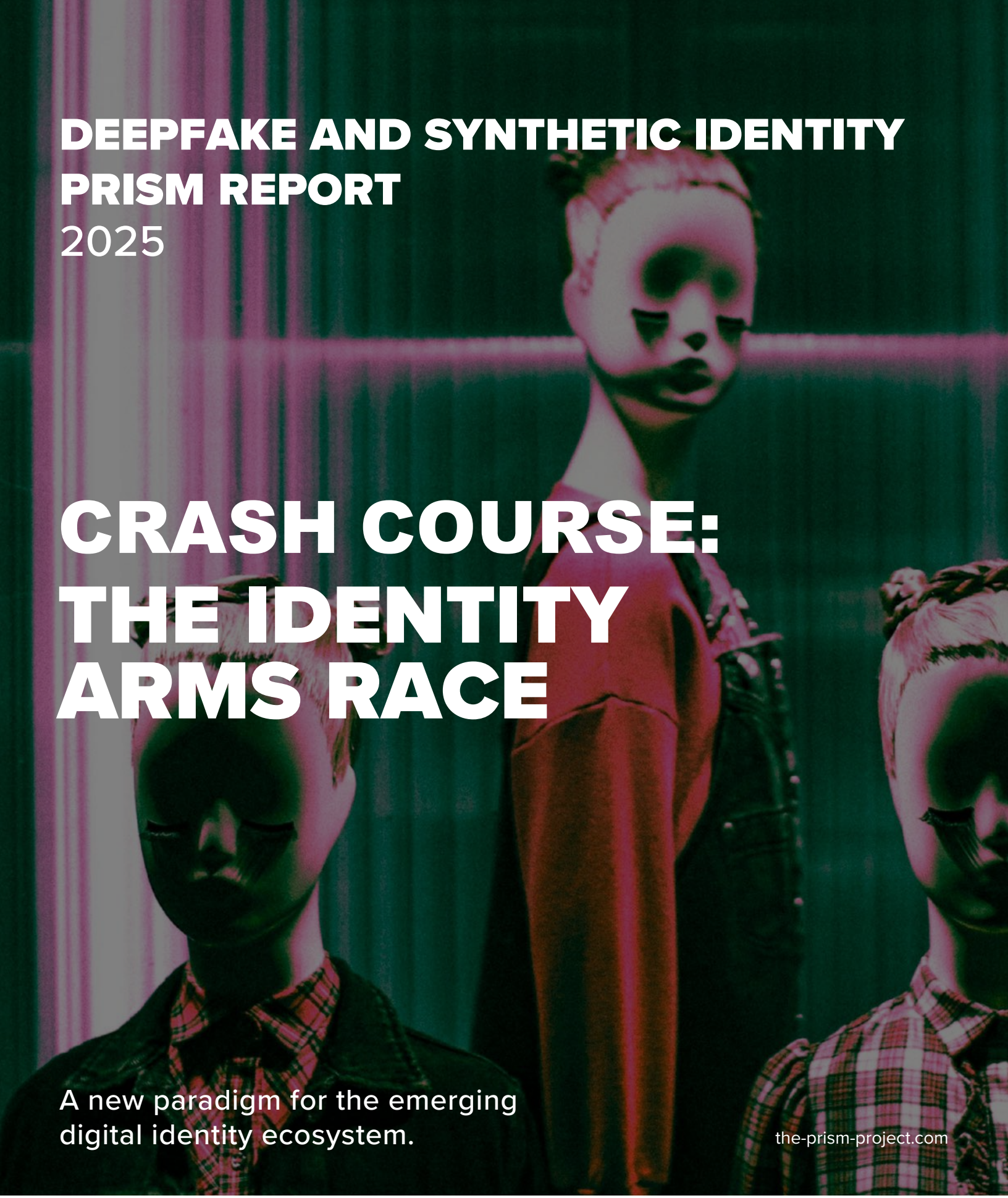

DEEPFAKE AND SYNTHETIC IDENTITY PRISM REPORT

2025

CRASH COURSE: 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 Deepfake and Synthetic Identity 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.

Crash Course: The Identity Arms Race

Deepfakes and synthetic identities pose an existential threat to every organization that operates through digital channels. But in order to understand why, you need to know how we got to this point in history: where real people and digital facsimiles have become indistinguishable in online contexts, opening the door to unprecedented levels of identity fraud. That story begins in 2013, when **biometrics** became a consumer product, igniting an arms race between fraudsters and the vendors protecting end users with a new class of security.

This crash course is designed to familiarize the uninitiated with key digital identity definitions and concepts and to contextualize them in the past decade of widespread digital transformation. Buckle up!

The Basic Idea Behind Biometrics and Digital Identity

In digital spaces, we don't have bodies, so our interactions are limited based on the **identity elements** we can provide in a transaction to prove we are who we claim to be. On a fundamental level there are three types of identity elements we can provide to corroborate our claim: something we know (**knowledge-based authentication** or **personal identifiable information**), something we have (token or device-based authentication, a key, or a physical ID), and something we are (biometrics).

Knowledge-based authentication is the most commonly used authentication factor, but it can be guessed, shared, stolen, forgotten, or cracked. Token or device-based authentication is analogous to physical keys. These factors can't be cracked or guessed, but they can be shared, lost, and stolen. Biometrics, however, stand apart as a stronger level of assurance.

Biometrics have long represented the pinnacle of identity elements because your face, fingerprint, or voice cannot be shared, stolen, lost, forgotten, guessed, or cracked when in template form. By incorporating biological identity elements into the non-corporeal interactions of online life, digital transactions approach the levels of trust we enjoy in the physical world. Things that used to require in-person interactions and painstaking identity checks, like opening a bank account or renewing a driver's license, can be performed remotely because the relying

Key Definitions:

BIOMETRICS: Technology that uses some kind of sensor (camera, microphone, fingerprint reader, etc.) to measure a user's unique biological trait—most commonly a face, voice, or fingerprint—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. A mathematical value that cannot be reverse engineered to recreate a representation of the original biological trait.

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.

party (a bank or DMV in this case) can trust that a user whose biometrics match the ones associated with their digital identity is authentically themselves. This is in contrast to a person with a password, or a hardware token who can only prove they are a person who knows something or a person who has something, rather than proving they are a specific person. In short, biometrics give you a body in digital spaces.

To see how that's possible, and the ways in which that concept can be undermined, it's important to understand the three phases of the biometrics lifecycle:

- Enrollment: a new user submits their biometrics for the first time, creating a biometric template that will be used as the comparison for future authentication transactions. This can be strengthened with the addition of other identity elements, like data from government issued IDs, in a process known as **identity verification (IDV)**.
- Authentication: an enrolled user submits their biometrics for the purposes of matching with a template. The user's biometrics are compared to the template and a positive match results in an authenticated transaction.
- Account Recovery: a user who has lost access to an account engages with a relying party or device in order to regain access. This can take many forms of varying assurance, from recovery codes and call center interactions, to in-person recovery processes or fully automated smartphone transactions.

IDENTITY VERIFICATION (IDV): A class of identity technology that compares a user's face biometrics to the image on an ID card (usually government issued) in order to prove a user is who they claim to be. This enables compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, and is most commonly used for remote onboarding and account opening applications.

As you can imagine, biometrics represent a problem for bad actors. While it is often combined with other factors, biometric authentication is fundamentally different from its KBA and DBA predecessors. Where the non-biological authenticators look for an exact match between strings of characters or the specific key to a lock, biometrics are probabilistic by nature. The only way to circumvent biometric security is by convincingly imitating the enrolled user.

The past decade-and-a-half has been an arms race between biometrics and digital identity vendors pursuing the goal of unimpeachable biometric authentication and fraudsters keeping pace to prevent that from happening. This is made manifest in a contest between increasingly accurate **Authentic Identity Elements** and increasingly convincing **Counterfeit Identity Elements**. Deepfakes and synthetic identities represent the apex of the fraudsters' attempts to prevent biometrics from taking hold, and if they succeed, the promise of digital transformation stands to permanently slip out of reach.

AUTHENTIC IDENTITY ELEMENTS: Biometrics, documents, and metadata that are undisputed in origin.

COUNTERFEIT 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.

The Mobile Revolution – Apple Launches Touch ID

Before 2013, online security was largely confined to knowledge-based authentication like passwords, PINs, and one-time passcodes. In some circumstances, that could be supplemented by physical tokens—something you have, like a card or FOB. This was limiting from an applications standpoint. Because things you know and things you have can be shared, stolen, and lost or forgotten, the use of a passcode or physical key did little to prove that the human being using them to assert a privilege (logging into an online account, authorizing a payment, etc.) was the actual human being entitled to that privilege. If a password was compromised or a token was stolen, then whoever had the authenticator also had the privileges it granted.

That began to change in 2013, when—after many years of early innovation in mobile technology and experimenting with biometric sensor making—Apple launched the iPhone 5S, which featured TouchID: a fingerprint sensor embedded in its home button. It wasn't the first biometric sensor on a mobile phone, but it was the first that was widely adopted, the killer application that introduced a third concept to consumer authentication: something you are.

The Apple Effect popularized biometrics as a convenient way to open a phone, putting fingerprint sensors on the radar of the average smartphone user. Samsung and LG followed course, and within a year, fingerprints were being touted as a password replacement. Software-based face and voice biometrics began to emerge, too, and we started to see a wild west of biometric authentication factors arise.

These were relatively primitive biometrics, however, and severely limited in scope.

Rise of the Spoofs – The Hacker Response

Early biometric authentication factors were an upgrade from passwords, but they had a long way to go before achieving the potential of a biological identity in an online space. These limitations can be summarized in three categories:

- Reducing to recovery codes – after a set number of failed authentications, most consumer biometrics default back to a passcode, completely negating the security of a fingerprint or face lock.
- No **biometric binding** – there was no requirement to link a

biometric to a user's personal information when enrolling on a new device, meaning that anyone could set up their own biometric on another person's device—a spouse, child, pet, or bad actor.

- Vulnerable to **presentation attacks** – each new biometric authentication feature introduced on a brand name smartphone was met by a community of hackers and security professionals ready to try and fool the sensor with presentation attacks (aka "spoofs").

While each of those shortcomings presented its own challenge—limiting the application of biometric authentication to low risk convenience-driven use cases—it was the presentation attack vulnerability that mobilized the identity community to strengthen the hardware and software used to capture biometrics.

BIOMETRIC BINDING: The act of connecting biometric data to trusted personal information on an ID in order to verify the identities of users.

PRESENTATION ATTACK: The act of presenting a counterfeit identity element to a sensor in an attempt to trigger a false positive signal, enabling a fraudster to wrongfully authenticate a transaction.

Countermeasures Emerge

In the face of presentation attacks, biometrics vendors turned to a number of countermeasures, all of which were an attempt to prove the so-called **liveness** of the data being submitted:

- Sensor fidelity – new sensors were developed to try and increase the volume and fidelity of data captured by devices. For fingerprints, this included multi-spectral imaging technology, which could scan subdermal layers of a user's digit. For face biometrics, this included using infrared sensors and 3D imaging technology, as demonstrated with Apple's Face ID.
- Test prompts – some solutions attempted to prove user liveness by issuing challenges during the capture process. This was most common with face and voice biometrics, in which a user might be asked to blink, move their face, or speak a random phrase to prove the images and sounds being submitted weren't recordings or artifacts.
- **Multi-factor authentication** – some vendors took a scaling approach to defending systems with biometrics, combining the strong authentication with a password or token factor, to essentially make breaking into a digital space too costly to be worth it.
- **Multi-modal** biometrics – layering multiple biometrics became quite popular in this regard, with face and voice frequently being combined under the logic that spoofing both factors would be too onerous. Other popular combinations included face and periocular biometrics, fingerprint and heartbeat biometrics, and behavioral biometrics with any other modality.

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

MULTI-FACTOR: The combination of multiple authenticator types—KBA, DBA, and biometrics—in order to increase security, often at the expense of user experience.

MULTI-MODAL: The combination of multiple biometric types—face, voice, fingerprint, vein, behavioral—in order to greatly increase security. Some biometrics have a level of synergy together that makes the effect on the user experience negligible.

At this point, consumer facing biometric authentication was in its infancy, so these countermeasures were untested at large scales in real scenarios. That was partially due to the complex nature of early presentation attacks, which required too much effort to produce en masse. Unless a specific target was valuable enough, simply increasing the number of factors required for authentication was enough to disincentivize business-minded bad actors.

The hypothetical nature of a serious identity threat leveraging biometric presentation attacks at scale served as a barrier to adoption and a motivation to continue innovating toward maturity. But with each step forward, and each adoption milestone, the need for standardization and testing grew.

Liveness Testing and Second Generation Liveness

Standards and conformance tests began to emerge in 2016, and with them third party testing, with an early focus on detecting physical artifacts in presentation attacks. This spurred industry competition, with frontrunners emerging in the areas of face biometrics software. Third party attested compliance with liveness standards became a key differentiator in the market at first but has since been normalized to a point of being table stakes. Biometric technologies that could tell the difference between an authentic human and a spoof competed further on user experience: was a solution passive or active in its ability to detect liveness? In other words: could it just tell you were authentic, or did you have to do something special to prove it?

In both scenarios, the general idea was the same. When faced with the threat of counterfeit biometrics, vendors stacked the odds against the impostors attempting to fool their way past probability-based authentication.

The Other Side of the Equation

While biometrics were competing in the liveness wars, increased **digital transformation** and regulation created new use cases for facial recognition in particular that began to solve the issue of biometric binding. This was done by combining biometric face capture and matching technology with **optical character recognition (OCR)** and **computer vision** enabling software to compare a human face to the picture on an individual's identity document, passport, national ID, or driver's license.

Initially, the addition of documents into the identity equation brought another trusted human element enhancing security in the digital space. But just as biometric sensors were under threat of presentation attacks, so were the OCR and computer vision

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

OPTICAL CHARACTER RECOGNITION (OCR): A class of computer vision technology that enables the reading of text on documents via a connected camera on a smartphone or computer.

COMPUTER VISION: A class of artificial intelligence that emulates object recognition through connected cameras.

technologies used to capture the personal data from physical documents. Forgeries and fake IDs had become a serious problem, with crateloads being seized at ports the world over. And while they posed immediate threats in regards to human trafficking, smuggling, and under age substance abuse—which remains the primary mainstream concern over falsified documents in North America—they also threatened the integrity of the emerging identity-proofing infrastructure. If a fake ID could be used in a remote identity verification scenario with an authentic face, there could be no trust in a customer database.

Digital Transformation Demand

In spite of the emerging threats, the benefits of remote identity verification through the combination of biometric and document capture and comparison had opened up a whole new world of online services, making higher risk transactions that once required in-person interaction faster and more accessible. And in 2020, when the world was forced into remote and long-distance interaction due to pandemic health measures and lockdowns, digital channels surged. Digital identity technology was there to enable safe online interactions, and the ensuing demand caused an influx of IDV providers to rush into the space. Acuity Market Intelligence joked that a new class of IDV vendor was emerging called "**two guys and an app**."

TWO GUYS AND AN APP: A derogatory term for a class of identity verification vendor, typical in the early 2020s, that sought to capitalize on the sharp rise in demand for remote IDV solutions without any foundation in or understanding of biometric identity.

This activity was not sustainable in the long term, and the market re-regulated after a 2022-2023 crash of what Acuity Market Intelligence termed at the time "a rogue wave"—an unsustainable series of market dynamics that temporarily "lifted the boats"—of every IDV vendor regardless of the quality of their technology, solution, or ability to execute. From the relying party side of things the digitization demand didn't abate, and neither did the need for digital identity solutions.

In 2024, the Prism Project polled relying parties from travel and hospitality, financial services, and the government sector about their intersecting experiences with digital transformation and digital identity. Motivated by the promise of regulatory compliance, enhanced customer experience, and fraud protection, businesses in these verticals had already deployed solutions for employee access control and customer authentication, but were still largely considering stronger controls for onboarding—which as we will see in the following section, is the primary threat vector for synthetic identities.

The Rise of AI and the Need for Provenance

As enterprise digitalization evolved from future innovation to mainstream adoption, advanced **generative AI (gen AI)** models began to emerge. In addition to automating business processes, gen AI empowered fraudsters with the ability to scale the creation of counterfeit identity elements—including deepfakes, fake IDs, and fabricated PII—that can be used for presentation attacks. This effectively negated all countermeasures that depended on the presupposition that spoofing took too much technical expertise and time to make a viable business for fraudsters.

GENERATIVE AI (GEN AI): A class of artificial intelligence technology that can create text, images, videos, and audio media based on prompts submitted by a human user.

While the biometrics industry was continuing to focus on liveness detection to defend against deepfakes, a group of prominent organizations from the tech and media worlds took on the challenge of **provenance**. The Coalition for Content Provenance and Authenticity (C2PA) was founded in 2021 with a mission to combat misinformation and online content fraud through technical standards. C2PA is a collaboration between Adobe's Content Authenticity Initiative (CAI)—in which the publishing giant partnered with The New York Times and Twitter (now X) —and Project Origin, a coalition of news agencies and tech companies from around the globe. Its open standards enable the secure and transparent auditing of a piece of media's history.

PROVENANCE: The history of a piece of digital media. In this report, provenance is used to describe the modification history of a synthetic identity, an authentic digital identity, an identity element, or deepfake. It can also be used to describe images, video, and audio used for news, social media, marketing, and government communications.

Given the nature of digital identity, which relies on photo, video, and audio elements to represent biological and biographical aspects of a user, provenance emerges as a crucial component of trust. While C2PA is designed primarily to combat misinformation through secure manifests that provide end users with tamper evident records of every change made to a piece of media, the integrity provided by such an audit trail is indispensable when it comes to ensuring the authenticity of identity documents and biometrics. Indeed, the emergence of AI and its hostile use cases has dragged an uncomfortable truth into the light: online we are no more than the culmination of sets of media. Just like a piece of fake news, marketing, or state propaganda, human beings are subject to counterfeit practices.

Where We Are Now

That brings us to the current moment: on the verge of new digital lifestyles protected by strong identity technology while under threat of AI-empowered impostors. The rapid evolution of Gen AI has democratized digital fraud with cheap, easily accessible online tools and created a nefarious new industry—Fraud

as a Service (FaaS). Today's bad actors can leverage two of the most powerful weapons in the identity arms race—deepfakes and synthetic identities—to create increasingly complex and difficult-to-detect attacks that threaten the foundation of global digital commerce, financial services, and national security.

In the following section, we define, dissect, and analyze these threats with the intent of offering insight, perspective, and defensive guidance.

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.