraud-resistant authentication methods. The Alliance's biometric certification initiatives further enhance resilience by ensuring that biometric factors used within passkey flows remain resistant to AI-driven manipulation, presentation attacks, and deepfake impersonation. In doing so, FIDO provides not only a path away from passwords but a comprehensive upgrade to the resilience of the global authentication fabric.

A Safer Digital Future

Together, FIDO's standards, certification programs, and global leadership are driving a future in which secure authentication is both stronger and simpler—protecting users, institutions, and digital ecosystems without introducing friction. By uniting privacy preservation and anti-fraud capability under a single, transformative philosophy—eliminate passwords—FIDO is enabling the next generation of seamless, secure digital interactions. Its unwavering commitment to interoperable, phishing-resistant authentication is laying the groundwork for a digital world in which identity is both private and protected by design, ensuring trust and resilience remain at the center of global digital transformation.

For a complete list of FIDO Alliance members, visit https://fidoalliance.org/members/

Contact FIDO Alliance: fidoalliance.org/contact

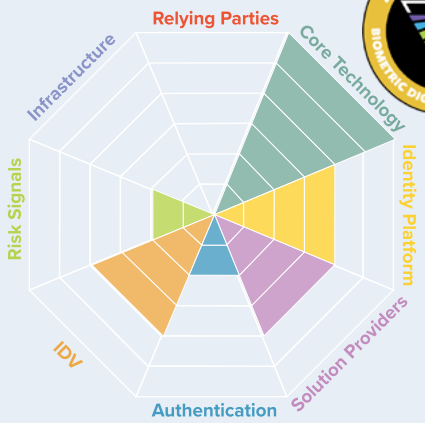
IDEMIA PUBLIC SECURITY

idemia.com

BEAM: **Resilient Trust Leaders** CLASSIFICATION: **Refractor**

(Core Identity Technology Luminary)

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
5.33	5.67	5.33	4.00	5.17	5.67	5.25	36.42	5.20



IDEMIA Public Security is the highest-ranked provider on the Core Identity Technology Beam, serving as the identity backbone for governments, border agencies, and national registries across more than 180 countries. As a Resilient Trust Leader, IDEMIA delivers the core biometric engines, secure credentials, AFIS/ABIS platforms, and mobile ID infrastructure that power enrollment, verification, and identity assurance at national scale. Its systems anchor foundational identity processes—national identity issuance, border management, law enforcement, election integrity, and digital credentialing—where trust and resilience are mission-critical.

IDEMIA's trust through privacy-by-design architecture includes non-reversible biometric templates, strict lifecycle controls, and compliance with GDPR, eIDAS, and national privacy frameworks. Its mobile and digital IDs follow global standards (ISO 18013-5, ICAO, EU digital identity wallets), producing privacy-aligned physical and logical credentials at national scale. These controls ensure that identity elements remain protected, auditable, and interoperable across borders and agencies. Meanwhile, IDEMIA's technology stack is engineered for resilience with multimodal biometric algorithms designed to defeat deepfakes, morphing, and synthetic-identity attacks. Its models analyze micro-movement signatures, texture and depth consistency, environmental cues, and temporal image structure to identify AI-generated overlays, injected imagery, and presentation attacks across every public-security workflow. IDEMIA delivers both operational resilience and population-scale accuracy. Its unmatched global footprint, data diversity, and decades of public-sector trust position IDEMIA as a key player shaping global identity infrastructure, security standards, and the next evolution of Resilient Trust.

Contact IDEMIA: idemia.com/contact-us/

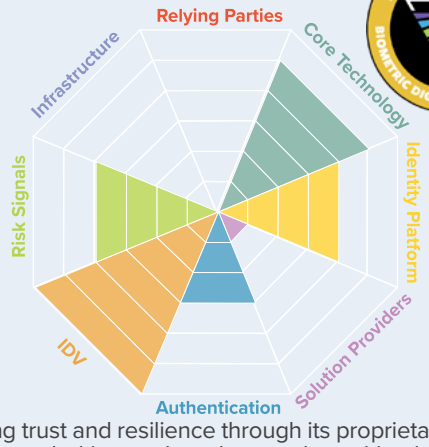
incode

incode.com

BEAM: **Resilient Trust Leaders** CLASSIFICATION: **Refractor**

(Identity Proofing & Verification Luminary)

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
5.17	4.00	5.67	5.17	5.67	5.67	5.83	37.17	5.31



Incode has emerged as a technically advanced and strategically ambitious identity platform, delivering trust and resilience through its proprietary, vertically integrated, AI-driven verification stack. With its recent acquisition of AuthenticID, Incode has expanded its reach and strengthened its document authentication, orchestration, and fraud-prevention capabilities across the U.S. financial services and telecommunications sectors.

Incode reports having performed more than 4 billion identity checks, processed over 400 million profiles, and prevented $40 billion in fraud and 30 million identity thefts across financial services, hospitality, social media, e-commerce, and the public sector—figures likely understated following the AuthenticID integration. The company's technology underpins high-stakes customer, employee, and business identity verification use cases, including linking AI agents to their human counterparts.

Incode distinguishes itself as a Resilient Trust Leader through its three-pillar strategy, built on:

- Proprietary, fully automated, vertically integrated AI—enabling rapid iteration, edge-case resolution, and agile anti-fraud adaptation.
- Access to billions of data points from high-fraud regions used to train its models, including integrations with government "sources of truth." Incode maintains direct DMV facial-biometric verification in multiple U.S. states and globally connects to biometric identity registries in Mexico, Brazil, Argentina, India, Australia, and others.
- Privacy-preserving fraud intelligence — its Trust Graph enables cross-institution fraud-signal sharing without exposing personal data, providing network-level defense while remaining privacy-aligned and regulator-friendly.

This FedRAMP-Ready Prism Refractor occupies a central position in the identity ecosystem, exemplifying what trusted, resilient, top-tier identity assurance looks like in an era of deepfakes, synthetic fraud, and AI-native digital interactions.

Contact Incode: contact@incode.com

Relying Parties

Organizations that drive end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Air Bank	2.17	1.83	2.67	2.67	2.67	3.67	4.33	20.00	2.86	Pulsar
Allianz	5.00	5.00	4.33	4.33	3.83	2.33	4.00	28.83	4.12	Catalyst
Amazon	5.83	5.50	5.17	5.67	6.00	5.00	3.92	37.08	5.30	Luminary
Aruba Airport	4.50	3.33	4.67	4.67	5.50	4.50	4.08	31.25	4.46	Catalyst
Atlanta Airport	5.00	5.50	5.50	5.50	5.17	3.33	2.50	32.50	4.64	Catalyst
ATT	5.00	5.17	4.17	4.50	3.83	3.00	3.92	29.58	4.23	Catalyst
Bank of America	5.83	5.67	4.50	5.50	4.67	1.83	3.33	31.33	4.48	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Barclays	4.83	5.17	4.17	4.50	4.67	2.17	3.67	29.17	4.17	Catalyst
Block	5.50	5.17	5.67	5.83	4.50	3.67	4.58	34.92	4.99	Catalyst
BMO Stadium	4.33	4.17	4.00	3.50	3.67	2.33	1.67	23.67	3.38	Catalyst
BNP Paribas	5.33	5.67	4.17	4.50	3.83	2.50	3.83	29.83	4.26	Catalyst
Changi Airport	4.67	5.00	5.33	5.50	5.50	5.17	3.42	34.58	4.94	Catalyst
Citi	5.83	5.83	4.50	5.17	4.67	3.00	4.00	33.00	4.71	Catalyst
Citi Field	4.33	4.17	4.00	3.50	3.67	2.33	1.67	23.67	3.38	Catalyst
CBA	4.83	4.83	4.17	4.50	3.83	4.50	5.17	31.83	4.55	Catalyst
Delta Airlines	4.00	4.50	3.67	4.67	5.00	2.67	3.42	27.92	3.99	Catalyst
Frankfurt Airport	4.83	5.33	5.17	5.33	5.17	3.83	3.58	33.25	4.75	Catalyst
Garanti BBVA	3.50	3.67	2.33	5.50	2.67	4.17	4.50	26.33	3.76	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Hong Kong Airport	5.00	5.83	5.33	5.50	6.00	4.33	2.50	34.50	4.93	Catalyst
HSBC	5.83	6.00	4.67	5.17	4.67	4.67	4.75	35.75	5.11	Luminary
ING Bank	4.83	5.00	4.17	4.50	3.83	5.00	4.92	32.25	4.61	Catalyst
JP Morgan Chase (Chase)	5.83	5.83	4.67	5.17	5.67	3.17	5.00	35.33	5.05	Luminary
Knab Bank	2.17	2.00	2.50	2.67	2.67	3.50	4.50	20.00	2.86	Pulsar
Lufthansa	4.00	4.67	3.83	4.00	3.83	2.17	3.50	26.00	3.71	Catalyst
Mastercard	5.83	6.00	4.83	5.50	5.83	3.00	4.67	35.67	5.10	Luminary
Orange	5.33	5.00	5.17	4.83	4.83	5.33	4.75	35.25	5.04	Luminary
PayPal	5.67	5.50	5.17	5.50	5.00	4.00	4.42	35.25	5.04	Luminary
Royal Bank of Canada	4.83	5.00	4.67	4.83	4.67	5.50	5.42	34.92	4.99	Catalyst
Santander Bank	5.33	5.00	5.00	5.50	4.67	3.67	5.50	34.67	4.95	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
State Bank of India (SBI)	5.17	5.50	4.83	5.00	4.83	5.17	4.83	35.33	5.05	Luminary
Stripe	4.17	4.50	4.67	4.33	4.83	5.00	4.83	32.33	4.62	Catalyst
Tata Communications	4.50	4.83	4.17	4.67	3.00	3.83	4.50	29.50	4.21	Catalyst
UBS	4.83	4.83	4.17	4.50	4.67	6.00	5.50	34.50	4.93	Catalyst
United Airlines	4.67	4.67	3.33	4.00	3.83	2.17	3.00	25.67	3.67	Catalyst
Verizon	5.00	5.00	4.00	4.67	4.00	3.67	4.50	30.83	4.40	Catalyst
Disney	5.50	5.83	4.17	5.33	5.50	2.67	3.83	32.83	4.69	Catalyst
Zayed international Airport	5.17	5.33	5.83	5.50	6.00	4.67	3.83	36.33	5.19	Luminary

Core Identity Technology

Core technology deployed across Prism to capture, process, encrypt, and match biometric data and/or PII used in the full spectrum of verification and authentication processes.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
3DiVi	1.33	1.33	2.17	1.17	1.33	2.83	2.92	13.08	1.87	Pulsar
Accura Scan	1.67	2.67	3.33	2.17	2.33	4.17	4.25	20.58	2.94	Pulsar
Attestiv	1.67	1.17	2.33	3.00	2.50	0.67	4.50	15.83	2.26	Pulsar
AWARE	3.83	4.17	5.00	5.33	5.33	6.00	5.92	35.58	5.08	Luminary
AWS Rekognition	5.00	4.83	5.00	4.50	4.83	4.83	4.17	33.17	4.74	Catalyst
BioID	1.50	2.67	2.50	1.83	3.33	4.50	4.17	20.50	2.93	Pulsar
Corsound AI (Voice Intelligence Technologies)	1.67	1.17	3.33	4.50	2.67	3.00	4.42	20.75	2.96	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
DeepMedia	2.50	2.50	3.33	3.17	2.17	2.67	4.92	21.25	3.04	Catalyst
Deepware	1.17	1.00	1.67	2.00	1.50	0.33	4.00	11.67	1.67	Pulsar
DUCK DUCK GOOSE	2.17	1.67	3.83	4.50	4.17	3.83	5.33	25.50	3.64	Catalyst
FaceOnLive	1.67	1.83	3.33	2.67	3.33	4.83	4.33	22.00	3.14	Catalyst
Facetec	4.67	3.83	4.83	3.67	4.50	5.50	5.92	32.92	4.70	Catalyst
Facia	1.83	1.67	3.83	2.83	2.33	3.67	3.92	20.08	2.87	Pulsar
Fujitsu	5.17	4.83	5.50	4.17	5.00	4.50	4.08	33.25	4.75	Catalyst
IDR&D a Mitek company	5.00	4.50	5.50	4.50	4.67	5.67	5.50	35.33	5.05	Luminary
Innovatrics	3.50	4.50	5.50	4.17	4.50	5.67	5.50	33.33	4.76	Catalyst
Intel FakeCatcher	5.00	3.00	4.17	4.00	3.00	2.17	4.92	26.25	3.75	Catalyst
iProov	4.50	4.17	5.00	5.67	5.33	4.67	6.00	35.33	5.05	Luminary

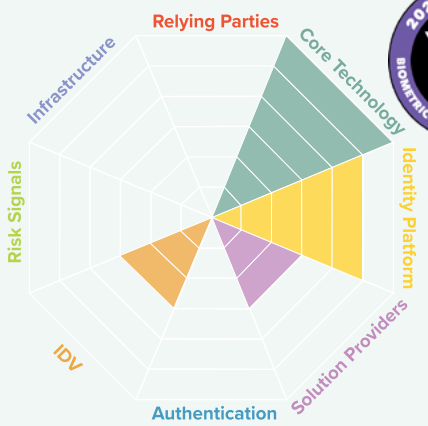
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
IrisID	4.50	3.83	5.17	4.50	4.83	5.67	4.50	33.00	4.71	Catalyst
KAIZEN VOIZ (simple·seamless·secure)	2.33	2.83	4.33	4.83	3.00	3.17	5.25	25.75	3.68	Catalyst
NEC	4.67	5.00	5.67	4.33	5.17	6.00	3.75	34.58	4.94	Catalyst
Neurotechnology	3.00	3.67	4.17	4.33	4.50	5.83	2.33	27.83	3.98	Catalyst
PARAVISION	3.83	4.33	5.33	5.50	5.33	4.83	5.92	35.08	5.01	Luminary
Reality Defender	2.50	1.67	3.50	3.00	2.83	2.83	4.25	20.58	2.94	Pulsar
ROC	4.17	3.67	5.17	5.67	4.67	5.50	5.50	34.33	4.90	Catalyst
sensity	1.17	1.83	2.67	2.83	1.67	2.67	4.08	16.92	2.42	Pulsar
Tech5	3.00	3.33	5.17	3.50	4.33	4.00	3.83	27.17	3.88	Catalyst
truepic	2.33	2.67	3.67	4.17	3.33	0.67	4.50	21.33	3.05	Catalyst

AWARE

aware.com

BEAM: **Core Identity Technology** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
3.83	4.17	5.00	5.33	5.33	6.00	5.92	35.58	5.08



Aware is one of the most enduring forces in biometric innovation, bringing nearly four decades of science-driven expertise to the modern identity ecosystem and redefining what secure, multimodal verification can achieve in an AI-threatened world. A U.S.-based pioneer with roots back to 1986—including foundational contributions to the FBI's first major fingerprint-digitization program—Aware has spent decades shaping the biometric digital identity landscape through science-forward innovation and a commitment to secure, privacy-preserving identity management. Today, its configurable Awareness Platform and extensive portfolio of biometric components support identity ecosystem trust through rigorous privacy protection and transparent data practices, while high-assurance biometric verification strengthens resilience at every layer of the identity hierarchy, across global deployments in digital finance, border security, travel and hospitality, government services, and enterprise workflows.

The Awareness Platform enhances privacy by design, leveraging end-to-end encryption, full data anonymization, a consent-forward architecture, and advanced image watermarking to help relying parties align with GDPR-inspired regulatory requirements without sacrificing performance. Aware also delivers powerful safeguards against modern AI-powered fraud—including passive and active liveness detection, deepfake and face-swap detection, and robust injection-attack prevention—to identify counterfeit elements and synthetic identities before they can compromise onboarding or authentication. These protections deliver measurable outcomes: one of Brazil's largest commercial banks achieved an 87% reduction in fraud in its first year using the Aware Intelligent Liveness and deepfake-detection models, significantly reducing scalable face-swap attacks during a period of explosive customer growth. With its unparalleled history, multimodal depth, technical maturity, and proven ability to expose the hardest-to-detect AI-driven threats, Aware occupies a uniquely authoritative position in the market as a guardian of both trust and resilience; a high-assurance bulwark against the accelerating fraud landscape.

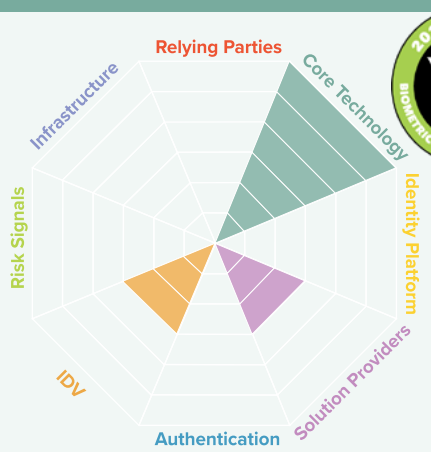
Contact Aware: sales@aware.com

KAIZEN VOIZ
simple·seamless·secure

kaizenvoiz.com

BEAM: **Core Identity Technology** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
2.33	2.83	4.33	4.83	3.00	3.17	5.25	25.75	3.68



Kaizen Voiz is redefining voice biometrics for a global, multichannel world with a lightweight, readerless authentication engine that delivers high-assurance identity verification without friction or specialized hardware. Built on a patented, ISO-certified biometric engine that analyzes more than 21 unique vocal-tract characteristics, the platform provides seamless authentication across telephony, mobile devices, automotive systems, and enterprise environments. Its language-agnostic, device-agnostic architecture enables passive, continuous, and cross-channel verification—extending strong authentication to contact centers, financial services, public-sector benefits, and emerging mobility use cases. By eliminating the need for dedicated sensors or enrollment equipment, Kaizen Voiz expands access to trustworthy biometric identity, reinforcing both trust and resilience across globally distributed user populations. This infrastructure-minimal approach positions Kaizen Voiz as a Core Identity Technology Catalyst in an increasingly AI-driven ecosystem.

Kaizen Voiz strengthens privacy and fraud defense through deepfake-aware signal analysis, passive anti-spoofing, and a biometric engine engineered to withstand synthesized speech, mimicry, and replay attacks. Its accuracy—validated against ISO/IEC 19795-1/2/3 and ISO/IEC 19794-13—ensures reliable authentication across accents, dialects, and varied acoustic conditions while reducing demographic bias and maintaining high assurance. These capabilities power secure customer and agent verification in contact centers, compliant MFA for sensitive financial operations, fraud-resistant password-reset flows, retiree verification for benefits distribution, and even driver authentication for autonomous-vehicle override scenarios. With a single-voice enrollment supporting multiple access modes—from IVR to mobile apps to ATMs—Kaizen Voiz delivers a globally agnostic, privacy-preserving, deepfake-resistant authentication layer built for the realities of modern digital identity, helping organizations strengthen identity assurance while keeping the user experience effortless.

Contact Kaizen Voiz: sales@kaizenvoiz.com

Identity Platforms

Identity platforms that may be built on a foundation of biometrics and centralized and/or decentralized identity.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
1Kosmos	5.00	4.67	5.33	3.83	4.50	5.67	5.50	34.50	4.93	Catalyst
Akamai	5.67	5.67	4.00	3.00	4.00	1.00	5.25	28.58	4.08	Catalyst
Anonybit	3.83	4.00	5.50	6.00	5.67	5.67	5.75	36.42	5.20	Luminary
AuthO	5.17	5.17	4.67	4.17	4.83	4.17	3.67	31.83	4.55	Catalyst
Curity	2.00	2.17	2.67	2.67	2.33	1.00	1.75	14.58	2.08	Pulsar
Cyberark	5.00	5.17	5.33	4.83	5.00	4.83	5.08	35.25	5.04	Luminary
Descope	4.33	3.33	5.17	3.83	4.17	4.00	4.83	29.67	4.24	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Dock Labs	2.00	2.17	3.17	3.33	4.00	3.67	4.50	22.83	3.26	Catalyst
Entrust	4.67	4.50	4.67	4.67	5.00	5.00	5.33	33.83	4.83	Catalyst
Facephi	4.50	3.83	4.50	3.67	4.17	5.83	5.17	31.67	4.52	Catalyst
Fischer Identity	2.00	1.67	1.83	2.17	2.33	1.50	2.25	13.75	1.96	Pulsar
HID Global	4.17	5.00	4.17	3.00	2.67	4.83	4.08	27.92	3.99	Catalyst
Linx	2.83	2.00	3.67	4.67	2.50	0.00	1.83	17.50	2.50	Pulsar
Microsoft Entra ID	5.50	5.17	5.00	5.00	5.50	4.00	4.50	34.67	4.95	Catalyst
NextgenID	3.00	4.33	4.67	5.33	4.33	5.33	4.33	31.33	4.48	Catalyst
Okta	5.33	4.67	4.67	5.17	5.67	5.00	4.67	35.17	5.02	Luminary
One Identity	4.00	3.50	4.17	3.33	4.67	1.50	3.42	24.58	3.51	Catalyst
Oracle	5.67	5.50	5.00	3.67	5.00	1.33	2.42	28.58	4.08	Catalyst

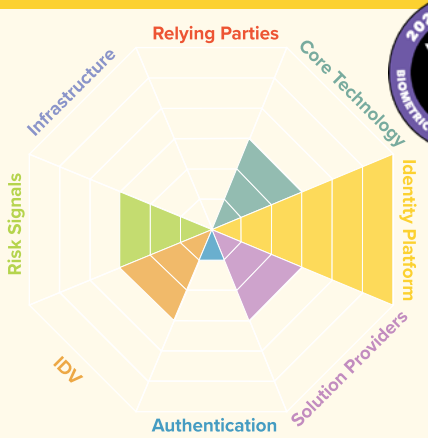
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Rippling	5.00	4.00	4.83	4.00	5.17	1.33	3.50	27.83	3.98	Catalyst
RSA Security	3.83	4.50	4.00	3.83	4.17	2.83	2.50	25.67	3.67	Catalyst
SailPoint	5.83	5.00	4.83	4.33	5.83	4.67	5.17	35.67	5.10	Luminary
Saviynt	4.33	3.83	4.50	3.17	3.67	4.33	4.83	28.67	4.10	Catalyst
SecureAuth	3.50	2.33	3.83	3.17	4.17	2.83	4.25	24.08	3.44	Catalyst
Simeio	5.00	5.00	4.00	3.00	4.00	2.00	3.92	26.92	3.85	Catalyst
Stych	2.83	2.33	3.83	2.83	2.83	1.83	2.42	18.92	2.70	Pulsar
Thales	4.83	5.50	4.83	4.17	5.00	5.33	5.83	35.50	5.07	Luminary
Transmit Security	4.67	4.33	5.00	5.00	4.17	5.50	5.42	34.08	4.87	Catalyst
Ubisecure	2.67	3.17	3.17	2.50	2.83	3.67	4.08	22.08	3.15	Catalyst
Yoti	4.83	4.33	4.83	4.83	4.83	4.33	5.67	33.67	4.81	Catalyst

Anonybit

anonybit.io

BEAM: **Core Identity Technology** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
3.83	4.00	5.50	6.00	5.67	5.67	5.75	36.42	5.20



Anonybit is redefining what privacy-first digital identity can achieve, proving that the strongest biometric security emerges when sensitive data never resides in a single place where it can be stolen, copied, or weaponized. An Identity Platform Prism Beam Luminary, Anonybit's patented privacy-preserving architecture dispenses trust and resilience by breaking biometric templates and identity elements into encrypted fragments and distributing them across a secure network—eliminating the catastrophic risks of centralized storage. Founded in 2018 and led by industry trailblazer Frances Zelazny, Anonybit has become one of the most influential forces in privacy-preserving identity, enabling high-assurance authentication without ever exposing raw biometrics. From financial services and hospitality to government and public-sector infrastructure, and emerging AI-driven ecosystems, Anonybit's Genie platform secures the full identity lifecycle—delivering fast, scalable biometric matching, anchored in cryptographic privacy guarantees that meet the highest global standards.

Anonybit protects privacy by ensuring that biometric templates are never stored, transmitted, or reconstructed in full. Instead, encrypted "Anonybits" remain permanently distributed across a multiparty cloud, removing the honeypot vulnerabilities that have plagued centralized systems for decades. This architecture enables extremely high-speed 1:1 authentication and 1:N deduplication—supporting up to 10 million searches in under a second—while keeping sensitive identity elements mathematically unrecoverable. At the same time, Anonybit strengthens organizational resilience against the most advanced forms of AI-powered fraud, including deepfake impersonation, synthetic-identity creation, and account takeover. Its deduplication and lifecycle-wide biometric assurance stop synthetic identities at onboarding and secure account recovery with non-replayable biometric verification. Real-world deployments demonstrate its impact: one Tier 1 Latin American bank reported a 99% reduction in fraud after adopting Anontbit's technology for large-scale deduplication to eliminate synthetic identities and account takeover fraud. By fusing privacy-preserving cryptography and distributed data storage with high-performance biometric fraud defenses, Anonybit stands out as a strategic innovator—proving that in the AI era, true resilience begins by protecting identity at its most foundational layer.

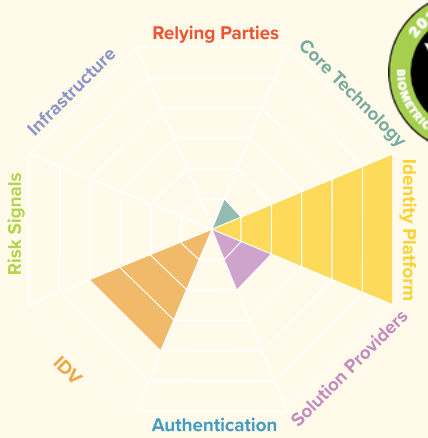
Contact Anonybit: info@anonybit.io

NextgenID

nextgenID.com

BEAM: **Core Identity Technology** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
3.00	4.33	4.67	5.33	4.33	5.33	4.33	31.33	4.48



NextgenID is redefining high-assurance identity enrollment with advanced, automation-driven technologies built to secure the most sensitive and regulated identity ecosystems in the world. Headquartered in the United States, the company specializes in supervised remote identity proofing, biometric enrollment, and compliant in-person identity capture—delivering solutions trusted across government, defense, public-sector services, and high-security commercial environments. Its Ultra-Secure Supervised Remote Identity Proofing (SRIP) platform enables organizations to meet the highest verification requirements (including NIST SP 800-63 AAL3 and IAL3) while dramatically reducing the logistical burden of traditional in-person enrollment. Through automated kiosks, multi-biometric capture systems, and secure workflow orchestration, NextgenID serves as a foundational enrollment specialist within the biometric digital identity ecosystem.

NextgenID strengthens both trust and resilience by combining multi-modal biometric capture—face, fingerprint, iris—with tamper-proof hardware, live supervision, and advanced liveness detection to counter deepfakes, synthetic identities, image injection, and impersonation. Its enrollment stations enforce strict chain-of-custody controls, ensuring that identity data is captured under secure, trusted, and fully auditable conditions. The company's supervised remote model drastically narrows attack surfaces by eliminating unsupervised document capture and reducing the opportunities for adversarial manipulation. Every credential issuance workflow is anchored in high-integrity identity data linked to authoritative documents and multifactor verification, enabling compliance with U.S. federal standards, global KYC/AML regulations, and emerging AI risk-mitigation frameworks. With its blend of ultra-secure enrollment, friction-reducing automation, and deep compliance alignment, NextgenID occupies a unique and increasingly indispensable position—bringing trusted, high-assurance identity to environments where accuracy, accountability, and resilience cannot be compromised.

Contact NextgenID: info@nextgenID.com

Integrators and Solution Providers

Integrators and solution providers that offer biometric digital identity as their primary product or service, or as part of their targeted market offerings for vertical or horizontal use cases that are at high risk for trust and resilience threats.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Accenture	5.17	5.50	4.67	4.00	5.00	4.67	4.92	33.92	4.85	Catalyst
ACI Worldwide	5.50	5.17	4.83	5.00	5.17	4.83	3.92	34.42	4.92	Catalyst
alcatraz	3.83	3.83	5.33	5.17	5.33	5.17	5.25	33.92	4.85	Catalyst
Alloy	4.33	4.83	4.83	5.00	5.50	5.33	4.67	34.50	4.93	Catalyst
Amadeus	4.83	5.50	4.83	4.50	5.50	4.50	4.25	33.92	4.85	Catalyst
BigID	4.00	5.00	4.00	3.00	5.00	1.00	4.00	26.00	3.71	Catalyst
Booz Allen Hamilton	5.17	5.00	4.83	4.83	5.67	5.17	4.92	35.58	5.08	Luminary

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
CACI	6.00	5.00	6.00	4.00	5.00	5.00	4.83	35.83	5.12	Luminary
Capgemini	5.33	4.00	4.50	4.17	5.00	4.50	4.92	32.42	4.63	Catalyst
Carahsoft	5.17	5.00	4.83	4.83	5.67	5.17	4.17	34.83	4.98	Catalyst
Cognizant	5.67	5.67	4.00	3.00	4.00	2.00	4.58	28.92	4.13	Catalyst
Collibra	4.00	5.00	4.00	3.00	5.00	1.00	4.00	26.00	3.71	Catalyst
Collins Aerospace	5.00	4.83	4.67	3.67	4.50	4.83	4.17	31.67	4.52	Catalyst
DataGrail	4.00	5.00	4.00	3.00	5.00	1.00	3.67	25.67	3.67	Catalyst
DeepTrust	2.17	1.83	3.83	3.50	2.33	3.00	4.25	20.92	2.99	Pulsar
Deloitte	5.50	6.00	5.50	5.50	5.83	5.50	4.50	38.33	5.48	Luminary
Didomi	4.00	5.00	4.00	3.00	5.00	1.00	3.83	25.83	3.69	Catalyst
Elenium Automation	2.33	2.17	3.50	2.67	2.17	3.83	3.83	20.50	2.93	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Enzuzo	2.67	3.33	3.83	2.83	4.17	1.00	3.00	20.83	2.98	Pulsar
Feedzai	5.17	6.00	6.00	6.00	6.00	5.00	4.42	38.58	5.51	Luminary
Fiserv	5.33	5.33	4.50	5.00	5.00	4.50	4.42	34.08	4.87	Catalyst
Gunnebo	4.67	4.50	4.50	3.67	4.83	3.83	3.58	29.58	4.23	Catalyst
Hyperproof	4.00	5.00	4.00	3.00	5.00	1.00	4.08	26.08	3.73	Catalyst
In Groupe	4.17	4.83	4.17	3.83	4.50	5.17	5.83	32.50	4.64	Catalyst
Ketch	3.50	4.00	3.67	2.50	4.33	0.50	2.42	20.92	2.99	Pulsar
Leidos	5.17	4.83	4.50	4.83	5.17	4.83	5.00	34.33	4.90	Catalyst
M2SYS	4.33	4.17	4.67	4.67	4.00	6.00	5.17	33.00	4.71	Catalyst
McKinesy & Company	5.67	5.67	4.00	3.00	4.00	2.00	4.58	28.92	4.13	Catalyst
MetricStream	4.00	5.00	4.00	3.00	5.00	1.00	3.83	25.83	3.69	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
MineOS	4.00	5.00	4.00	3.00	5.00	1.00	3.33	25.33	3.62	Catalyst
Mulhbauer	4.33	4.83	4.67	4.33	4.17	5.17	3.75	31.25	4.46	Catalyst
Navax	4.00	5.00	4.00	3.00	5.00	1.00	3.33	25.33	3.62	Catalyst
Netwrixx	4.33	5.00	4.00	3.00	5.00	1.00	4.08	26.42	3.77	Catalyst
Onetrust	4.00	5.67	4.00	3.00	5.00	1.00	3.83	26.50	3.79	Catalyst
Osana	3.50	5.00	4.00	3.00	5.00	1.00	3.67	25.17	3.60	Catalyst
PANINI	3.50	3.67	4.17	3.67	3.33	4.00	2.92	25.25	3.61	Catalyst
Pindrop	4.17	2.83	4.67	3.83	4.17	3.17	4.67	27.50	3.93	Catalyst
Plaid	4.83	5.00	5.17	5.00	5.50	5.33	5.58	36.42	5.20	Luminary
Protiviti	5.33	5.50	5.17	4.83	5.83	5.00	4.58	36.25	5.18	Luminary
Qualys	4.00	5.00	4.00	3.00	5.00	1.00	3.58	25.58	3.65	Catalyst

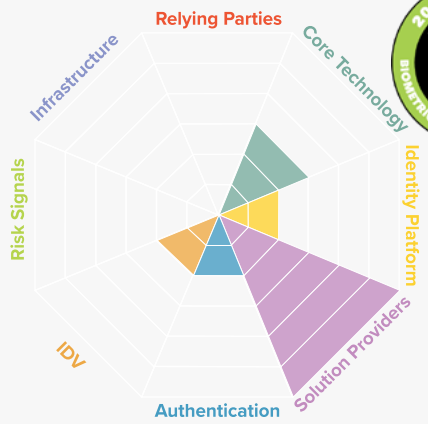
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Secure Cloud	2.83	5.00	4.00	3.00	5.00	1.00	3.58	24.42	3.49	Catalyst
Securiti	4.00	5.00	4.00	3.00	5.00	1.00	3.83	25.83	3.69	Catalyst
Sprinto	4.00	5.00	4.00	3.00	5.00	1.00	3.58	25.58	3.65	Catalyst
Travizory	2.83	3.17	4.67	4.33	3.83	5.50	4.25	28.58	4.08	Catalyst
TrustArc	4.00	5.00	4.00	3.00	5.00	1.00	3.83	25.83	3.69	Catalyst
Vanta	5.00	5.00	4.00	3.00	5.00	1.00	4.17	27.17	3.88	Catalyst
Veridos	4.67	4.17	4.33	4.00	4.17	4.67	4.75	30.75	4.39	Catalyst
wicket	4.67	5.00	5.50	5.50	6.00	4.33	4.42	35.42	5.06	Luminary

alcatraz

alcatraz.ai

BEAM: **Integrators & Solution Providers** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
3.83	3.83	5.33	5.17	5.33	5.17	5.25	33.92	4.85



Alcatraz is redefining the future of physical access security with AI-powered facial authentication that delivers frictionless entry without compromising privacy, accuracy, or control. A U.S.–based company serving Fortune 500 enterprises, data centers, critical infrastructure, and other high-security environments, Alcatraz anchors trust and resilience in the biometric digital identity ecosystem by offering a privacy-first alternative to conventional facial recognition, ensuring that all identity elements used for access are non-identifying, encrypted, and tightly governed. Its flagship solution, Rock, integrates directly into existing access control systems and uses AI-driven facial authentication tied exclusively to badge IDs—never to PII—offering consent-based, high-assurance entry with exceptional speed and industry-leading accuracy.

Alcatraz enhances privacy by converting facial scans into non-identifying templates linked solely with access permissions, ensuring compliance with stringent regulations such as GDPR, CCPA, and BIPA while avoiding the surveillance risks inherent in video analytics systems. Its multilayered defenses against AI-powered fraud include liveness detection to block deepfakes and presentation attacks, tailgating detection to prevent unauthorized piggybacking, and AI-based anomaly detection to flag suspicious or anomalous access patterns in real time. Real-world deployments—such as modernization of Scott Data's legacy system—demonstrate how Rock rapidly enrolls users, eliminates tailgating, and hardens physical perimeter security within minutes of installation. With centralized management, configurable consent workflows, and flexible, seamless cloud or on-prem deployment, Alcatraz is not merely upgrading physical access control—it is reshaping the boundary between digital trust and physical security with a future-ready, fraud-resistant platform built for a world that demands uncompromising safety.

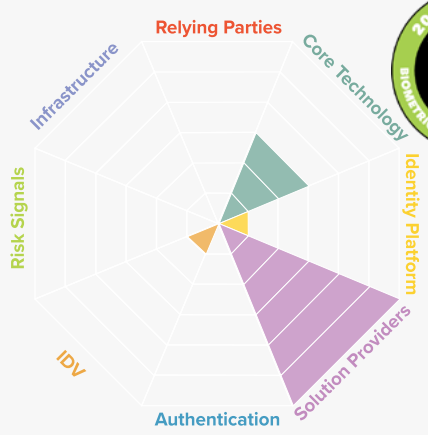
Contact Aclatraz: alcatraz.ai/contact

PANINI

panini.com

BEAM: **Integrators & Solution Providers** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
3.50	3.67	4.17	3.67	3.33	4.00	2.92	25.25	3.61



Panini brings decades of expertise from Italy's banking and financial infrastructure to the evolving landscape of modern digital identity. Renowned for serving highly regulated sectors with advanced document verification, biometric authentication, and in-branch identity solutions, Panini has earned deep trust across financial services, retail, and government markets. As digital transformation accelerates, Panini is expanding its portfolio to support high-assurance identity proofing and fraud prevention at scale. Its flagship innovations—including high-performance fingerprint verification and ergonomic, user-friendly document-authentication systems—help organizations comply with strict regulatory requirements, prevent identity misuse, and deliver seamless customer experiences rooted in privacy and security. In the biometric digital-identity ecosystem, Panini stands out as a bridge between physical and digital trust, bringing proven reliability to the front lines of modernization.

Panini bolsters trust and resilience by combining mature biometric science with fraud-resistant document-verification workflows designed to withstand today's AI-driven threat landscape. Its FBI Appendix F–certified fingerprint technology uses advanced image filtering and minutiae extraction to reduce false acceptance and false rejection rates, preventing attackers from exploiting poor-quality captures or presentation attacks. This capability is embedded in BioCred, Panini's universal in-branch identity platform that enables strong authentication, secure payments, and identity binding without exposing sensitive user data or relying on intrusive practices. Complementing biometrics, Panini's document-verification systems apply multi-light imaging, chip access, barcode validation, and machine-learning-based fraud detection to expose forged, altered, or synthetic identity artifacts—critical defenses against deepfakes and AI-generated documents. By combining ergonomic design, robust security, and regulatory alignment, Panini delivers the trusted and resilient infrastructure organizations need to modernize safely, maintaining strong identity assurance without sacrificing operational efficiency or user experience.

Contact Panini: panini.com/product-inquiry/

Passwordless Authenticators

Physical and virtual credentials, including hardware tokens, OTPs, authenticator apps, eWallets, biometric-generated keys, passkeys, etc.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
1Password	4.50	4.67	4.83	4.83	4.33	2.67	4.25	30.08	4.30	Catalyst
Allthenticate	1.33	1.17	2.83	2.83	1.00	1.33	3.67	14.17	2.02	Pulsar
AuthSignal	3.83	3.33	5.17	5.17	5.00	4.00	4.67	31.17	4.45	Catalyst
Axiad	2.83	2.50	2.83	3.17	2.67	2.50	3.83	20.33	2.90	Pulsar
Badge	3.50	2.67	3.67	2.83	3.00	3.00	2.83	21.50	3.07	Catalyst
Beyond Identity	4.00	3.50	3.83	4.33	3.83	3.83	5.83	29.17	4.17	Catalyst
DUO	5.00	4.83	4.67	4.67	4.83	3.17	4.75	31.92	4.56	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Entersekt	4.00	3.33	4.50	3.17	3.33	2.67	4.17	25.17	3.60	Catalyst
Giesecke+Devrient	5.33	5.00	5.17	4.83	4.50	5.67	5.00	35.50	5.07	Luminary
Hypr	4.17	3.33	4.67	4.17	4.50	5.17	5.92	31.92	4.56	Catalyst
ideem	2.00	2.17	2.83	2.50	2.00	3.00	4.17	18.67	2.67	Pulsar
Idmelon	1.17	2.00	4.00	2.17	2.83	2.00	2.42	16.58	2.37	Pulsar
Indicio	3.00	3.00	4.00	3.00	4.00	5.00	5.75	27.75	3.96	Catalyst
intercede	2.50	3.00	3.17	3.00	2.83	3.33	3.42	21.25	3.04	Catalyst
KEYLESS	4.50	4.67	5.50	5.00	5.33	5.17	5.42	35.58	5.08	Luminary
Loginradius	3.67	3.67	3.50	3.00	3.33	2.50	3.67	23.33	3.33	Catalyst
Nok Nok	2.83	3.33	3.50	3.17	3.00	0.83	3.67	20.33	2.90	Pulsar
Portnox	3.50	2.33	3.33	2.67	2.83	1.00	3.75	19.42	2.77	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Prove	4.33	3.67	4.50	4.17	4.00	2.17	4.25	27.08	3.87	Catalyst
rf IDEAS	3.00	2.50	2.83	2.83	3.00	2.33	3.00	19.50	2.79	Pulsar
Secret Double Octopus	2.50	2.33	3.50	2.67	2.50	2.00	2.50	18.00	2.57	Pulsar
Traitware	2.17	2.00	2.67	2.17	2.00	2.67	3.50	17.17	2.45	Pulsar
Trinsic	2.17	2.33	3.00	3.00	2.50	3.00	4.25	20.25	2.89	Pulsar
Trusona	2.83	3.17	3.50	3.33	3.00	3.67	4.25	23.75	3.39	Catalyst
Yubico	3.83	4.17	4.33	4.83	4.33	1.33	5.83	28.67	4.10	Catalyst
ZEROBIOMETRICS™	2.33	2.33	3.00	3.33	2.50	3.83	5.33	22.67	3.24	Catalyst

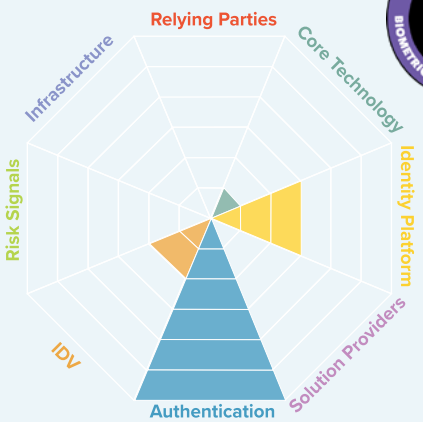
KEYLESS

keyless.io

BEAM: Passwordless Authentication

CLASSIFICATION: Luminary

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
4.50	4.67	5.50	5.00	5.33	5.17	5.42	35.58	5.08



Passwordless Authentication Luminary Keyless is redefining the future of authentication with privacy-preserving biometrics that eliminate passwords, protect users, and resist the most advanced forms of AI-enabled fraud. The London-based company specializes in Zero-Knowledge Biometrics™—technology that converts facial biometric data into unreadable cryptographic representations that ensure the original biometric data is never stored either locally or in the cloud. Their architecture also enables in-built multifactor authentication by binding facial recognition and device possession to the originally enrolled user, delivering a high-assurance identity experience for financial services, crypto platforms, and enterprises. Keyless is also fricitonless—its unique technology results in a small payload which allows for authentication in under 300 milliseconds with just one glance. Keyless' privacy-first model directly advances trust in the biometric digital identity ecosystem, removing the risks inherent in centralized biometric repositories and allowing organizations to deploy strong authentication without ever handling raw biometric data.

Keyless protects privacy through ephemeral, on-demand biometrics that cannot be reconstructed or repurposed, ensuring no biometric honeypot exists and no PII is exposed—even in the event of a cloud compromise. At the same time, its platform delivers deepfake-resilient, fraud-aware authentication: Genuine Identity Assurance ties users to both their live biometric and their enrolled device; passive liveness detection examines textures, patterns, and light indicators beyond the reach of face-swap models; and system-side controls detect risky device behavior, blocking injection and emulation attacks before they reach the matcher. These multilayered safeguards have made Keyless an MFA provider of choice for privacy-sensitive sectors such as crypto, where organizations like the Bitcoin wallet Relai selected it to satisfy strict regulatory requirements without storing biometric data. Now part of the Ping Identity ecosystem, Keyless stands uniquely positioned to shape the next era of digital trust—delivering the rare combination of privacy-first architecture, AI-proof resilience, and effortless user experience that modern identity systems demand.

Contact Keyless: info@keyless.io

Identity Proofing & Verification

Leveraging biometrics, OCR, NFC, and mDLs combined with authoritative sources to enable onboarding and authentication for secure, customer experience-enhancing access to applications and services.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Acupixel	3.50	3.50	4.33	5.33	4.17	4.17	5.50	30.50	4.36	Catalyst
Au10tix	3.50	3.33	4.33	3.83	4.33	5.67	5.75	30.75	4.39	Catalyst
AuthID	3.83	4.33	5.17	4.83	5.17	5.33	5.83	34.50	4.93	Catalyst
Clear	5.17	4.50	5.33	4.83	4.50	5.17	5.58	35.08	5.01	Luminary
Daon	4.33	4.83	5.50	4.67	5.33	5.83	5.67	36.17	5.17	Luminary
Fourthline	4.33	4.33	4.00	4.00	3.83	3.33	4.42	28.25	4.04	Catalyst
GBG	5.00	5.00	5.17	4.33	5.33	5.00	5.83	35.67	5.10	Luminary

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
iddataweb	4.50	4.83	5.50	4.83	4.83	4.67	5.92	35.08	5.01	Luminary
ID.me	5.33	5.00	4.83	5.00	5.17	5.17	4.33	34.83	4.98	Catalyst
IDnow	4.33	4.17	4.83	3.67	3.67	3.00	5.33	29.00	4.14	Catalyst
ID-Pal	1.33	2.00	3.00	2.33	2.33	4.50	4.08	19.58	2.80	Pulsar
IDRamp	1.00	1.33	2.67	3.17	2.33	5.00	4.08	19.58	2.80	Pulsar
IDVerse (LexisNexis)	4.33	3.83	4.83	4.50	5.50	5.17	5.33	33.50	4.79	Catalyst
iiDENTIFii	4.33	4.67	5.00	5.00	5.50	5.33	5.92	35.75	5.11	Luminary
Intellicheck	2.50	2.33	3.50	2.67	2.83	3.50	3.50	20.83	2.98	Pulsar
Mitek	4.67	5.17	5.17	4.33	5.00	5.67	5.92	35.92	5.13	Luminary
Nametag	1.67	1.33	3.00	1.50	1.33	5.00	4.92	18.75	2.68	Pulsar
Ondato	3.00	3.00	5.00	3.00	4.00	5.67	5.25	28.92	4.13	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
OVD KINEGRAM a KURZ company	4.83	5.17	5.00	4.50	4.50	5.00	6.00	35.00	5.00	Luminary
Persona	5.33	3.83	5.00	4.50	5.17	5.50	5.75	35.08	5.01	Luminary
Regula	5.00	5.00	4.83	4.50	4.50	5.33	5.42	34.58	4.94	Catalyst
resistant AI	3.00	1.67	3.33	3.17	2.67	3.00	4.58	21.42	3.06	Catalyst
ShuftiPro	3.17	3.00	3.50	3.00	2.83	4.67	4.58	24.75	3.54	Catalyst
Smile ID	3.00	3.83	4.33	3.67	4.33	4.17	4.92	28.25	4.04	Catalyst
Socure	5.33	4.50	5.00	5.17	5.33	5.00	5.92	36.25	5.18	Luminary
Sumsub	5.00	4.50	4.50	4.17	5.00	5.33	5.92	34.42	4.92	Catalyst
Trulioo	5.17	5.00	4.83	3.50	3.00	5.00	5.92	32.42	4.63	Catalyst
Trust Stamp	2.67	3.00	4.00	3.00	4.00	5.17	5.33	27.17	3.88	Catalyst
veriff	5.00	4.67	5.00	4.83	4.83	5.67	5.92	35.92	5.13	Luminary

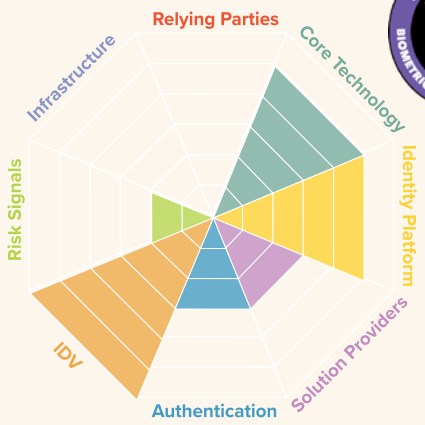
	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Vouched	3.33	3.33	4.50	4.67	4.33	5.17	5.42	30.75	4.39	Catalyst
YouVerse	1.67	1.67	3.33	2.33	1.67	5.00	4.50	20.17	2.88	Pulsar

Daon

daon.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
4.33	4.83	5.50	4.67	5.33	5.83	5.67	36.17	5.17



Daon stands out as a world-leading biometric and digital identity influencer, a multiple-Prism Luminary whose technology has shaped global trust frameworks for more than two decades and continues to anchor the resilience of modern digital ecosystems. Founded in Dublin and now headquartered in the United States, Daon delivers advanced biometric, identity verification, and authentication solutions across financial services, crypto, telecom, retail and e-commerce, telecom, healthcare, government, and travel and hospitality. Its global reach, patented capabilities, and privacy-centric architecture make Daon a defining force in the identity technology market—trusted wherever accuracy, compliance, and holistic identity security converge.

Trust by Design

Daon strengthens trust in the digital identity ecosystem by empowering organizations to collect, process, and store identity elements in line with privacy-first, compliance-forward principles. At the center of this approach is Identity Continuity, Daon's model for verifying a single identity at onboarding, then weaving that identity across all user touchpoints, from authentication to recovery, without duplicating efforts or scattering identity records across siloed systems. This reduces operational risk, simplifies governance, and creates a transparent, auditable chain of trust. Daon's flagship offerings—xProof for identity verification and xAuth/xFace/xVoice for biometric authentication—bring together multimodal biometrics (face, voice, and behavioral), advanced liveness detection, and cryptographic binding to documents and authoritative identity records. IdentityX and TrustX are Daon's orchestration platforms designed to be tailored to the needs of each business, while enforcing data minimization, granular consent, and transparent handling of identity elements. These controls allow relying parties to collect only what is needed, operate with clarity and integrity, and uphold strong privacy guarantees at every step of the digital-identity transaction. This architecture reinforces trust at scale by ensuring identity is managed with precision, accountability, and policy-driven discipline.

Integrity and Resilience in the AI Era

As deepfakes, synthetic identities, and AI-powered impersonation accelerate, Daon's resilience architecture is designed to defend against the most advanced forms of digital deception. Its platform integrates biometric liveness, deepfake detection, synthetic-voice forensics, and real-time risk assessment to detect manipulated or counterfeit identity elements across multiple modalities—including face and voice. Biometric verification is backed by multi-frame analysis, anomaly detection, and device-context signals that identify artifacts of AI-generated media and anticipate new attack vectors. Identity Continuity enhances this resilience by ensuring that once a legitimate identity is established, it remains cryptographically anchored across channels—reducing opportunities for account take-over and strengthening the integrity of every subsequent transaction. By orchestrating biometrics, document verification, device intelligence, authoritative data, and anti-deepfake algorithms, Daon creates layered, escalating defenses that increase the cost, time, and sophistication required for attackers to succeed. Organizations benefit from a system built not only to authenticate real users but to detect, deflect, and expose impostors in real time, preserving operational and transactional integrity.

Protecting a Human-centric Future

Daon's technology and philosophy are shaping a safer era of digital transformation for users and relying parties alike. By protecting identity elements and orchestrating effective fraud countermeasures, this Prism Luminary aligns with the trust and resilience imperatives shaping the digital-identity domain. Daon's platform approach empowers organizations to scale onboarding and authentication globally while maintaining compliance, user-centric control, and resilience in the face of accelerating AI-driven threats. As digital identities become ever more foundational to commerce, government, and daily life, Daon stands at the forefront of the digital identity revolution—ensuring that every identity transaction is secure, seamless, and anchored to a genuine human being.

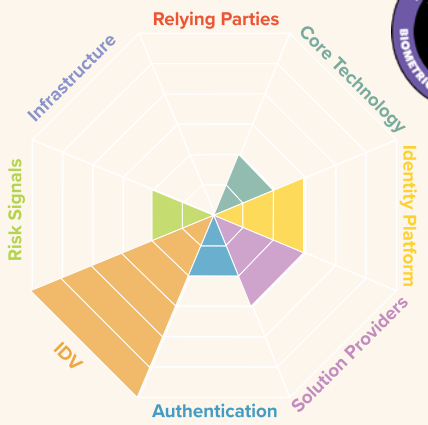
Contact Daon: daon.com/contact-us

iiDENTIFii

iidentifii.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
4.33	4.67	5.00	5.00	5.50	5.33	5.92	35.75	5.11



iiDENTIFii is one of the most powerful and influential forces shaping digital identity in Africa, delivering high-assurance biometric verification rooted in government-validated foundational identity and advanced face biometrics engineered for real-world complexity. Founded in South Africa, the company serves banking, telecom, insurance, government services, and large enterprise markets, providing identity verification to institutions serving the majority of the country's population. Trusted by more Tier 1 banks than any other provider in the region, iiDENTIFii has become a cornerstone of African identity infrastructure. With integrations into authoritative systems of record and proprietary innovations such as 4D Liveness®, the company consistently solves some of the world's most complicated digital-identity challenges—where infrastructure constraints, fraud intensity, and regulatory requirements intersect at massive scale. Deployments with institutions such as Standard Bank, the largest bank on the African continent, which set a new benchmark for digital identity excellence, underscore iiDENTIFii's unmatched market leadership.

Grounded in Authenticity

iiDENTIFii reinforces trust in the biometric digital-identity ecosystem by grounding every verification in authentic, authoritative identity elements. Integrations with government databases bind a user's biometrics to their verified foundational identity, creating a strong, auditable anchor for every digital transaction. Document forensics, anti-tampering controls, and strict alignment with global privacy and security certifications enable regulated organizations to meet and exceed compliance requirements, including FICA, KYC, RICA, and global AML frameworks. The platform's no-code and low-code deployment options make high-assurance verification accessible across devices, bandwidth levels, and operational environments—including regions with intermittent connectivity. By minimizing identity silos and ensuring consistent provenance of identity data throughout the lifecycle—from onboarding to recovery—iiDENTIFii empowers relying parties to uphold privacy, data minimization, and regulatory trustworthiness while delivering frictionless user experiences.

Solidifying African Enterprise Identity

iiDENTIFii's proprietary 4D Liveness® technology delivers one of the strongest biometric-integrity checks in the market. Its temporal-based analysis detects replay attacks, injection attempts, AI-generated faces, and deepfake impersonation across mobile and remote channels. It provides deep data analytics and real-time reporting and enterprise-grade dashboards. With fraud patterns intensifying across African and global financial and government ecosystems—including hybrid synthetic identities, call-center impersonation, and remote-channel attacks—iiDENTIFii's layered defenses provide resilience against high-velocity and high-volume fraud. Automated workflows reduce manual exposure, while built-in redundancy and offline verification capabilities ensure identity assurance even when networks degrade or go offline — an operational necessity across diverse African geographies. Continuous monitoring of global threat vectors and real-time model adaptation allow iiDENTIFii to maintain a hardened security posture that reliably distinguishes human users from digital impostors and AI-enhanced adversaries.

Defining Safe Identity on a Continental Scale

iiDENTIFii's technology, philosophy, and regional leadership are helping define a more secure, inclusive, and resilient digital-identity future for Africa—and increasingly, for global markets. By uniting privacy-first data practices with uncompromising biometric fraud prevention, iiDENTIFii demonstrates how trust and resilience reinforce one another to protect citizens, institutions, and national economies. Its ability to deliver high-assurance identity verification across both high-connectivity urban environments and connectivity-challenged rural regions establishes a global benchmark for equitable, future-ready digital identity. As governments modernize services and enterprises accelerate digital transformation, iiDENTIFii ensures that every interaction—regardless of device, location, or risk level—remains anchored to a genuine human identity, laying the foundation for a safer, more trusted digital era.

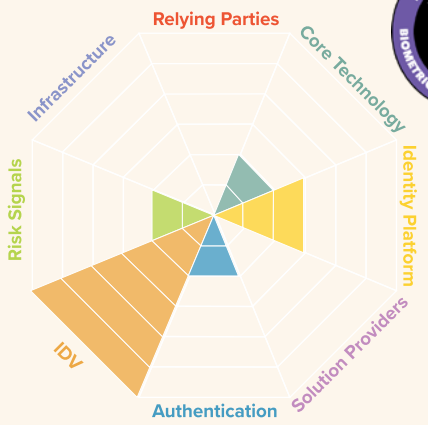
Contact iiDENTIFii: info@iidentifii.com

veriff

veriff.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
5.00	4.67	5.00	4.83	4.83	5.67	5.92	35.92	5.13



Veriff is one of the most globally scalable identity verification platforms in the market today, delivering AI-powered biometrics, document verification, and automated compliance that deliver unmatched reach, speed, and inclusivity to digital identity ecosystems. Founded in Estonia in 2015, Veriff serves financial services, digital marketplaces, gaming, social media, and mobility/gig economy, enabling organizations to verify identities seamlessly across borders and devices. Its platform supports 48 languages, more than 12,000 document types, and users from 230+ countries and territories, enabling instant onboarding at global scale. Achieving unicorn status in 2022 with a valuation of $1.5 billion, Veriff distinguishes itself through exceptional accuracy, fraud defense, and user experience—earning a leadership position among the next generation of identity-verification providers.

Anchoring Trust For Everyone, Everywhere

Veriff strengthens trust at the foundational layer of digital identity by ensuring that the initial verification event—the moment where trust is first established—is both highly accurate and broadly inclusive. Its automated verification can confirm identity in as little as six seconds, while biometric authentication recognizes returning users in under one second, creating a reliable chain of trust throughout the identity lifecycle. Passive liveness detection ensures that the person enrolling is a real human and remains the same individual across all subsequent authentication attempts, countering impersonation at the point of origin. Veriff's ability to support global documents, diverse languages, and frictionless integrations ensures that trustworthy identity is accessible to anyone, anywhere, making Veriff a universal trust anchor across digital ecosystems.

Authentic Identity Elements Only

In an era defined by synthetic identities, deepfakes, scalable spoofing tools, and credential-based attacks, Veriff delivers robust and layered resilience. Its machine-learning-driven fraud-prevention tools—Fraud Protect and Fraud Intelligence—analyze network, device, behavioral, environmental, and biometric risk signals to detect suspicious activity in real time. AI-powered liveness detection and anti-spoofing controls ensure that biometric submissions come from legitimate users, not manipulated media or injected content. This resilience generates measurable outcomes: at fintech platforms such as Kueski, Monzo, and Junacho te Presta. For Uphold, Veriff increased verification success rates, reduced manual review overhead, and significantly lowered fraud within months of deployment. This combination of automation, accuracy, and anti-fraud capability positions Veriff as a leading shield against AI-driven identity threats.

A Cornerstone of Next Generation Identity

By combining global reach, advanced biometrics, passive liveness, and real-time fraud intelligence, Veriff is helping define a safer digital era—one in which trust and security scale together without introducing friction. Its philosophy centers on making verification effortless for genuine users while rendering digital impersonation unviable for attackers, a balance essential to modern digital transformation. As organizations continue to adopt remote onboarding, cross-border services, and AI-enabled digital experiences, Veriff's commitment to privacy, compliance, and anti-fraud innovation positions it as a cornerstone provider for the next generation of secure, user-centric identity ecosystems.

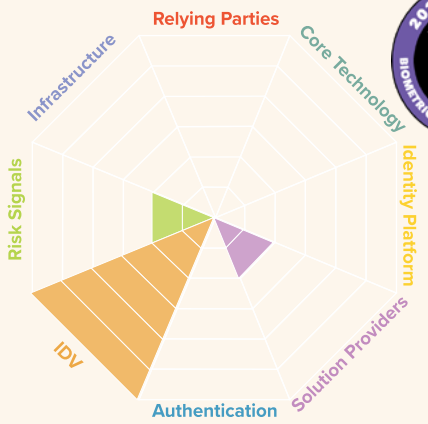
Contact Veriff: sales@veriff.com

iddataweb

iddataweb.com

BEAM: **Identity Proofing & Verification** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average
4.50	4.83	5.50	4.83	4.83	4.67	5.92	35.08	5.01



ID Dataweb is redefining modern identity verification by fusing technology from more than 70 trusted attribute providers into a single, agile orchestration platform. Serving highly regulated sectors—including financial services, e-commerce, gaming, healthcare, aviation, insurance, and government—its no-code, rapid-deployment toolkit unifies contextual, biometric, and document-based identity signals to support verification flows in over 200 countries. By empowering organizations to assemble high-assurance identity proofing with minimal friction, ID Dataweb reinforces trust in the biometric digital identity ecosystem through precise verification and privacy-aligned data handling, while delivering resilience through dynamic, fraud-aware orchestration across the entire identity lifecycle.

ID Dataweb protects privacy by verifying only what is necessary for any given transaction and routing checks through vetted attribute providers, keeping sensitive data distributed rather than concentrated in breach-prone repositories. Simultaneously, it defends against AI-powered fraud with real-time document authentication, biometric face-to-ID matching with liveness detection, and adaptive Just-In-Time (JIT) step-up authentication that evaluates contextual risk signals—such as device intelligence, environmental metadata, and mobile-carrier data—to escalate challenges only when required. These layered capabilities stop deepfakes, synthetic identities, and counterfeit documents before they gain traction, while maintaining a user-friendly onboarding process that compresses multi-week KYC processes into minutes. With unmatched orchestration breadth, same-day deployment, and a proven ability to unify privacy, compliance, and advanced fraud defenses, ID Dataweb stands as a formidable identity engine powering the next generation of trusted, resilient digital identity ecosystems.

Contact ID Dataweb: sales@iddataweb.com

Environmental Risk Signals

Signals intelligence solutions and services that identify a range of environmental risk and fraud factors based on devices, geolocation, behavioral patterns, etc.

Evaluations

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Accertify	5.50	4.17	4.33	4.50	4.17	2.67	4.42	29.75	4.25	Catalyst
Alessa	1.17	1.50	2.83	2.33	1.67	4.17	4.33	18.00	2.57	Pulsar
Arkose Labs	4.67	4.00	4.83	3.67	4.50	2.67	4.50	28.83	4.12	Catalyst
BioCatch	4.67	5.17	4.67	3.83	4.83	2.83	5.92	31.92	4.56	Catalyst
BIVE	2.50	2.50	2.83	2.83	2.67	3.17	4.42	20.92	2.99	Pulsar
Callsign	3.17	2.33	3.00	3.17	2.00	2.17	3.42	19.25	2.75	Pulsar
Datavisor	3.17	2.33	3.50	2.50	2.50	2.17	1.83	18.00	2.57	Pulsar

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
Experian	5.33	4.83	5.17	4.67	5.67	5.67	5.75	37.08	5.30	Luminary
Featurespace	4.67	4.00	4.83	3.67	4.50	2.67	4.75	29.08	4.15	Catalyst
HAWK AI	3.50	4.00	4.00	4.00	4.00	4.00	4.33	27.83	3.98	Catalyst
IBM Trusteer	5.33	5.17	5.00	4.67	5.00	5.00	5.00	35.17	5.02	Luminary
Incognia	3.50	4.00	4.00	5.00	4.00	5.00	5.25	30.75	4.39	Catalyst
Kount (Equifax)	4.83	4.83	5.17	5.00	5.00	4.67	5.58	35.08	5.01	Luminary
Minerva	2.50	2.17	2.67	2.50	3.00	1.33	4.25	18.42	2.63	Pulsar
NeuroID (Experian)	3.33	4.00	4.00	4.00	4.00	4.00	4.42	27.75	3.96	Catalyst
NuData Security	5.33	5.17	5.00	5.00	5.00	5.00	5.00	35.50	5.07	Luminary
Sardine	4.17	4.33	5.00	5.00	4.67	4.50	5.83	33.50	4.79	Catalyst
SEON	4.00	4.33	4.83	4.67	5.00	5.00	4.83	32.67	4.67	Catalyst

	Growth & Resources	Market Presence	Proof Points	Unique Positioning	Business Model & Strategy	Biometric & Doc Auth Capabilities	Resilient Trust Leadership	Total	Average	Beam Position
SHIELD	4.50	3.83	4.50	3.50	4.17	2.17	3.92	26.59	3.80	Catalyst
Sifnifyd	3.67	4.17	4.67	4.67	5.00	5.00	5.83	33.00	4.71	Catalyst
Sift	4.50	4.17	4.67	4.83	5.00	5.00	5.17	33.33	4.76	Catalyst
Telesign	3.83	4.00	4.00	4.00	4.00	4.00	4.75	28.58	4.08	Catalyst
ThreatMark	3.50	4.00	4.00	4.00	4.00	2.00	4.58	26.08	3.73	Catalyst
Transunion	5.33	5.50	5.17	5.17	5.50	4.50	5.75	36.92	5.27	Luminary
Unit21	3.83	5.00	4.83	4.33	5.17	5.00	4.00	32.17	4.60	Catalyst

Infrastructure, Community, Culture

Public and private sector organizations engaged in standards, policy, regulation, and technology frameworks that validate, certify, and provide guardrails for the ethical capture, storage, matching, and disposal of digital identity elements.

Evaluations

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
ACLU	3.00	4.00	5.67	4.00	2.00	2.00	5.08	25.75	3.68	Catalyst
Adobe	5.67	5.33	5.17	5.50	5.33	3.00	5.17	35.17	5.02	Luminary
AAMVA	4.75	5.00	5.17	5.83	5.00	5.00	5.58	36.33	5.19	Luminary
Anthropic	4.17	3.50	4.17	5.50	4.67	0.00	4.83	26.83	3.83	Catalyst
Biometrics Institute	4.75	4.50	3.67	4.33	4.17	4.50	5.33	31.25	4.46	Catalyst
BixeLabs	2.75	3.00	4.50	6.00	6.00	6.00	5.50	33.75	4.82	Catalyst
C2PA	6.00	6.00	5.50	6.00	6.00	0.00	5.92	35.42	5.06	Luminary

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
CDT	3.00	4.17	5.17	5.00	5.17	4.33	5.25	32.08	4.58	Catalyst
Decentralized Identity Foundation	2.75	2.67	3.00	3.17	3.50	1.00	3.92	20.00	2.86	Pulsar
DIACC	4.00	4.50	5.33	5.50	5.33	5.00	5.75	35.42	5.06	Luminary
EPIC	3.00	4.00	5.00	4.17	4.17	2.00	5.25	27.58	3.94	Catalyst
eu-LISA	5.25	5.17	4.33	5.50	5.00	5.33	5.50	36.08	5.15	Luminary
European Association for Biometrics eab Human Identity in Europe	4.00	5.00	5.17	4.83	4.50	6.00	5.33	34.83	4.98	Catalyst
European Comission	5.00	5.33	5.17	5.50	5.00	5.83	5.75	37.58	5.37	Luminary
Fime	5.00	4.83	4.67	4.50	4.67	5.33	4.33	33.33	4.76	Catalyst
FinCEN	5.00	4.67	4.83	4.83	4.67	1.00	5.25	30.25	4.32	Catalyst
finra	3.00	5.00	5.00	3.00	3.00	2.00	5.50	26.50	3.79	Catalyst
Future of Privacy Forum	4.25	5.17	5.67	5.33	5.00	4.00	5.92	35.33	5.05	Luminary

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
Google AI	5.67	6.00	5.33	5.33	5.50	2.00	4.33	34.17	4.88	Catalyst
GAO	5.00	4.33	3.50	4.83	3.50	4.00	4.50	29.67	4.24	Catalyst
IAPP	4.25	5.50	5.00	5.33	5.00	4.00	5.75	34.83	4.98	Catalyst
iBeta	1.50	3.00	2.33	2.00	1.33	4.50	2.83	17.50	2.50	Pulsar
IBIA	1.75	1.83	1.83	2.33	1.17	3.50	2.58	15.00	2.14	Pulsar
ID4Africa	4.75	5.33	5.00	6.00	5.33	6.00	5.83	38.25	5.46	Luminary
IDSA	2.75	3.00	2.67	2.83	2.50	1.00	4.58	19.33	2.76	Pulsar
Identity Mangament Institute	3.00	4.00	4.00	4.00	2.00	3.00	5.08	25.08	3.58	Catalyst
Ingenium Biometrics	2.00	2.67	3.33	2.50	2.17	4.67	3.50	20.83	2.98	Pulsar
ISO	5.00	5.00	5.50	5.33	5.50	5.00	5.92	37.25	5.32	Luminary
kantara INITIATIVE	4.25	4.67	4.83	5.33	4.33	4.67	5.50	33.58	4.80	Catalyst

	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
Meta AI	5.67	6.00	4.33	5.33	5.67	2.17	3.25	32.42	4.63	Catalyst
National Cyber Security Centre	4.75	5.33	5.67	6.00	5.83	5.00	5.42	38.00	5.43	Luminary
NIST	5.00	4.83	5.50	5.33	5.50	6.00	5.92	38.08	5.44	Luminary
Nvidia	5.83	5.67	5.17	6.00	6.00	0.67	5.58	34.92	4.99	Catalyst
OAIC	3.00	4.00	5.00	4.00	2.00	4.67	5.17	27.83	3.98	Catalyst
OpenAI	5.17	4.00	4.50	4.17	5.00	0.83	4.92	28.58	4.08	Catalyst
Privacy International	4.25	5.17	5.33	5.33	5.00	3.33	5.67	34.08	4.87	Catalyst
SECURE TECHNOLOGY ALLIANCE	3.25	4.50	4.83	4.67	5.17	5.17	5.17	32.75	4.68	Catalyst
TSA	5.25	5.33	4.83	5.83	5.17	6.00	4.75	37.17	5.31	Luminary
US CBP	5.25	5.33	5.17	5.83	5.17	6.00	3.67	36.42	5.20	Luminary
US DHS	5.25	5.33	5.83	5.83	5.17	6.00	3.67	37.08	5.30	Luminary

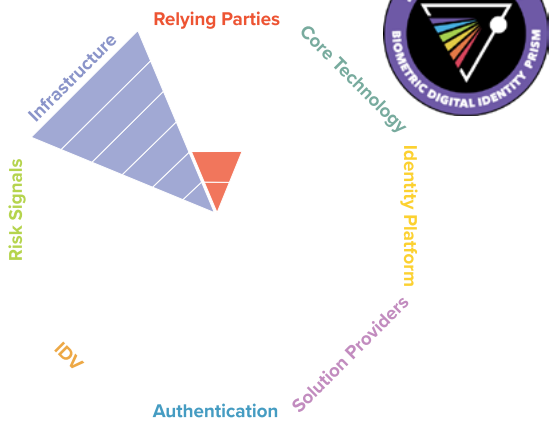
	Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average	Beam Position
World Privacy Forum	5.25	5.00	5.50	5.00	5.00	5.33	2.67	33.75	4.82	Catalyst

DIACC

diacc.ca

BEAM: **Infrastructure** / CLASSIFICATION: **Luminary**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average
4.00	4.50	5.33	5.50	5.33	5.00	5.75	35.42	5.06



The Digital ID & Authentication Council of Canada (DIACC) is a national nonprofit public–private strategic alliance dedicated to delivering resources that help build secure, privacy-enhancing digital trust and identity verification infrastructure for Canada. Serving government, financial services, e-commerce, telecommunications, and public-safety sectors, DIACC is remarkable for its role as a global model of multi-stakeholder governance and digital trust design. Its signature innovation—the Pan-Canadian Trust Framework™ (PCTF)—provides a standards-based blueprint comprising auditable criteria that support interoperable, user-centric digital trust and identity verification, enabling organizations across sectors to align on consistent definitions of assurance, consent, authentication, and accountability. In an era of accelerating digitization and cross-border data exchange, DIACC stands out for its work to promote a layered approach to policy harmonization that respects jurisdictional authority while balancing technology interoperability and market needs, ensuring privacy remains at the center of every transaction.

Aligning Canadian Digital Trust and Identity Verification With Confidence

DIACC strengthens confidence in the biometric digital trust and identity verification ecosystem by embedding privacy, ethics, and transparent governance into the foundations of Canada's digital trust and identity verification infrastructure. The PCTF provides a structured framework for ensuring that data—including biometrics, contextual metadata, and credential attributes—is collected, stored, and used in accordance with rigorous, privacy-first standards. Its guidance complements core compliance frameworks such as KYC and AML, helping financial institutions strengthen identity verification while minimizing data exposure and supporting decentralized identity and verifiable-credential architectures that give individuals and organizations greater control over their data elements. DIACC's collaboration with international bodies—such as Trust Over IP, SIROS Foundation and peer governance groups—ensures that Canada's digital trust and identity verification infrastructure evolves in alignment with international best practices, interoperability requirements, and the next generation of global trust frameworks.

Laying the Groundwork for Digital Trust and Identity Verification Resilience

DIACC also plays a pivotal role in strengthening digital trust and resilience in identity verification across Canada's digital economy. Its policy, guidance, and architectural recommendations help reduce fraud, mitigate synthetic identity risks, and modernize authentication practices amid escalating AI-powered threats. Sector-specific directives highlight how PCTF-aligned implementations can reinforce onboarding security, reduce e-commerce and mobile banking fraud, enhance identity verification for emergency responders, and streamline regulatory reporting.

Through its work on cross-border verification, decentralized proofs, and digital credentials for government services such as driver's licenses and passports, DIACC delivers resources that support resilient infrastructure capable of withstanding deepfakes, misinformation, and manipulation—while improving accessibility and operational efficiency across Canada's digital economy.

Earning Public Trust as Digitization Accelerates

As digital transformation accelerates and reshapes society, DIACC is helping shape a safer future for both users and relying parties by championing a cohesive, privacy-forward, and fraud-resistant digital trust and identity verification ecosystem. Its philosophy emphasizes transparency, responsible innovation, and the protection of individual rights—an approach that positions Canada as a leader in global digital trust. By uniting the strengths of industry, governments, and civil society around a shared vision for secure digital trust and identity verification, DIACC is laying the groundwork for a future in which digital services are not only efficient and resilient but fundamentally worthy of the public's trust.

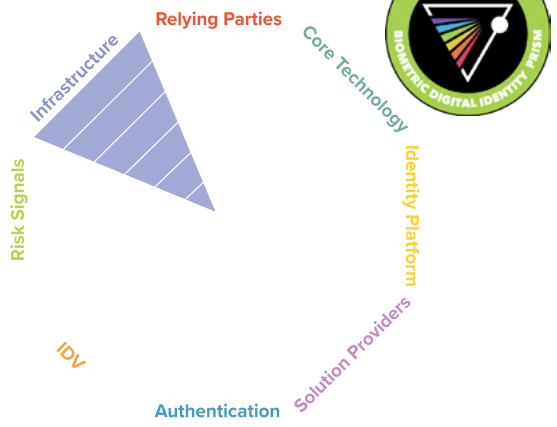
Contact DIACC: contact@diacc.ca

European Association for Biometrics eab Human Identity in Europe

eab.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average
4.00	5.00	5.17	4.83	4.50	6.00	5.33	34.83	4.98



The European Association for Biometrics (EAB) is one of Europe's most influential independent voices on responsible biometric innovation, shaping how privacy, security, and digital identity evolve across one of the world's most regulated data-protection landscapes. A nonprofit, nonpartisan organization founded in 2011 to unite public institutions, industry, academia, and civil-society groups, the EAB operates at the intersection of policy, regulation, and technology—helping stakeholders navigate Europe's uniquely complex identity environment. With members spanning public services, border control, financial services, research institutions, enterprise security, and digital identity vendors, the EAB has become the continent's leading authority on harmonizing biometric innovation with cultural diversity, regulatory rigor, and cross-border interoperability. In a region defined by GDPR and a strong heritage of privacy protection, the EAB plays a pivotal role in advancing identity systems that are both technologically sophisticated and fundamentally human-centric.

Strengthening Trust at the Ecosystem Level

The EAB reinforces trust across the biometric digital identity ecosystem by championing fairness, accessibility, privacy, and secure identity management. Through extensive education, lectures, working groups, and multi-stakeholder collaborations, the EAB seeks to ensure that biometric deployments meet Europe's high bar for data minimization, transparency, and user rights. Its Industry, Academia, and Operator Special Interest Groups (SIGs) each contribute to developing best practices, conducting independent research, providing public-policy guidance, and undertaking forward-looking analysis tied to EU legislation. Whether examining template security, usability, demographic-performance considerations, or algorithmic implications under European law, the EAB's coordinated work helps vendors and public institutions uphold the privacy contract with citizens. By fostering knowledge-sharing and alignment across sectors, EAB advances Europe's digital identity ecosystem with integrity, accountability, and adherence to core European values.

Emboldening Stakeholders in the AI Fraud War

EAB also strengthens resilience by preparing stakeholders to defend against the accelerating risks of AI-powered fraud, including deepfakes, synthetic identities, and multimodal spoofing. Through multidisciplinary workshops, operator-focused training, regulatory analysis, and transparency-oriented discussions, the Association guides governments and organizations toward safe, repeatable, and compliant deployment practices—reducing the need to "reinvent the wheel" as threats evolve. The EAB promotes harmonized standards, secure storage methods, robust performance evaluation, and privacy-preserving research to ensure biometric systems remain effective under adverse conditions and resilient against emerging attack vectors. Its annual EAB Research Projects Conference—the largest EU-funded biometric research event—accelerates resilience by showcasing cutting-edge scientific findings, supporting technology transfer, and fostering collaboration between academia, industry, and public agencies. Through this work, the EAB helps fortify Europe's identity infrastructure against AI-driven threats without compromising civil rights.

Shaping Europe's Privacy-first Identity

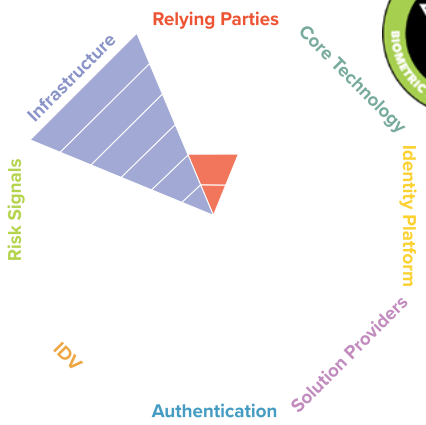
Policy leadership– another core pillar of EAB's activities, helps the association define the next generation of secure, privacy-first digital identity across Europe. This is done through research coordination, industry engagement, and unwavering commitment to user rights. As digital and physical transactions converge and biometric use cases expand across borders and sectors, the EAB serves as a strategic compass—guiding organizations toward technologies and practices that uphold Europe's heritage of data protection while resisting the growing sophistication of fraud. By uniting diverse stakeholders around a shared vision of trustworthy biometric innovation, the EAB is laying the foundation for a safer, more interoperable, and more resilient digital future for citizens, enterprises, and governments throughout Europe.

Contact EAB: secretariat@eab.org

kantarainitiative.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average
4.25	4.67	4.83	5.33	4.33	4.67	5.50	33.58	4.80



The Kantara Initiative has rapidly emerged as a global player shaping the trustworthy use of identity and personal data by defining how privacy, assurance, and interoperability will evolve in the next era of digital identity. Founded in 2009 and uniquely authorized to assess identity solutions against NIST 800-63 guidance, Kantara operates worldwide as a central hub for standards development, collaboration, and technical leadership. Serving government, financial services, mobile identity, healthcare, and enterprise security, the organization contributes directly to trust—by advancing privacy-preserving frameworks—and resilience—by preparing institutions to withstand the emerging fraud vectors reshaping biometric and remote-verification systems.

Anticipating Next-Gen Identity Risks

Kantara proactively strengthens privacy and fraud defense through initiatives designed to anticipate and neutralize the next wave of identity threats. Its Privacy Enhancing Mobile Credentials (PEMC) working group develops safeguards ensuring that mobile ID ecosystems respect consent, prevent mission creep, and protect individuals from unauthorized data use—even when interacting with otherwise trusted relying parties. Its newly formed Biometric Data Discussion Group will provide guidance for ethical and responsible biometric data management, augmenting standards with pragmatic, deployment-ready best practices. Kantara has also taken a leading role in addressing AI-driven impersonation: its groundbreaking 2024 Deepfake Threats to Identity Verification & Proofing project mapped the remote verification workflow, catalogued synthetic-identity and deepfake threat vectors, and identified corresponding mitigation strategies. This work now informs broader industry and government preparedness—including the IDV process diagrams used by The Prism Project—giving organizations a clear, defensible path for hardening digital identity against rapidly accelerating AI attacks.

Writing the Playbook For Trust and Resilience

Through its community-driven governance model, rigorous assurance programs, and unmatched ability to translate complex identity challenges into actionable frameworks, Kantara has become a foundational pillar of modern digital identity infrastructure. Its ongoing research publications, convening of global experts, and continuous updates to its NIST-aligned assessment program ensure that vendors, relying parties, and regulators are aligned on a common, future-ready set of requirements. By uniting technical standards, policy guidance, and practical deployment expertise, the Kantara Initiative is setting the benchmarks that will guide trusted identity for years to come while shaping a safer, more privacy-preserving, and fraud-resilient digital world for users and institutions alike. In doing so, Kantara distinguishes itself as a leading voice in the biometric digital identity community.

Noatable Members:

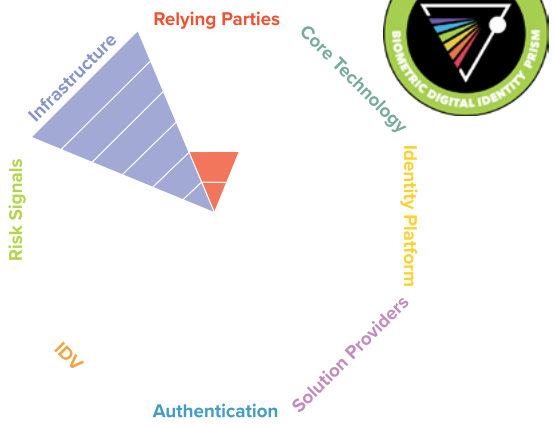
Contact The Kantara Initiative: hello@kantarainitiative.org

SECURE TECHNOLOGY ALLIANCE

securetechalliance.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Resilient Trust Leadership	Total	Average
3.25	4.50	4.83	4.67	5.17	5.17	5.17	32.75	4.68



The Secure Technology Alliance (STA) is a driving force in secure identity, payments, and digital trust in the United States—guiding the nation through three decades of technological change at a time when authentication, privacy, and safety have become existential priorities. Founded in 1993, a widely recognized pioneer of the smart-card movement, the STA has consistently championed technologies that protect users across both physical and digital environments. Today, the Alliance s a leading national advocate for mobile driver's license (mDL) adoption, championing this next-generation, cryptographically verifiable credential as a foundational tool for strengthening trust and resilience across the biometric digital identity ecosystem.Through its leadership across payments, identity, access control, and public-sector modernization, STA ensures that emerging technologies are deployed not only in ways that are interoperable and secure but also privacy-centric and fraud-resistant.

Driving Privacy and Authenticity in the AI Era

In an era defined by synthetic identities, deepfakes, and AI-driven impersonation, STA plays a critical role in advancing verification methods that both protect users and strengthen identity resilience. Its mDL Jumpstart Committee, chaired by industry expert David Kelts, promotes mobile driver's licenses as a modern alternative to conventional document capture—eliminating the analog-to-digital conversion step that attackers routinely exploit. Unlike conventional workflows that rely on images vulnerable to spoofing, mDL verification uses cryptographically signed, issuer-controlled data shared with explicit user consent, without exposing raw biometric or image data to relying parties. There is no facial image capture, no sensor-dependent liveness check, and virtually no opportunity for deepfake manipulation, significantly reducing the attack surface. STA also confronts privacy concerns head-on by elevating the pseudonymous, consent-first model inherent in mDL standards (ISO 18013-5). Users control exactly which identity fields are shared; relying parties receive only the minimum information required; and all transactions are built on privacy-by-design principles. This dual emphasis on privacy protection and authenticity assurance positions STA as a central leader in defining how secure identity must evolve in the age of AI.

Technology, Policy, Adoption

As a national convener, STA accelerates the adoption of next-generation identity infrastructure by bringing together technology providers, government issuers, standards bodies, financial institutions, mobile platforms, and enterprise relying parties. Its evolution—from stewarding the U.S. Payments Forum to also establishing the Identity and Access Forum (IAF)—reflects a strategic understanding that payments and identity are intertwined pillars of digital commerce and public trust. STA unifies stakeholders around common standards, shared deployment models, and actionable best practices that streamline implementation and reduce fragmentation. STA's critical influence is evident in advancing statewide mDL deployments, harmonizing public- and private-sector trust frameworks, and adopting privacy-enhancing verification methods designed to withstand AI-enabled fraud, escalating regulatory expectations, and accelerating market complexity. By bringing coherence to the intersection of technology, policy, and operational adoption, the Secure Technology Alliance is helping shape a safer, more trusted digital future—one where secure identity is interoperable, user-centric, and fundamentally worthy of public confidence.

Identity & Access Forum Steering Committee Members:

For a complete list of STA members, visit https://www.securetechalliance.org/alliance-members/

Contact STA: info@securetechalliance.org

The Resilient Trust Convergence Imperative

As we have seen, widespread digitization unlocks the potential for a world of secure, seamless, integrated physical and logical access powered by biometric digital identity. Yet, the rapid expansion of identity data also introduces profound risks to trust and systemic resilience. As global regulations race to keep pace—and as deepfakes, synthetic identities, and AI-driven fraud escalate—relying parties must treat privacy protection and fraud resistance not as competing priorities but as inseparable pillars of responsible identity governance. By grounding their strategies in the foundational layers of the Prism Identity Hierarchy—where authentic biometric binding, minimal data exposure, and system-of-record assurance converge—organizations across sectors can uphold user trust, strengthen compliance posture, and safeguard the integrity of every transaction.

Resilient Trust is The Way

The past decade has been defined by adoption—of biometrics, of digital wallets, of new identity platforms. The present moment, 2025, is defined by two converging forces—resilience and trust. Deepfakes, synthetic identities, and escalating data-governance expectations are reshaping the biometric digital identity ecosystem at its core. This is not a temporary state of play. It is a permanent shift. Fraudsters will not relinquish AI-powered impersonation. Regulators will not relax the rules around privacy and user control. Customers will not compromise their demand for seamless, human-anchored digital experiences.

The future of digital identity is not defined by fraud prevention or privacy in isolation, but by reconciling these tensions and their intersection with user empowerment.

Convergence Imperative

The digital identity ecosystem, therefore, faces a dual mandate:

- Protect human identity against the escalating risks of synthetic fraud, deepfakes, and systemic exploitation.
- Empower individuals with privacy, transparency, and control, transforming compliance into confidence and experience into differentiation.

This dual mandate is not optional. **It is the foundation of trust in the digital economy.**

The Prism calls this the Convergence Imperative: a recognition that only by aligning fraud defense with privacy and user empowerment can we build the resilient, trust-centered ecosystems demanded by the digital age. Organizations that adopt the convergence imperative will embrace:

- **Easy and accessible onboarding** that binds human biometric identity to authoritative records, enabling trusted identity establishment, rejecting synthetic identities early, and keeping pace with evolving privacy and compliance requirements.
- **Strong, continuous authentication**—reinforced by liveness, deepfake detection, and behavioral intelligence—that carries trust forward from enrollment through high-risk events such as account recovery and sensitive transactions.
- **Seamless user experiences** that satisfy rising expectations for convenience while maintaining cryptographic, biometric, and contextual safeguards that ensure only genuine users can interact within digital ecosystems.
- **Hybrid centralized/decentralized identity architectures** that minimize data exposure, operationalize user consent, support offline and online use cases, and eliminate the honeypot risks that erode long-term trust.
- **Privacy-first design philosophies** that embed principles of data minimization, security, and consent into the foundation of all user-facing operations.
- **User-centric identity systems** that prioritize empowerment and sovereignty across the digital and physical landscapes of a post-digitization reality.

Strategic Guidance for the Ecosystem

Resilience cannot be built in isolation. No vendor, platform, or regulator can secure the ecosystem alone. The Prismatic Future demands cross-sector collaboration:

- **Technology, Platform, and Solution Vendors** must embed privacy and synthetic defense into interoperable systems.
- **Relying Parties** must orchestrate fraud, privacy, and customer experience in unified strategies.
- **Policymakers and Regulators** must align laws with innovation, enabling trust without stifling progress.
- **Infrastructure, Community, and Culture Contributors** must proactively engage, ensuring identity systems meet rigorous performance, trust, and resilience standards and are designed and built for everyone.
- **End-Users** must expect and demand the highest levels of trust and resilience from public and private sector stakehold-

ers that deploy digital identity solutions, using their electoral and economic power to drive adoption.

The Prism Project's 2025 analysis dictates three calls to action for all ecosystem participants:

Adopt Multi-Layered Resilience

- Defend the entire identity lifecycle with orchestrated controls.
- Invest in AI-powered defenses, continuous monitoring, and privacy-enhancing technologies.

Elevate Trust from Burden to Strategy

- Treat privacy as an enabler and strategic advantage, not an obstacle or checkbox.
- Use certifications, transparent practices, and privacy-first design as market differentiators.

Design Seamless, Inclusive Experiences

- Ensure that security and compliance enhance—not compromise—the customer journey.
- Design customer journeys to be accessible and inclusive. Identity solutions must be designed and built for everyone

Let the Prism Be the Guiding Light

The Prism Project exists to illuminate pathways forward. Enterprise leaders today face a vast and rapidly shifting landscape of biometric digital identity solutions—but the organizations featured in this report have demonstrated readiness, maturity, and the proven ability to deliver Resilient Trust, reinforcing both privacy and fraud defense as digital and physical worlds converge. By adopting identity technologies built with biometrics, privacy preservation, and system-of-record assurance at their core, organizations now have not only the opportunity—but the responsibility—to restore global confidence in identity itself, repel AI-powered manipulation, and accelerate a safer, more accountable era of digital transformation.

The 2025 Flagship is both a warning and a blueprint: a warning that identity is under active siege, and a blueprint for how resilience, privacy, and user empowerment can unite to produce a trust-centered identity future.

The Prismatic Future is a world where fraud is neutralized before it can act, privacy is the default setting of every interaction, and identity becomes an empowering force that protects people everywhere. In the world of biometric digital identity

Resilient Trust is not just possible; it is inevitable.

Prism Partners

The Prism Project is proud to collaborate with the following publication partners:

ID Tech is a leading online publication dedicated to the digital identity and biometrics industry. The platform provides daily news, in-depth articles, and expert thought leadership covering the latest trends, technologies, and regulatory updates in digital identity. Its content spans a broad range of topics, including government initiatives, private sector innovations, and the evolving landscape of biometric authentication and identity verification solutions. The site is recognized for its timely reporting and comprehensive coverage, making it a go-to resource for professionals, policymakers, and technology enthusiasts seeking to stay informed about advancements in identity management.

In addition to news updates, ID Tech features interviews with industry leaders, podcasts, and featured articles that offer insights into the practical applications and challenges of digital identity technologies. The platform also maintains a company directory, providing visibility to key players in the field. With a focus on thought leadership and expert commentary, ID Tech plays a crucial role in fostering dialogue and knowledge exchange within the identity technology ecosystem.

IDENTITYWEEK
GLOBAL • TRUSTED • VISIONARY

IdentityWeek is a leading online publication and news platform serving the global identity and security ecosystem. As the digital arm and sister publication to the renowned Identity Week series of events, it delivers breaking news, expert analysis, and in-depth features on the latest developments in digital identity, biometrics, secure credentials, verification, authentication, decentralized identity, and identity management. The platform

curates content for government, enterprise, and industry professionals, highlighting innovations, regulatory shifts, and emerging threats such as deepfakes and fraud. Its coverage is closely aligned with the work of the broader identity sector, reporting on how organizations authenticate and protect identities across physical, digital, and mobile domains.

IdentityWeek also acts as a community hub, supported by a bi-weekly newsletter and regular multimedia content, including interviews and short-form video insights from key stakeholders and industry experts. The publication's audience includes over 10,000 readers, reflecting its role as a trusted source of information and trend analysis for decision-makers and practitioners worldwide. In addition to news, IdentityWeek.net promotes and reports on its flagship global events-such as Identity Week Europe and Identity Week America-which offer networking, education, and business development opportunities for companies and professionals involved in identity verification, fraud prevention, and digital trust.

PEAK iDV

PEAK IDV is a media and enablement provider specializing in digital identity and identity verification (IDV). Founded in 2022 and led by industry veteran Steve Craig, the company offers media and expert advisory services to enterprise buyers, solution providers, and investors navigating the rapidly evolving digital trust landscape. PEAK IDV's media offerings include tailored enablement programs through their PEAK IDV ACADEMY. Additionally, its PEAK IDV LIVE virtual events create engaging and timely livestream content for the broader community featuring experts and in-depth coverage of topics such as artificial intelligence, authentication, biometrics, fraud prevention, and more.

PEAK IDV is also recognized for its thought leadership within the industry. The company produces the EXECUTIVE SERIES video podcast and newsletter, featuring interviews with innovators and CEOs, and covers merging topics like deepfakes and synthetic identity fraud. By combining deep market intelligence with community-driven learning, PEAK IDV positions itself as a trusted partner for organizations and investors seeking to navigate the complexities of digital identity, compliance, and fraud prevention in today's digital-first world.

KYC AML Guide is a specialized intelligence platform and consultancy focused on helping businesses navigate the complex landscape of Know Your Customer (KYC) and Anti-Money Laundering (AML) technology solutions. Headquartered in London with additional presence in Dubai and Milwaukee, the company operates at the intersection of compliance journalism, technology evaluation, and B2B matchmaking. KYC AML Guide assists financial institutions and new economy businesses in selecting the most suitable KYC solutions to streamline customer onboarding and identity verification processes. Their platform offers objective, data-driven vendor analysis—leveraging over 165 testing metrics and more than 100 deployment consultations—to ensure clients make informed decisions based on transparent and quantitative criteria.

Beyond consultancy, KYC AML Guide acts as a marketplace for compliance expertise, connecting organizations with seasoned KYC/AML professionals for short-term projects across industries and regions. Their services encompass a comprehensive suite of KYC and AML offerings, including biometric verification, document and age verification, eID, video KYC, PEP and sanctions screening, adverse media checks, and payment fraud prevention. The company is recognized for its rigorous and transparent methodology, as well as exclusive vendor performance ratings, positioning itself as a trusted partner for compliance-driven organizations seeking to reduce onboarding friction, enhance regulatory adherence, and stay ahead in the rapidly evolving RegTech space.

The Prism Project Reports and Sponsorship Opportunities

Showing Identity in a New Light

The Prism Project arose organically out of a collaborative survey-based research project launched by Acuity Market Intelligence and FindBiometrics in late 2022. The intent of the Project is to use the proprietary Prism framework as the lens through which we continue to analyze and evaluate the rapidly evolving biometric digital identity industry as we help influencers and decision makers understand, innovate, and implement digital identity technologies.

Published Reports

In 2024 and 2025 The Prism Project published seven reports, focused on biometric digital identity adoption in key vertical markets and the major threats facing the industry:

- The Financial Services Prism Report
- The Travel and Hospitality Prism Report
- The Government Services Prism Report
- The 2024 Flagship Prism Report
- Deepfake and Synthetic Identity Prism Report
- Privacy and Compliance Prism Report
- The 2025 Flagship Prism Report

2026 Sponsorship Opportunities

The Prism Project will publish, promote, and distribute two new Full-Spectrum reports in 2026, focusing on the financial services sector and the next evolution of biometric digital identity:

- The 2026 Financial Services Prism Report
- The 2026 Flagship Prism Report

Additionally, we will be introducing new Focal-Point Reports: shorter, sharper reports that laser-focus on flashpoint issues in identity, like:

- Airport customer journeys

- Agentic AI
- Gaming
- Decentralized identity

Download our 2026 brochure for more information.

Ongoing Collaboration

The Prism Project is conducting on-going research and continuing to explore how biometric digital identity is being used today, where the roadblocks to adoption lie, what obstacles must be overcome to successfully deploy these technology solutions, and where they are being used and by whom. We welcome collaborators and are open to discussing how your organization might benefit from and/or leverage the opportunities The Prism Project presents. To reach out, visit www.the-prism-project.com or email us at info@the-prism-project.com.

About the Author

Maxine Most

Internationally recognized biometrics and digital identity thought leader celebrated for provocative market insights, accurate market predictions and forecasts, and unbiased, pragmatic market intelligence.

Strategic innovator, market visionary, and forecasting guru Maxine Most is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic research and analysis consultancy recognized as the definitive authority on global biometrics market development. Throughout her decades long career, Maxine has evangelized emerging technology on five continents. Since 2001, she has applied her unique ability to bring clarity to the unpredictable and volatile world of emerging technology to the rapidly evolving biometric and digital identity marketplace.

As an executive strategist, Maxine has earned a stellar reputation for innovative thought leadership by consistently providing unique, unvarnished, and reliable market insight while accurately anticipating biometric and digital identity market trends. Under her leadership, Acuity has provided strategic guidance to Global 1000s, established technology market leaders, start-ups, and a range of organizations in between. Most leverages her deep understanding of technology evolution, emerging market development, and the process through which industry leaders are created to provide candid strategic analysis, highly targeted implementation plans, and quantifiable, measurable results.

Ms. Most is the author of numerous biometric and digital identity research reports including Face Verification & Liveness for Remote Digital Onboarding," "The Global Automated Border Control Industry Report: Airport eGates & Kiosks," "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy," "The Global National eID Industry Report," "The Global ePassport and eVisa Industry Report," and "The Future of Biometrics," as well as a contributor to several books including "Digital Identity Management" edited by digital identity thought leader David G. Birch.

Ms. Most regularly offers insight and analysis in on and off-line publications, is quoted often in industry, business, and consumer press, is an active contributor to the Kantara Initiative, and presents

regularly at industry events on the evolution and development of biometrics and digital identity markets. She is a graduate of the University of California, San Diego with a multi-disciplinary degree in Mathematics and Computer Science and minors in Visual Arts and Economics.

Let The Prism Project be Your Guiding Light!

The Prism Project (www.the-prism-project.com)
The Prism Project is an innovative framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is **the only market model that is truly biometric-centric** based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics.

Maxine Most
Principal, Acuity Market Intelligence
cmaxmost@acuity-mi.com
Founder, The Prism Project
cmaxmost@the-prism-project

About Acuity Market Intelligence:

With decade of practical expertise in the unpredictable and volatile world of emerging technology, Acuity Market Intelligence consistently delivers consistently original, thought-provoking, and reliable insight and analysis. Proud, self-proclaimed technology business development and marketing geeks, Acuity is globally renowned for its uniquely customized business and marketing strategies and for creating and deploying innovative programs that integrate digital and traditional channels and platforms.

Visit acuitymi.com and let us help your organization thrive.