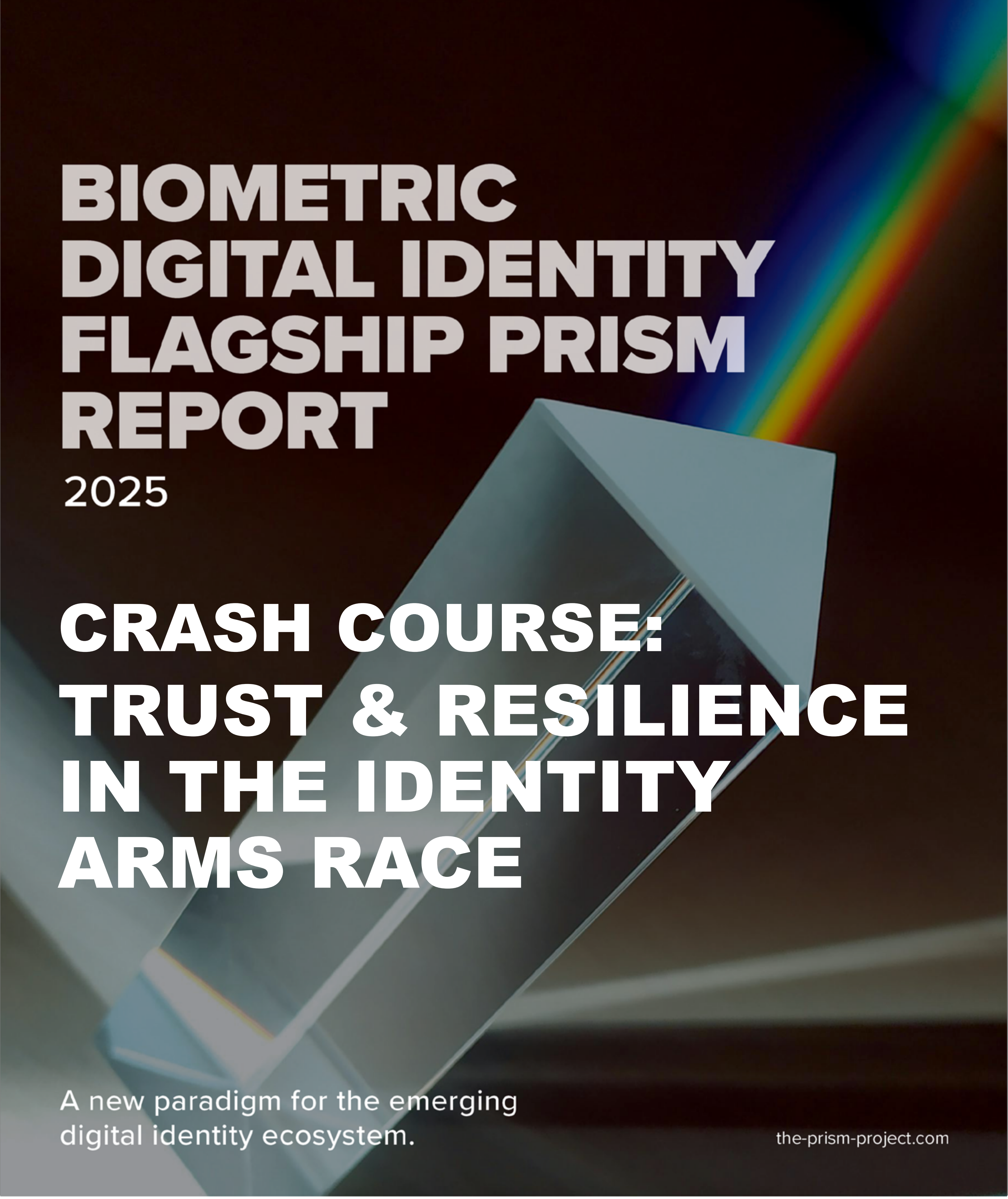

BIOMETRIC DIGITAL IDENTITY FLAGSHIP PRISM REPORT

2025

CRASH COURSE: TRUST & RESILIENCE IN THE IDENTITY ARMS RACE

A new paradigm for the emerging digital identity ecosystem.

the-prism-project.com

THE PRISM PROJECT

ACUITY MARKET INTELLIGENCE

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

Daon
iiDENTIFii
veriff
European Association for Biometrics eab Human Identity in Europe
fido ALLIANCE
DIACC
kantara INITIATIVE
SECURE TECHNOLOGY ALLIANCE
AWARE
alcatraz
iddataweb
Anonybit
KEYLESS
incode
PANINI
IDEMIA PUBLIC SECURITY
sodec TECHNOLOGIES
NextgenID
KAIZEN VOIZ simple · seamless · secure
PARAVISION
Corsound AI Voice Intelligence Technologies
ideem
OVD KINEGRAM a KURZ company
DUCK DUCK GOOSE
ID R&D a Mitek company
Mitek
wicket
ZeroBiometrics
iProov

PARTNERS

IDENTITYWEEK GLOBAL • TRUSTED • VISIONARY
ID TECH
KYC/AML GUIDE
PEAK iDV

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.

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).

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.).

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.

- 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.

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.

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

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.

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.