2025 Digital Identity Verification Market Report & Buyers Guide

by Biometric Update and Goode Intelligence

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

2025 Digital Identity Verification Market Report

Digital identity verification plays a critical role in establishing identity in a world of increasing risks and AI-driven fraud attacks. Biometric Update and Goode Intelligence have partnered to create reports that demystify the market around the technologies that are of greatest importance to digital identity, detailing where gaps exist in how well market participants understand them.

Digital Identity verification (IDV) establishes that a person is who they claim to be and is used in a variety of situations where it is either mandated by regulation or is essential in combating fraud.

With rising levels of fraud, including AI-driven fraud, the need for IDV has become ever more critical and is leading to its use outside of the traditional onboarding scenarios. As such, IDV solutions need to be increasingly easy-to-use and inexpensive.

This report comes at a critical time for the industry with the IDV market at an important crossroads. The emergence of reusable digital identity verification, government-issued digital identity, and digital identity wallets and apps is reshaping the industry.

This Biometric Update / Goode Intelligence report explains the key concepts in digital identity verification, presenting the commercially available technologies that organizations can implement to perform it, and guiding those organizations in selecting a digital identity verification provider.

The study also investigates the market for digital identity verification products and services, including adoption examples, sector and application analysis, and three-year forecasts for transactions and revenue.

About Biometric Update and Goode Intelligence

This study has been created by a partnership bringing together Biometric Update and Goode Intelligence to produce analytical market reports stakeholders can use to make informed strategy, product and technology procurement choices.

Reports produced by the partnership are based on analysis of recent transactions and trends in the biometrics market, reviews of the regulatory, standards-development and competitive landscapes, and feedback from key insiders in each given area of focus.

Biometric Update is the world's leading source for daily news, opinion and insight into biometrics and digital identity.

Goode Intelligence is the world's leading independent biometrics market analyst and consulting firm, providing quality advice to global decision makers in business and technology.

Executive Summary

Identity verification (IDV) establishes that a person is who they claim to be. It's used in a variety of situations including digital onboarding, for instance opening a bank account, proving how old we are (age assurance), travelling (especially when travelling across international borders), applying for and starting a job (employment onboarding), joining an educational establishment, including a college or university, buying a new mobile phone, buying a new home. The list is extensive and growing.

Identity verification confirms who a user is, while authentication validates that a user is who they claim to be and authorized to access specific resources. Remote verification focuses on determining a user's true identity using official documents or biometric data, while authentication focuses on confirming a user's access to a specific system or resource, often through passwords or biometric scans. As such, identity verification is typically performed at the beginning of an interaction – when a bank account is opened, or early in a loan application – while authentication occurs repeatedly.

The identity verification market is complex and fragmented with many competing technologies being used to solve some of the issues facing digital business. Added to the complexity is the emergence of new methods with which to prove a person's identity including reusable digital identity, often held in a digital identity wallet.

The question of how we effectively and securely identify people and enable them to perform tasks in a safe and secure manner is one of the fundamental ones of our generation.

Digital identity verification answers the following questions:

1. Is it a real user?
2. Is the user alive?
3. Is it authorised to use the data it presented?
4. Can you do business with the user?
5. What is the risk of doing business with the user?

The IDV market is at an important crossroads. The emergence of reusable digital identity verification, government-issued digital identity, digital identity wallets and apps, and biometric authentication is reshaping the industry.

Identity verification is not authentication:

While the processes for biometric identity verification and authentication are similar, there are important differences in both method and purpose. Identity verification provides the **initial binding** between a person and a claimed identity, while authentication proves a claim about a **previously established** identity.

Introduction to digital identity verification

Digital identity verification as a process can differ widely across use cases, but there are basic elements common to all. In its simplest form, identity verification is a comparison that tells us a person's identity matches the identity they claim (or does not).

Boarding a plane, for instance, an attendant can hold up a passport and compare the photo to the person standing in front of them, enabling them to know that the traveler is the person who bought the ticket.

Digital identity verification takes this process onto a kiosk, a scanner or, increasingly, a mobile phone. Often, this involves a transaction between a business and a customer looking to access its services. How does the business establish a user's legitimate identity?

Many travelers will have by now encountered a customs kiosk that takes their photo and compares it to a scan of their passport. Remote work has increased the need for remote onboarding, which often takes place on a personal device, using a selfie photograph or a webcam feed. Online services and platforms, such as social media, increasingly require identity verification (often performed by confirming an email address).

The use cases for digital identity verification continue to grow, and the market diversifies in tandem. The wider ecosystem of identity verification encompasses orchestration providers, age verification services, deepfake detection, blockchain-based proof-of-personhood firms, and more.

Overall, the industry continues to move from traditional identity verification methods to more secure, convenient digital identity verification options such as reusable digital IDs. However, the core focus remains the same: how can biometrics, identity documents or other personally identifiable information prove a person is who they claim to be? And where can businesses look to for support in deploying effective, secure and reliable identity verification systems? In the end, like most matters of identity, those questions boil down to the simplest and most complex question. Who can you trust?

Who needs identity verification? KYC and beyond

Identity verification can be useful, or necessary, in government services, insurance transactions, legal activity, healthcare, travel, retail (for age restricted sales) and other sectors. In some cases, identity verification is performed exclusively to prevent identity fraud, but in many cases it is mandated by regulatory requirements. Financial services have a particular need for robust identity verification.

Typically, any high value or high stakes transaction – for example, a down payment on a property – will involve identity verification.

In a financial context, identity verification is a necessary step in Know Your Customer protocols, or KYC. KYC makes up the identity piece of anti-money laundering (AML) regulations, and as such the other components of AML, like sanctions list checks, depend on it.

AML requirements vary across different types of financial institutions, transactions and jurisdictions, but are typically enforced with fines for noncompliance.

Biometrics and identity verification

Biometrics are of value in identity transactions for the same reason they are classified as sensitive information: a biometric is by definition unique to an individual – a measurement of biology – and cannot be replaced in the manner of a password.

The primary use of biometrics in identity verification is matching face biometrics (the face being presented, either physically or digitally) with an ID document that has been scanned and authenticated. It replaces the manual process of a person visiting a physical store or bank branch to open up an account, or to buy a mobile phone on a contract, and having to provide a trusted government-issued ID that is manually scanned for authentication. In this case, the bank teller or store assistant will check that the person is alive (liveness) and that the presented face matches that on the identity document. For remote or digital transactions, this is done by scanning in the ID (OCR or chip) to check that it is genuine and then doing a selfie check against the captured ID image to verify identity.

Privacy and security considerations

Verifying personal information comes with the need to preserve privacy and provide data security protections, particularly for biometrics, which are unique and cannot be replaced; they are often encrypted for security. Identity verification vendors should provide products and services that conform to all applicable privacy laws and regulations, and employ digital safeguards to ensure any data collection, processing and storage keeps data as secure as possible from breaches and other identity fraud threats.

Laws differ across the world, requiring various measures and safeguards to ensure privacy and data security. For example, firms operating in Europe and the UK are covered by the General Data Protection Regulation (GDPR), whereas privacy laws in the U.S. vary by state. The use of algorithmic machine learning models in identity verification and the emergence of generative AI-assisted identity fraud has only increased the need for vigilance around privacy and security.

Standards and testing

International standards for identity verification exist alongside frameworks and guidelines issued at the national level.

ISO/IEC standards

The International Standards Organization has several standards covering aspects of identity verification and systems that make identity-based decisions.

The ISO/IEC 24760 series, including ISO/IEC 24760-1:2019, IT Security and Privacy, specifies a framework for the "issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations."

Online identity verification processes carried out by comparing selfie biometrics to an identity document typically rely on the ISO/IEC 19794-5 standard for image quality that supports facial recognition. This standard is also referred to in the ICAO Doc 9303 standard for machine-readable travel documents (MRTDs).

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems is "the world's best known standard for information security management systems (ISMS)" that address information risk management.

ISO/IEC 30107-3, Information technology – Biometric presentation attack detection establishes principles and methods for the performance assessment of presentation attack detection (PAD) mechanisms.

ISO/IEC 18013-5 defines the specifications for mobile driver's licenses (mDL) and their use in digital identity verification in person, while ISO/IEC 18013-7 does the same for secure online verification.

NIST digital identity guidelines and assurance levels

The U.S. National Institute of Standards and Technology (NIST) publishes the SP-800-63 Digital Identity Guidelines, which define technical requirements in identity proofing and related digital identity services.

They also include standards for different Identity Assurance Levels (IALs), which denote risk management. For IAL1, there is "no requirement to link the applicant to a specific real-world identity." A user can apply as they please and self-assert identity.

IAL2, on the other hand, denotes high confidence that a person's claimed identity is their real one. For IAL2, "evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity." In other words, IAL2 requires identity proofing, done either in person or remotely, typically through biometrics. It is the required standard for remote identity verification.

For IAL3, physical presence is required for identity proofing.

Other standards and certification

The FIDO Alliance operates an Identity Verification Certification program based on ISO standards and its own contributions, along with several related compliance programs. FIDO has accredited biometrics testing labs around the world to perform certifications for its IDV and other programs.

Injection attack detection (IAD) can provide a layer of protection against deepfakes and other synthetic or manipulated content. A European standard for IAD, CEN/TS 18099, was finalized near the end of 2024, and is already used for compliance evaluation by CLR Labs and the Age Check Certification Scheme (ACCS). This EU standard is also being used as the basis for the development of the international ISO/IEC 25456 standard.

The Kantara Initiative performs certification to the Identity Assurance Levels (IALs) defined by NIST SP 800-63 rev. 3. Kantara is also one of only two bodies currently approved for testing against the UK's Digital Identity and Attributes Trust Framework (DIATF), which governs technologies for identity verification and other types of interactions.

Advancing the State of the Art

The most significant development in identity verification in the twenty-first century has arguably been the smartphone, the mass adoption of which put powerful cameras and processors into everyone's hands. The iPhone 4, released in 2010, was the first modern smartphone to have a front-facing camera, enabling the selfie, which has become a key element of face-to-document matching models and enabled widespread mobile IDV. Smartphone cameras also put advanced document scanning functionality into standard mobile devices.

In the modern age of remote digital identity verification, to accommodate increasing demands for strong privacy and security, an ecosystem of technologies has evolved to enable businesses and individuals to securely verify identity online. The ecosystem includes government agencies and private firms, such as those profiled later in this report.

Businesses selecting an identity verification provider should consider the developers that have advanced the state of the art, because the challenge they address is a dynamic one. As such, those engaged in ongoing research and development are more likely to maintain or improve their effectiveness over time.

Many of these organizations are part of a larger shift from traditional identity verification and physical credentials to what the industry calls "reusable digital identity." This means that, instead of having to repeat identity verification for every platform and service that requires it, people can verify their identity once by registering an identity document with a third party provider, which will issue a digital credential that can be housed in a digital wallet and used for verification across platforms. New models are exploring how to leverage blockchain or decentralized ledger technology for identity verification and so-called proof of personhood.

Digital wallets specifically intended for identity verification, such as the EU Digital Identity Wallets, are joining the market. Digital wallets originally used mostly to store payment credentials or digital tickets for entry into events are also adding support for digital IDs.

Reusable digital IDs are typically shared in the form of Verifiable Credentials (VCs). VCs are a W3C-standard protocol for cryptographic attestation. This means they can be used to verify an identity that has already been established without recapturing all of the information used in the IDV process. The identity verification flow for the user is reduced to completing reauthentication and granting consent to share the VC.

Airports and airlines have been notably active in adopting biometrics and digital ID for identity verification, notably at border checkpoints. Banking and FinTech are both sectors wherein strong compliance requirements drive demand for digital IDV. Use cases exist in healthcare, law enforcement and defense and disaster relief.

Globally, identity verification is a function of national digital identity systems such as India's Aadhaar, a 12-digit unique identity number that can be obtained by residents with their biometrics and demographic data. Other significant national digital identity systems include Singapore's National Digital Identity (NDI) system and Singpass app, Estonia's eID and eHerkenning in the Netherlands.

Market Analysis & Forecasts

Identity Verification Market Analysis

This section investigates key drivers, important sectors, and applications for the adoption of IDV services, and examples from around the world.

Key Drivers

The four key drivers for Identity Verification are:

1. Compliance
2. Fraud Detection and Prevention
3. Customer Experience
4. Enabling Remote Digital Onboarding

Compliance

Compliance with AML and KYC legislation is a key driver for the adoption of identity verification services. Many regions explicitly reference the types of technology that should be adopted to ensure compliance. AML 5/6 regulation explicitly references IDV and is seen as a major driver for this market.

Fraud Detection and Prevention

IDV supports onboarding fraud and account fraud. Detecting fraudsters attempting to open an account using forged, stolen or synthetic identity and preventing fraud once an account has been opened. Financial fraud has been steadily rising and IDV can assist fraud teams in reducing their fraud exposure. Reducing the risk of onboarding a fraudster or a bad (high-risk) customer. Threats have risen dramatically as a result of AI-driven fraud including deepfakes.

Customer Experience

In today's digital-first world, customer experience is key in delivering compelling digital services. Ensuring that modern IDV services fit into customer workflow processes is a critical consideration especially in the first mile of customer experience.

Enabling Remote Digital Onboarding

The ability to support remote digital onboarding with robust, accurate, compliant and secure solutions is a must-have for service providers. Traditional IDV and, increasingly, reusable digital identity verification enables remote digital onboarding.

Key Sectors

Six key sectors are leading the way with adoption of Identity Verification:

1. Banking, Financial Services & Insurance (BFSI)
2. Government
3. Telecommunications
4. Gambling
5. Travel & Hospitality
6. Workforce (employer)

BFSI

Traditional Identity Verification: Adoption of traditional identity verification services for the BFSI sector, excluding payments, has been strongly driven by a combination of AML/KYC compliance, fraud reduction and digital transformation programs within the financial service providers.

The ability to quickly and securely onboard new customers to a financial and insurance service using smartphones has many benefits to financial service providers and fits in with the strategy of challenger banks and FinTech providers who only have a digital presence.

There is a feeling from the supplier community that a high percentage of companies in the BFSI community are actively providing traditional IDV solutions to their customers, in particular for KYC and digital onboarding. This means that growth potential in this sector may be limited and, in some cases, be restricted to removing an incumbent supplier.

Reusable Digital Identity Verification: Financial institutions, banks and payment providers traditionally have a solid trust bond with their customers and digital identity and strong authentication is the bedrock of that relationship.

There is a growing movement, kick-started by the digital identity schemes emanating from the Nordics, which sees normally competitive banks join together to offer a digital identity scheme (network) collective.

These digital identity networks usually start off by operating in a single state and can include collaboration with other sectors, in particular the telecommunications sector.

If the digital identity scheme is intended to be used to access government digital services, then this would require the backing of the government and potentially a change in the legislation.

There are regional differences in these schemes with good availability and adoption in the European regions of the Nordics (BankID) and Benelux (itsme).

Government

Traditional Identity Verification: Adoption of identity verification for governments is being driven by a number of factors including:

- Digital transformation.
- Acceleration of government digital identity schemes.
- Demand from citizens for easy access to digital services.
- Economic imperative of increasing GDP due to easy to access digital services.
- Inclusivity: Opening up government services to citizens traditionally excluded.

Governments around the world provide trust anchors for digital (electronic) identity verification. This has traditionally involved issuing citizens with physical identity documents that can allow travel across borders (passport), proof of citizenship (national identity), and permission to drive a vehicle. These trusted documents provide the trust anchor for traditional IDV.

Reusable Digital Identity Verification: For government reusable digital identity verification, we are seeing two trends:

1. Governments issue digital replicas of existing identity documents:
   a. Mobile driver's licenses
   b. Digital travel credentials
   c. Digital national IDs
2. Governments, or third parties within a certified framework, issue new digital identities for use in the digital world

There is significant activity around the world with governments seeing the benefit of issuing and accepting reusable digital identity verification.

Telecommunications

The GSMA's Mobile Connect programme has been an important catalyst for the use of digital identity for the telecommunications industry and beyond.

Telecommunications providers are also working in conjunction with governments and commercial identity providers in supporting a wide range of schemes.

Mobile Network Operators are similar to banks in that they manage a significant amount of verified identity data that can be valuable when verifying a person's identity. This includes name and address, and age.

Identity fraud, national regulations on ID registration (KYC and Anti-Terror) when activating new subscriptions and SIM-Swap prevention are major drivers for adoption of IDV for telecom operators.

This is a sector that has been traditionally a heavy user for face-to-face identity verification where a new subscriber (customer) will be required to present a combination of government-issued identity documents and proof of address credentials (often copies of utility bills). The telecom operator office or shop will use hardware (readers) to verify identity documents with a high level of accuracy and security. These can be either operated by telecom operator staff, or provided by self-service kiosks, see below. The readers support infra-red (IR) and ultraviolet (UV) light that is considered to be at a higher level than a remote check using a smart phone as it can detect some of the covert security print characteristics found on many ID documents.

However, things are changing, and telecom operators are now starting to adopt remote traditional identity verification to provide convenient 'at home' identity verification.

Telco operators also have a critical role to play in providing identity intelligence for identity verification services. Both device and network intelligence are important components for identity verification and can significantly improve accuracy rates.

In November 2020, the major UK mobile operators, EE, O2, Three and Vodafone collaborated to launch ***NumberVerify (NV)***, an API to verify mobile phone numbers for businesses. Number Verify helps with the fight against fraud by verifying customers through matching phone numbers used in a web or app session to ensure the details being provided are the same registered on the customer's account. This will help businesses be confident that the customer's identity is genuine and reduce fraud whilst still preserving their privacy. The service is provided by accredited partners that include Prove, Boku and IDlayr.

France announced a similar initiative in December 2024. France's four major mobile operators, Bouygues Telecom, Free, Orange, and SFR, announced a joint initiative to strengthen digital identity protection and combat online fraud. The collaboration is part of the global GSMA Open Gateway initiative, which seeks to standardize network-based services for developers and enterprises worldwide. The operators have introduced two APIs, KYC match and SIM swap, based on the CAMARA standard, designed to unify specifications across mobile networks. The service APIs are accessible via the CAMARA repository, an open-source project developed by the Linux Foundation.

Workforce

Identity verification for the workforce is the process of confirming that an individual is who they claim to be for employment purposes. This involves verifying their claimed identity and is crucial for security, preventing fraud, and ensuring compliance with regulations.

This is especially important for highly regulated, highly secure, and highly qualified (needing professional qualifications in order to do their job, e.g. a medical doctor).

It is an area of increasing importance where the threat of deepfakes and identity theft is causing alarm for employers, especially those hiring remote workers in foreign countries.

Two deepfake interviewees

Source: Palo Alto Networks' Unit 42

In April 2025, a news story ran that detailed the risks of not doing adequate identity verification for new hires. It was discovered that North Korean IT workers are using deepfake technology to create synthetic identities for online job interviews aimed at securing remote work. This identity manipulation is part of ongoing state-sponsored employment scams aimed at infiltrating US and other organisations globally for malicious intent. The story was discovered by researchers at Palo Alto Networks' Unit 42 who documented a case study involving a Polish AI company that encountered two separate deepfake candidates. Interviewers suspected the same individual operated both personas, particularly when the operator showed notably increased confidence during the second technical interview after previously experiencing the interview format and questions.

With the easy availability of deepfake creation tools, organisations must ensure that they employ robust and secure technology that can detect and prevent these kinds of AI-driven fraud attacks.

Palo Alto Networks Unit 42 recommends the following to prevent these deepfake attacks:

- Implement a comprehensive identity verification workflow that includes:
  - Document authenticity verification using automated forensic tools that check for

security features, tampering indicators and consistency of information across submitted documents.

- ID verification with integrated liveness detection that requires candidates to present their physical ID while performing specific real-time actions.
- Matching between ID documents and interviewee, ensuring the person interviewing matches their purported identification.

Gambling

Identity verification for the gambling industry is being driven by a combination of AML/KYC regulation, age verification checks, digital transformation to support streamlined customer onboarding and fraud reduction.

Regulation for KYC and AML is not as strong as for financial institutions and as such, there has so far not been the high levels of adoption for traditional IDV seen for the BFSI sector.

However, a raft of children's online protection regulation, including the UK's Online Safety Act (OSA), enforcing online service providers to put in safety controls to protect children could lead to greater levels of IDV adoption for online gambling.

This in combination with gambling regulators legislating for identity verification, especially age verification.

Travel & Hospitality

The travel and hospitality sector has seen strong demand for identity verification services as a result of rapid increase in digital transformation projects.

For travel, there is also a taste for the use of reusable digital identity verification with projects combining ICAO conformant digital travel credentials (DTCs) with Verifiable Credentials (VCs). We shall examine that use case in the next section on reusable digital identity verification adoption.

Travel and Hospitality has proven to be a leading adopter of reusable digital identity verification with solutions managed by both governments and private companies, including travel operators (airlines, airports, sea operators including cruise line operators, and rail operators).

A combination of global standards, in particular ICAO DTC, and travel industry body involvement, including IATA One ID, is facilitating the adoption of portable reusable digital identity that can be used for verification purposes.

The hospitality industry is a broad category of fields within the service industry that includes lodging, food and drink service, event planning, theme parks, travel and tourism. It includes hotels, tourism agencies, restaurants and bars.

Key Applications

Identity Verification (IDV) is used in many ways and by many companies across a variety of sectors.

The prime reason for using IDV is for account registration and onboarding. Onboarding customers and citizens when opening new accounts. Often, this is mandated by AML and KYC regulation.

The level of IDV applied by organisations is often directly related to the strength of AML/KYC regulation and how strictly it is enforced.

With rising levels of fraud, including AI-driven fraud, the need for IDV has become ever more critical and is leading to its use outside of the traditional onboarding scenarios. As such, IDV solutions need to be increasingly easy-to-use and inexpensive.

There are many reasons why organisations choose to deploy IDV solutions. The following seven application examples for IDV highlight the popular, the emerging, and the not so obvious.

Key applications include:

1. **Account Registration**: When creating new accounts for online services, identity verification ensures legitimacy and prevents fraud.
2. **Customer Onboarding**: Businesses verify identities to comply with regulations and prevent fraudulent transactions.
3. **Employment Screening**: Employers confirm the identity and qualifications of job applicants.
4. **Government Services**: Identity verification is required for accessing services such as tax filings, social benefits, and voting.
5. **Financial Transactions**: Banks and financial institutions use identity verification to prevent money laundering and fraud.
6. **Company Registration**: In the UK, recent regulation ensures that individuals must verify their identity to set up, run, or control a company.
7. **Digital Signatures**: Identity verification ensures the authenticity of e-signatures and digital agreements.

Account Registration and Digital Onboarding

Identity verification is commonly used for account registration and customer onboarding.

Account registration refers to creating new accounts for online services, identity verification ensures legitimacy and prevents fraud.

For customer onboarding, businesses verify identities to comply with regulations and prevent fraudulent transactions.

Account registration and customer onboarding are umbrella terms that cover a number of business processes associated with a potential customer or citizen signing up for a service or opening-up an account.

There has been an unprecedented move towards delivering services digitally under the umbrella of digital transformation. With rising levels of digital transformation, comes risk. The need to quickly stand-up digital services has proved to be challenging for many organisations. As businesses have taken their customer activities and conversations online, they need assurance that they are dealing with legitimate people, particularly with increased digital threats and attacks on digital platforms becoming commonplace. There has been an exponential rise in fraud and

2024

76 PERCENT INCREASE IN ACCOUNT TAKEOVER

cyberattacks, largely the result of AI-driven fraud.

AI-driven fraud is a growing problem where fraudsters will use AI tools to create sophisticated phishing attacks that are harder to detect. The fraudster doesn't even need to know the native language of the target as AI will create hard-to-detect phishing campaigns that can fool even the best-trained people. The financial impact of ATO fraud is significant and rising. For the UK online and according to Cifas, account takeover cases skyrocketed, up 76% in 2024, with over 74,000 cases recorded. Mobile phone accounts were a primary target, making up 48% of all filings, with the telecoms sector recording a 105% overall rise in cases of account takeover. Meanwhile, unauthorised SIM swaps increased by a staggering 1,055%, with almost 3,000 cases reported affecting mobile providers.

Digital onboarding is growing rapidly, with businesses increasingly adopting technology to streamline customer and employee onboarding processes. According to Statista, **72% of companies** now use digital onboarding tools.

Employee Screening / Onboarding

As remote digital onboarding becomes the standard for account registration and opening, the same trend is extending to employee screening and onboarding processes.

Remote employee screening is the process of evaluating job candidates virtually, without in-person interactions. It typically includes:

- Identity and background checks to verify a candidate's credentials.
- Virtual interviews using video calls to assess skills and cultural fit.
  - Online assessments for technical skills, cognitive abilities, or personality traits.
  - Reference checks conducted remotely to validate past work experience.
  - Digital right-to-work verification to ensure compliance with employment regulations.

With the rise of remote work, companies are refining their screening methods to ensure they hire reliable and qualified employees.

It is a vital area of hiring and employment with research from software provider Buffer claiming that remote onboarding programs increase staff retention by 20% with virtual processes accommodating flexible work models.

Remote employee screening does have its risks if robust identity verification is not employed. In April 2025, it was reported that North Korean state operatives are using deepfakes to get employment, particularly targeting IT jobs.

In addition to proving that a person is real, robust IDV could also be used to prove employment history and qualifications. This is where the use of digital identity wallets and Verifiable Credentials could revolutionize how companies check the validity of a new employee's claims.

Government Services

Identity verification is required for accessing services such as tax filings, social benefits, and voting ensuring that the correct citizen is signing up for digital government services.

IDV is also a major component in applying for government identity, including national identity, driver's licenses, and passports.

The push for citizens to interact with government through digital services is a major one for governments around the world.

It is leading governments to initiate major digital identity schemes and programs that support secure identity verification and authentication.

This includes India's Aadhaar program. Aadhaar is India's unique identification system, managed by the Unique Identification Authority of India (UIDAI). It assigns a 12-digit unique number to residents, linked to their biometric and demographic data. Aadhaar is widely used for identity verification, financial transactions, and government services and is available as an identity card and as digital variant, (e-Aadhaar). In 2023, it was reported that 99% of the population of India had signed up to Aadhaar (approximately 1.4 billion people).

The European Union's (EU) digital identity program incorporates digital identity wallets coupled with digital signing capabilities built around eIDAS 2.0. eIDAS 2.0 is the updated version of the Electronic Identification, Authentication, and Trust Services (eIDAS) Regulation, which establishes a framework for secure digital identity and trust services across the EU. It aims to enhance the original eIDAS regulation by introducing a European Digital Identity Wallet, allowing citizens and businesses to securely store and share identity credentials online.

Government services IDV aims to move towards citizens holding identity documents and identity attributes in digital wallets or in apps that have digital wallet capabilities, i.e., the ability to share (prove) identity and identity attributes with digital service providers in a secure repeatable way.

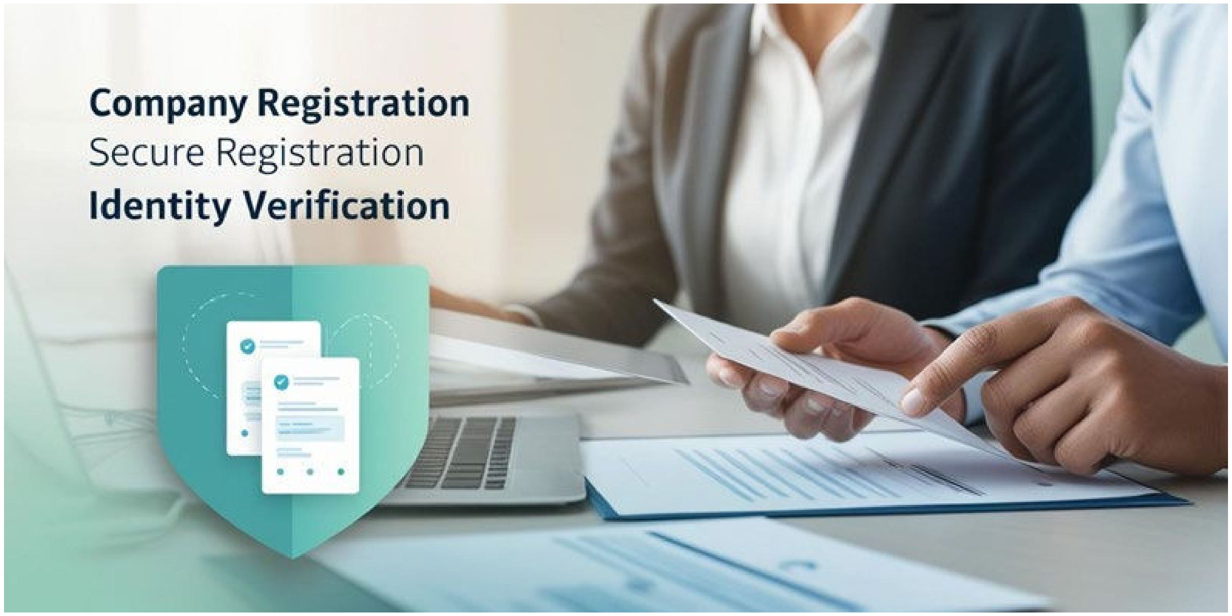
Financial Transactions

Identity verification services are very popular for the financial services industry, in particular to support new account registration and onboarding.

In addition to the use of IDV for new account registration and onboarding, banks and financial institutions are using identity verification to prevent money laundering and fraud by being applied throughout a customer's journey.

Typically, a customer's biometric will be captured during the account registration / onboarding stage and then this will be used for verification at different stages of a customer's journey. This can include being applied to verify identity for higher risk / higher value transactions but can also be used to support security for account management tasks, including device rebinding, password reset, contact centre interaction and changing personal details including change of address and name.

As biometric authentication and identity verification becomes more familiar to use for financial institutions, then it is being adopted in more parts of the workflow.



Company Registration

A single fraudulent company registration can create a cascade of financial crime. For example, it can be used to trick individuals out of cash because they wrongly assume that any company on the register is legitimate. It can also be used to obtain loans and overdrafts from banks, and even government grants.

In the UK, recent regulation ensures that individuals must verify their identity to set up, run, or control a company.

In the UK, company registration is managed by Companies House. Fraud on Companies House has been a significant problem, and the consequences for consumers can be serious. In 2023, 10,000 people applied to have their address removed from the Companies House register; after discovering it was being used without their consent.

Between April 2021 and April 2022, Companies House received 2,432 applications for removal by directors who have 'not consented to act', an increase of 59% in three years.

Even more common is the use of unconnected addresses, often residential homes, as a company's registered address. There were 10,387 applications in 2021-22 to change a company's 'disputed registered office address'. This number has tripled in three years.

Putting down incorrect names and addresses means police and debt collectors have nowhere to go when the alarm is raised.

To counteract this fraud, Companies House has decided to make identity verification compulsory. Changes to identity verification requirements for company directors, and individuals with significant control, come into effect from 8 April 2025 on a voluntary basis. Mandatory ID verification comes in for new appointments and incorporations from autumn 2025, which also marks the start of a 12-month transition period for existing directors to complete ID verification. This is covered by the Economic Crime and Corporate Transparency Act 2023 (ECCTA).

Digital (Electronic) Signatures

Identity verification ensures the authenticity of e-signatures and digital agreements.

Identity verification for digital signatures ensures that the signer is who they claim to be, adding security and authenticity to electronic documents.

Digital signatures use cryptographic techniques to verify the integrity of a document and the identity of the signer.

In the EU, Qualified Electronic Signature (QES) requires identity verification. It is the most secure and legally binding type of electronic signature, equivalent to a handwritten signature under the eIDAS Regulation in the EU.

To obtain a QES, the signer must prove their identity through a Qualified Trust Service Provider (QTSP), which verifies and stores their personal data. This process often involves face-to-face verification or an equivalent method before issuing a qualified digital certificate.

Identity Verification Forecasts

Introduction

Market forecasting is very important in the Goode Intelligence (GI) research and analysis methodology especially when dealing with new or emerging markets and products.

GI has an excellent track record of forecasting in emerging technology areas including correctly predicting the growth of the mobile as an authentication device in 2009, the emergence of biometrics on mobile devices in 2011, and the growth in digital identity in 2015.

Market forecasting is one of the tools that GI uses in predicting the degree of success a new product or service will enjoy in the marketplace. The GI methodology considers areas such as *product awareness*, *distribution*, *price*, *fulfilling unmet needs* and *competitive alternatives*.

The forecasts are taken from the Goode Intelligence Identity Verification (IDV) Market & Technology Analysis & Forecasts 2025-2030.

» **Identity Verification checks include** both traditional identity verification checks (based on scanning a government-issued identity document, e.g., passport, driver's license, or national identity card) and reusable digital identity verification (including identity credentials and Verifiable Credentials stored in digital identity wallets / apps, and biometric identity verification).

GI creates forecasts by gathering data from diverse sources like company filings, economic reports, and direct interactions (interviews) with both suppliers and buyers, some of which are bound by NDAs. GI then applies both quantitative methods and qualitative assessments (such as expert opinions) within financial models. These models are designed to estimate future performance by incorporating macroeconomic factors, industry trends, and company-specific details to provide a comprehensive view of expected growth and profitability

Revenue forecasting at Goode Intelligence (GI) involves collecting data from a variety of sources such as company filings, economic reports, and interviews with suppliers and buyers, often under NDA. This information feeds into financial models that use both quantitative and qualitative methods, including expert opinions, to project future performance. These models consider macroeconomic factors, industry trends, and company-specific details.

For revenue projections, GI calculates an average price, taking into account the variability in vendor pricing and potential discounts. The result is a comprehensive estimate of expected revenue growth and profitability for new or emerging products and markets.

We always welcome feedback from readers on the accuracy of the forecasts and are open to reflecting your opinion in future reports.

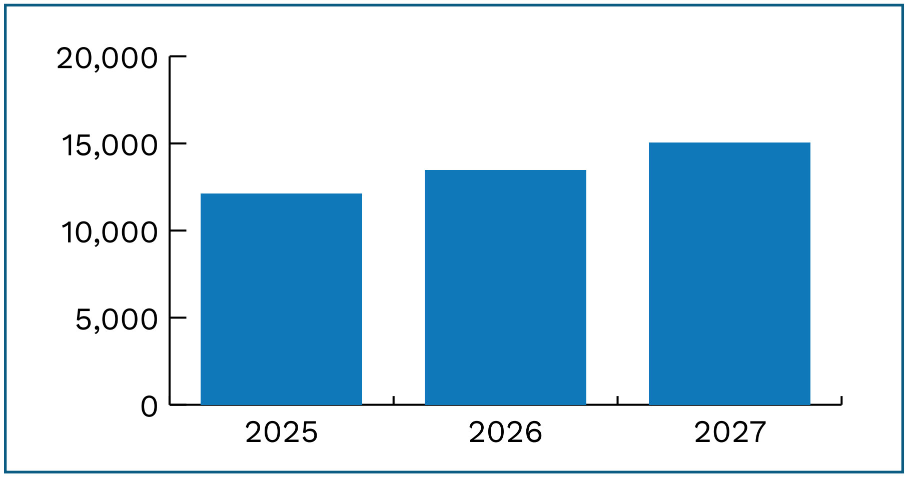
There are three-year forecasts, 2025-2027, covering:

1. Total Identity Verification Checks
2. Total Identity Verification Revenue

Identity Verification Forecasts – Checks

These forecasts are for total global identity verification checks made annually.

Chart 1: Identity Verification Forecasts: Total Global Checks (m)



Source: Goode Intelligence © 2025

Table 1: Identity Verification Forecasts: Total Global Checks (m)

	2025	2026	2027
Total	12,128.88	13,470.95	15,057.54

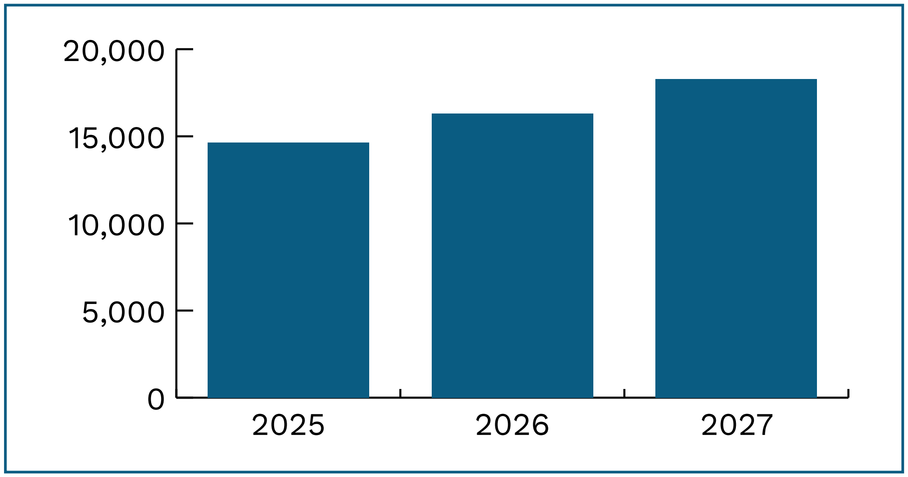
Source: Goode Intelligence © 2025

Total Identity Verification Checks will exceed 15 billion annually by 2027

Identity Verification Forecasts – Revenue

These forecasts are for total global Identity Verification revenue in US Dollars (million).

Chart 2: Identity Verification Forecasts: Total Global Revenue (m)



Source: Goode Intelligence © 2025

Table 2: Identity Verification Detection Forecasts: Total Global Revenue (US$m)

	2025	2026	2027
Total	14,637.45	16,309.69	18,292.89

Source: Goode Intelligence © 2025

Identity Verification Revenue will exceed $18.29 billion by 2027

Identity Verification Buyer’s Guide

This section provides potential buyers of Identity Verification products and services with a guide to how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing identity verification solutions as that is based on an organization’s individual and specific requirements that should be included in a comprehensive assessment.

The buyer’s guide also includes a list of Identity verification vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strive to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a “best efforts” basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

Common Terms and Definitions

Biometric

A unique, measurable biological feature of an individual. Commonly used biometrics include fingerprint and face (both used to unlock phones). In identity verification, biometrics usually means face biometrics, or the capture and measurement of an individual's facial geometry. Also see Selfie.

Compliance

Adherence to applicable rules and laws; in digital identity, this encompasses international standards, local laws and regulations, and rules on the organizational level.

Deepfake

A piece of fake or altered digital media created using artificial neural networks, deep learning algorithms and other generative AI technologies, typically used to impersonate an individual.

Digital ID

A digital identity document, such as a mobile driver's license (mDL).

Digital identity

The aggregate identity of an individual as defined by digitally encrypted data and other digitized information.

Digital travel credential (DTC)

A travel credential in a digital format that conforms with the specifications established by the International Civil Aviation Organization (ICAO). A DTC can replace a physical passport.

eIDAS

eIDAS stands for electronic Identification, Authentication and Trust Services. It is an EU regulation with the stated purpose of governing electronic identification and trust services for electronic transactions. It was amended in 2024, leading to the term eIDAS 2.0.

ID

Identity document, such as a driver's license or passport.

Identity Verification

The process of establishing that a person is who they claim to be, typically using identity documents.

IDV

See Identity Verification.

KYC/AML

Know Your Customer and Anti Money Laundering, protocols to protect businesses from financial fraud.

Liveness

The quality of being alive, and therefore a real person and not a digital fake. **Liveness detection** is a key part of remote identity verification, in that a system must be able to confirm that the media presented to it shows a genuine human user. Historically referred to as Presentation Attack Detection (PAD).

Reusable Digital Identity

A digital credential, issued by a verifying authority such as a government or third party provider, that can be stored in a digital wallet and used to verify identity across platforms, eliminating the need to repeat identity verification for every service requiring it.

Selfie

The ubiquitous digital self-portrait enabled by the development of two-way smartphone cameras. Selfie biometrics refers to facial images captured with a front-facing camera and used to match against documents or templates.

Verifiable Credential (VC)

A specific way to express a set of tamper-evident claims and metadata made by an issuer to cryptographically prove provenance; examples could include a driver's license or an education certificate.

Wallet

Also called a digital wallet or digital identity wallet. A mobile app that holds digital versions of ID, payment cards, loyalty cards and other credentials. Apple, Google and Samsung all make widely used wallets. In the EU, member countries are mandated to offer citizens a digital identity wallet by 2026.

What do you look for in an Identity Verification supplier

This section provides a guide for buyers in what to look for in an Identity Verification supplier.

It is important to repeat that this guide should not be used as the sole method for assessing identity verification solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

This report identifies the following baseline criteria for measuring whether an identity verification solution or product is suitable.

1 **Cost:** Does it meet your budget expectations? This is especially important when dealing with suppliers that charge per transaction, which is often the case. If you are entering into a per transaction contract, have you sized your requirements for now and for future growth and does your budget meet this?

2 **Accuracy and Speed:** The software should have high accuracy (low false positives and false negatives) and be able to process physical documents and identity data quickly.

3 **Liveness Compliance:** Is it a certified / tested product? The main standards for testing liveness detection are the ISO/IEC 30107-3:2023 standard and certain FIDO certifications. This is considered to "table stakes" when assessing whether a face liveness detection solution is effective.

4 **The Extra Mile:** Does the supplier 'go beyond' ISO/IEC 30107-3:2023 and FIDO certifications? Can the solution detect deepfakes and injection attacks, and what steps are being taken to detect and prevent the latest spoof attacks?

5 **Deepfake Detection:** Deepfakes are created using various methods (e.g., face-swapping, face reenactment, GAN-based generation). Ensure the solution detects these different approaches.

6 **Bias:** Ensure the solution has been tested for bias and is fair in its analysis of different types of presented biometric data.

7 **Reusable Digital Identity Verification:** Does your supplier support next generation reusable digital identity verification including support for government-issued or certified digital identity including EU Digital Identity and EIDAS 2.0, Mobile Driver's Licenses (mDL), ICAO Digital Travel Credentials, bank identity schemes such as BankID, digital identity wallets and apps supporting W3C Verifiable Credentials (VCs).

8 **Trusted Identity Data Signals:** Does the solution support trusted identity signals supplied by trusted sources including mobile network operators, banks, or credit reference bureaux's.

9 **Security:** Does the supplier have cybersecurity certifications and adhere to cybersecurity guidance / best practice?

10 **User Experience:** The ability to fit in with your usability (UX) requirements is an important consideration when choosing an identity verification supplier.

11 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

12 **Integration / Orchestration:** Check whether the solution can be easily integrated into existing systems and workflow (orchestration).

Vendor Profiles & Case Studies

Biometric Update and Goode Intelligence have identified approximately 50 vendors that provide identity verification technologies. Identity verification solutions combine a number of core technologies including face verification, liveness and deepfake detection, document scanning (optical and chip-based) and authentication, and personal data verification. The industry is made up of both component suppliers and also platform providers that own much of the IP offered in their solutions. As more countries offer their citizens the opportunity to have digital identities, in addition to physical identity documents, often stored in digital identity wallets, the methods in how identity verification takes place changes. As the pace of government-issued digital identity quickens, It is important that traditional identity verification solution providers support digital identities as part of their orchestrated end-to-end offering.

Innovatrics

innovatrics.com
sales@innovatrics.com
Tomášikova 64
831 04
Bratislava, Slovakia +421 2 2071 4056

Independent EU biometrics provider Innovatrics develops high-performance, multimodal biometric solutions and industry-leading identity verification technology used by governments, businesses and law enforcement agencies to keep people safe, onboard new customers and build institutional trust. Its full technology stack, developed in-house, includes biometric face verification, liveness detection and video injection detection, deepfake detection, document verification, autocapture components and mobile palm verification.

Innovatrics provides support for biometric identity management, criminal investigation, civil identification, identity fraud prevention, biometric voter registration, digital onboarding, NFC verification, identity management platforms, identity verification as a service, and OEM solutions, among others.

Founded in 2004, the firm is headquartered in Bratislava, Slovakia, but has offices in the U.S., Brazil, Saudi Arabia, Taiwan and Singapore, with a research and development facility in the Czech Republic. It claims its head offices are “the most biometric building in the world,” a living demonstration of biometric architecture where employees require no physical credentials at all. It is among the first firms to launch mobile palm recognition technology, which requires only a mobile phone or an IP camera for verification and identification.

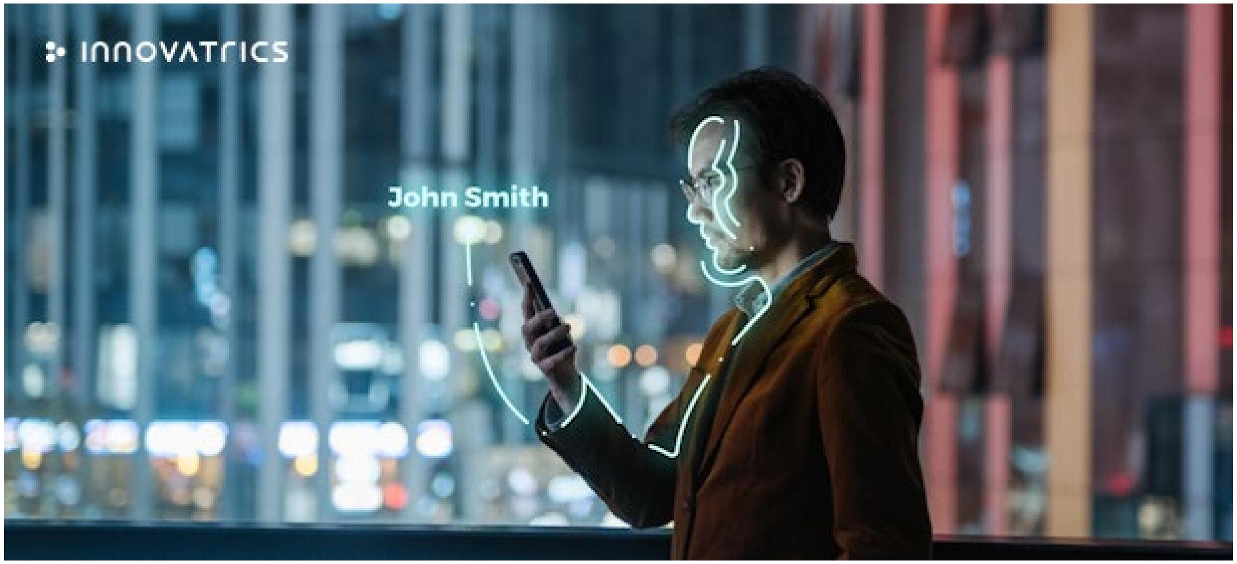
Innovatrics processes around 200 million IDV transactions per year for clients from a variety of sectors; notable names include Vodafone, Erste Group, Signicat, Home Credit, and Banco Estado. It also has partnerships with HID, Veridos, Credence ID and Precise Biometrics, among others. Its solutions are used in more than 80 countries, benefiting more than a billion people worldwide.

Innovatrics’ biometric recognition algorithms consistently rank among the fastest and most accurate across fingerprint, face and iris modalities. Its face comparison algorithm is the second best in the world according to NIST’s FRTE 1:1 test, with a false non-match rate (FNMR) of just 0.002 at FMR 10-6 (mug-shot dataset). The firm’s passive liveness detection tech is fully compliant with ISO 30107-3 standard (Level 2), and APCER 0%, according to iBeta independent testing. Its age estimation algorithm has the lowest mean absolute error across all categories according to NIST FATE AEV results, with 94% of users able to verify their face using auto-capture component in less than 15 seconds and 92% of users able to verify their ID document using auto-capture component in less than 30 seconds.

Innovatrics Powers Signicat's EU Remote Identity Proofing

Norway-based Signicat provides digital identity services across the EU, where clients demand remote identity proofing with legal validity equivalent to in-person checks. To comply with eIDAS regulations and SEPBLAC's anti-money laundering requirements in Spain, Signicat needed to upgrade its patented VideoID platform. The original in-house biometric check was functional but lacked the scalability, configurability, and robustness required for regulated use. Fraud threats such as face spoofing, deepfakes, and video injection were rising, while inclusiveness issues affected elderly and ethnically diverse users.

After evaluating alternatives from major cloud providers, Signicat chose Innovatrics to embed its top-ranked biometric face verification engine with passive liveness detection into VideoID. The integration aligned with SEPBLAC and eIDAS requirements, added configurable thresholds to balance compliance with user experience, and reinforced fraud prevention through a layered defense: injection protection, passive liveness, and deepfake detection.



The upgraded platform now supports thousands of daily verifications across the EU for banks, public administrations, and trust service providers. Outcomes are legally recognized as equivalent to in-person verification, enabling remote issuance of eIDs and qualified certificates. Benchmark-tested improvements lowered false rejection rates, boosting inclusiveness for elderly and diverse demographics while increasing fraud resilience.

"Innovatrics identity verification technology strengthened the heart of our VideoID solution, giving us the flexibility and reliability needed to strike the complicated balance between usability and security," says Silvia Lafuente, Tribe Lead at Signicat.

Ondato

ondato.com/book
sales@ondato.com
1 Canada Square, Level 39
London E14 5AB United Kingdom

Ondato is a global identity and age verification provider dedicated to preventing fraud and ensuring compliance in a complex regulatory landscape, addressing challenges from client onboarding to comprehensive databases for ongoing customer monitoring. Recognized by the Financial Times as one of the top 1,000 fastest-growing companies in Europe, Ondato leverages AI technologies to verify users globally by checking identity documents, biometrics and liveness in seconds.

A wide range of industries use Ondato’s verification solutions, spanning financial services, legal, telecommunications, online marketplaces, online entertainment and more. Major banks and fintechs that have adopted Ondato include Luminor (a leading Baltic bank), which partnered with Ondato to digitize its KYC onboarding process, and InRento (an EU crowdfunding platform), which uses Ondato to ensure investor compliance. In the telecom sector, Ondato has worked with Qatari telecom operator Ooredoo to streamline fan registrations for a global sporting event.

Ondato also supports online marketplaces like Vinted, and is prominent in the adult-content industries; platforms like OnlyFans rely on Ondato for secure age and identity verification of their creators and subscribers, and adult-oriented social site Fansly and online gambling operators such as TonyBet have integrated Ondato to strengthen KYC/AML compliance.

Ondato’s identity verification solutions achieve a 99.8% verification accuracy rate with a 97% average pass rate for customer onboarding. The U.S. National Institute of Standards and Technology (NIST) tested Ondato’s facial age estimation technology and noted low false-positive rates alongside exceptional accuracy across demographics. NIST found Ondato’s system to have “minimal bias” in results and strong consistency, which is critical for avoiding false approvals or denials across different user groups.

Ondato uses only certified third-party technologies that meet the highest industry standards. Its facial recognition solution operates under a $100,000 Spoof Bounty Program and has successfully passed NIST Level 1 & 2 PAD testing with 0% FAR. The company is eIDAS-compliant as a Qualified Trust Service component and holds ISO/IEC 27001:2013 certification for information security management. Its tools are fully GDPR compliant, with privacy and security embedded by design.

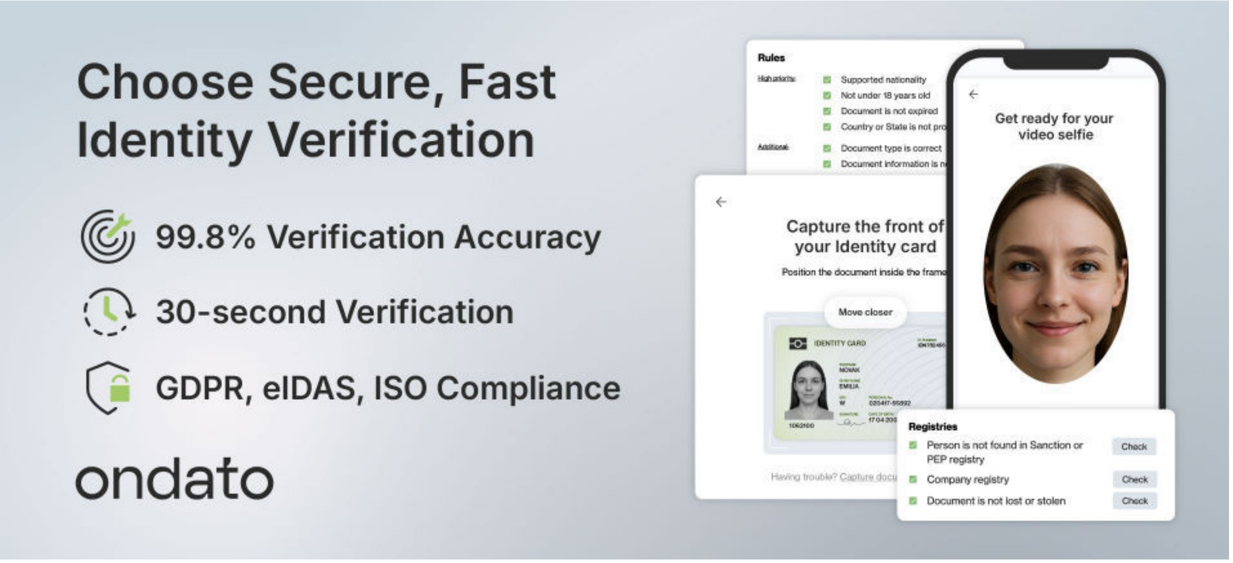
Ondato is beginning to embrace reusable digital identity verification models, launching “OnAge,” a reusable and anonymous age verification solution. Additionally, its authentication solutions for returning users indicate plans to streamline repeat identity use, preparing for a future where digital identities can be stored or tokenized and reused across different services.

How Luminor Bank Transformed KYC & AML with Ondato

Luminor Bank, the third-largest financial services provider in the Baltics, serves nearly one million customers and holds €1.6 billion in shareholders' equity. With its scale and long-term commitment to digital innovation, Luminor sought more efficient solutions for KYC and AML compliance.

Partnering with Ondato was a natural step. The collaboration began with a focus on enabling customers to open accounts remotely while meeting strict compliance and security standards. Speed, simplicity, and automation were key priorities.

The new identity verification solution allowed customers across all Baltic states to complete onboarding in under one minute. Multi-level verification ensured security and compliance: customer data and documents were automatically reviewed in registries and databases, while biometric verification compared ID photos with live images captured during the application process. This process adhered fully to legal requirements for handling biometric data.


Choose Secure, Fast Identity Verification
99.8% Verification Accuracy
30-second Verification
GDPR, eIDAS, ISO Compliance
ondato
Rules
High priority:
Supported nationality
Not under 18 years old
Document is not expired
Country or State is not pro
Additional:
Document type is correct
Document information is n
Capture the front of your Identity card
Position the document inside the frame
Move closer
IDENTITY CARD
NOWAK
EMILIA
Having trouble? Capture docu
Get ready for your video selfie
Registries
Person is not found in Sanction or PEP registry
Check
Company registry
Check
Document is not lost or stolen
Check

The result was a seamless digital onboarding journey. Customers no longer needed to visit a branch, an internet connection, electronic signature, or Smart-ID was enough to get started. After completing an application, a short video call with a bank consultant confirmed data accuracy, and accounts were activated within minutes.

By transforming customer identification with Ondato's IDV, Luminor achieved both compliance excellence and user-friendly onboarding. The solution not only streamlined KYC and AML processes but also reinforced the bank's commitment to digital-first innovation. Today, becoming a Luminor customer is faster, safer, and more convenient than ever.

Oz Forensics

ozforensics.com
Office 384, Saih Shuaib bldg 2 area,
DIC, Dubai UAE

Oz Forensics was founded in 2017 by professor and researcher Artem Gerasimov, with the objective of making digital identification safer and more convenient. It specializes in developing biometric identification and fraud prevention solutions based on facial recognition and liveness detection technologies. Today, its offices are located in the UAE (Dubai), Kazakhstan (Almaty), and Portugal (Lisboa).

The company’s solutions for combating cyber fraud and ensuring reliable identity verification are applied in over 30 countries and comply with relevant global security standards. Industries served include banks (the National Bank of Kazakhstan, Eurasian Bank), financial services and fintech, telecommunications, e-commerce and government agencies. It processes around 1.5M identity verification transactions a year, and is exploring opportunities to be involved in the EU digital wallet project.

Oz Biometry offers NIST-FRTE (Face Recognition Technology Evaluation)-tested facial recognition with 99.99% accuracy to defeat fraud effortlessly. A dual mode solution, it runs both on device and on server. Used alongside the Oz Liveness solution, it prevents the most sophisticated presentation and injection attacks, such as those weaponizing deepfakes and synthetic identities.

In 2025, it confirmed the effectiveness of its injection attack detection (IAD) technology with testing by BixeLab, which used the EU’s CEN/TS 18099 technical specification – the starter document for an ISO standard in development. Its SDK achieved a 0% APCER, meaning all attempted injection attacks were blocked.

The compliance test was performed with Oz Forensics SDK versions 8.16.2 for iOS and 8.17.0 for Android and SDK Web version 1.7.12, and confirmed the technology’s robustness in spoof detection across mobile and web browser environments. It consisted of more than 600 presentation attacks with a combination of 6 Level A and 6 Level B presentation attack instruments (PAIs).

In 2024, Oz Forensics was acquired by Brazilian digital identity unicorn Unico, which is backed by the likes of Goldman Sachs, SoftBank and General Atlantic. It retains full technical autonomy of its products and operations, and has honed its focus on core capabilities in face biometrics and liveness detection.

Paravision

paravision.ai
info@paravision.ai
San Francisco, California

Paravision builds trusted Identity AI building blocks for face recognition, liveness, deepfake detection and age estimation. Based in the U.S., the company delivers ethically developed AI software used globally for identity, security and authentication, running seamlessly across cloud, edge and embedded environments.

Paravision Face Recognition technology supports hundreds of millions of identity verifications annually through integrations with large-scale government programs, national identity systems, leading fintech companies, and payment and consumer platforms worldwide. It powers enterprise authentication for leading identity providers including ID.me, Persona, PopID, Globant, Entrust, HID, SITA and secunet. Applications span border security, national ID systems, digital onboarding, payments and access control. Together with liveness, deepfake detection, and age estimation, its facial recognition technology provides a comprehensive Identity AI toolkit known for its proven accuracy, demographic performance, and scalability.

Paravision ranks among the top global performers in the National Institute of Standards and Technology's (NIST) FRTE for 1:1 verification and 1:N identification, achieving top-5 global rankings in the July 2025 evaluations, and number one rankings across the Americas and Europe. Its algorithm demonstrates extremely low false match and false non-match rates across demographics.

Paravision also offers Liveness Detection, which has been independently tested to ISO/IEC 30107-3 standards by iBeta, achieving compliance against Level 1 & 2 presentation attacks, with a 0% Combined Error Rate at Level 2. Paravision Liveness also successfully met all criteria in the Ingenium Biometrics Level 3 PAD Evaluation, widely regarded as one of the most rigorous global tests for biometric security, confirming both outstanding spoof resistance and real-world usability. It also demonstrated outstanding performance in the U.S. Department of Homeland Security's Remote Identity Validation Technology Demonstration (RIVTD) Track 3, achieving the lowest combined error rate among all participants and the fastest overall processing time.

Paravision's Identity AI products for trusted onboarding and authentication offer flexible deployment options via SDKs, APIs, and containers.

Powering Scalable, Trusted Identity Verification Worldwide

Paravision's AI technology powers a wide range of use cases worldwide. Through its partnership with ID.me, Paravision helps enhance how Americans verify their identities.

ID.me is redefining how Americans sign in and verify their identity with a trusted, user-friendly digital wallet designed for security, privacy, and inclusivity. By leveraging Paravision's face technology, ID.me makes identity verification safer, faster, and easier for everyone. Americans rely on digital identity systems to access critical services—whether applying for government benefits, filing taxes, managing healthcare, or traveling.

Traditional identity proofing methods such as manual document review, in-person visits, or knowledge-based questions often create unnecessary barriers. By integrating advanced biometric authentication, ID.me reduces friction dramatically. Wait times are cut from days to minutes, rural and underserved populations no longer need to travel distances, and individuals with limited documentation gain access to critical services. This approach improves user experience while strengthening fraud prevention.

At the heart of this transformation is Paravision Face Recognition. By matching users to their government-issued IDs, ID.me simplifies identity proofing while meeting stringent U.S. federal authentication standards. The result is a trusted, user-friendly digital wallet that empowers citizens to access services securely and seamlessly across agencies and industries.

Ranked among the global top five in NIST FRTE evaluations, Paravision delivers high-performance, inclusive, and scalable biometric matching. Combined with Liveness, Deepfake Detection, and Age Estimation, Paravision offers a full Identity AI toolkit—helping partners like ID.me deliver secure, inclusive, and future-ready digital identity at scale

IDV Vendors Directory

1

1Kosmos

1kosmos.com

1Kosmos is a venture-backed company founded in 2018 and headquartered in Iselin, New Jersey, USA. The company offers a digital identity platform that unifies identity proofing and passwordless authentication, using advanced biometrics while safeguarding privacy via a decentralized architecture.

1Kosmos uses PAD-2 certified biometrics to detect and block deepfakes while verifying users with high assurance. Certified to NIST 800-63-3, FIDO2, and ISO/IEC 30107-3, the platform enables secure user onboarding and frictionless passwordless access. The 1Kosmos platform is delivered as a cloud service and is the only Kantara-certified full services Credential Service Provider (CSP) that is also FedRAMP High Authorized.

A

Advance.AI

advance.ai

ADVANCE.AI is a leading global provider of digital identity verification, KYC/ KYB, compliance, risk management and credit information services. It currently partners enterprise clients across banking, financial services, fintech, payment, crypto, retail and e-commerce sectors across five continents. ADVANCE.AI is listed among the World’s Top 250 Fintech Companies by CNBC.

ADVANCE.AI is part of Singapore-headquartered Advance Intelligence Group, which is backed by top tier investors SoftBank Vision Fund 2, Warburg Pincus, Northstar, and Singapore-based global investor EDBI.

Aware

aware.com

Aware, Inc. (NASDAQ: AWRE) is a proven global leader in biometric identity and authentication solutions. Its Awareness Platform transforms biometric data into actionable intelligence, empowering organizations to verify identities and prevent fraud with speed, accuracy, and confidence.

Designed for mission-critical enterprise environments, the platform delivers intelligent, scalable architecture, real-time insights, and reliable security—ensuring precise identification when every millisecond matters. Aware is headquartered in Burlington, Massachusetts.

AU10TIX

au10tix.com

Established in 2002, AU10TIX is a global leader in identity management and fraud intelligence, enhancing trust, safety, and compliance for businesses worldwide. Protecting the world’s most trusted brands, AU10TIX delivers advanced automation, identity verification, and fraud prevention.

Its future-proof solutions enable seamless onboarding in seconds while adapting to new threats and regulations. As the only 100% automated global identity system, AU10TIX detects organized fraud through traffic analysis and a consortium of 60+ companies. With deep roots in airport security, it has authenticated billions of identities and prevented over $24 billion in fraud.

D

Daon

daon.com

Headquartered in Fairfax, Virginia, with additional operations in Dublin, Ireland, and regional offices across Serbia, Australia, and Japan, Daon has been delivering digital identity solutions for over 25 years. The company specializes in engineering biometric technology and cross-channel identity assurance solutions that provide fraud-resistant digital identity verification and multi-factor authentication for customer onboarding and transaction workflows.

Daon's AI-powered platforms incorporate presentation and injection attack detection (liveness) technology to prevent bypass attempts using images, videos, masks, and deepfakes. The company's solutions include orchestration platforms, facial and voice recognition, FIDO authentication, document validation, age verification, and synthetic identity detection.

Dock Labs

dock.io

Dock Labs is a leader in decentralized identity solutions, empowering businesses to launch ID ecosystems where their partners can create, share, and monetize verifiable digital credentials.

By creating an ID ecosystem, companies accelerate customer onboarding, boost transaction speeds, and enhance overall business efficiency. Dock Labs offers a complete solution with a robust API, an intuitive web app, and secure ID wallet infrastructure, delivering everything needed for decentralized identity management.

E

Entrust

entrust.com

Entrust Identity Verification offers a suite of verifications, no-code orchestration, and AI-driven analysis to enable secure and compliant onboarding. Whether you're looking to reduce fraud, meet regulatory compliance, digitalize onboarding, we can help you verify identities in over 195 countries to help grow your business.

From streamlining interoperable digital credential issuance to providing biometric access to services, Entrust offers onboarding solutions, built in house for trusted digital government transformation.

H

HID

hidglobal.com

The HID Identity Verification Solution is a robust, AI-powered verification service for banks and financial services providers to ensure smooth identity verification for digital onboarding and beyond.

HID Identity Verification Solution helps prevent financial crimes by contributing to financial institutions' AML and KYC strategy.

F

FacePhi

facephi.com

Facephi is a global leader in digital identity verification and biometrics, trusted by over 150 financial institutions and enterprises worldwide. Our AI- and ML-driven multibiometric platform enables secure, fast, and seamless digital onboarding and authentication, fully aligned with the strictest regulatory standards (ISO, SOC2, DIACC, NIST).

With a strong presence across EMEA, LATAM, and APAC, Facephi delivers end-to-end identity solutions — from onboarding and authentication to fraud prevention — empowering organizations to build trust, enhance user experience, and fight financial crime.

FaceTec

facetec.com

Founded in 2013, and headquartered in the US with expert staff in the UK, Brazil, Portugal, Canada, and Mexico, FaceTec is a global force and leading provider of 3D Liveness and Face Verification software, providing over 3.5 billion 3D Liveness Checks annualized, bringing exceptional security levels to remote identity proofing.

FaceTec’s patented, industry-leading Certified 3D Liveness Detection and face matching, breakthrough UR® Codes, OCR, KYC, and age estimation biometrically bind unique, live, 3D users to their accounts, anchoring a secure chain of trust in the IDV process for secure and safe access to high-risk/high-value mobile and web applications.

G

GBG

gbg.com

Founded in 1989, GBG’s history in identity verification began in 2002. The company is headquartered in London, UK and is a London Stock Exchange listed company. GBG offers document and biometric security to protect remote identity proofing from deepfakes and forgeries.

Rapidly verify genuine customers on the other side of the screen with comprehensive access to trusted identity sources. Accurately and securely verify identity ownership and genuine presence anywhere with document and biometric verification. Optimise customer onboarding and outperform competitors with the identity confidence score that makes identity count.

I

ID-Pal

www.id-pal.com

Headquartered in Dublin, with offices in New York and London, ID-Pal specialises in cutting-edge AI-powered solutions that deliver real-time verification results with zero access to customer data.

ID-Pal fights deepfakes with a multi-layered approach - combining 50-point biometric facial match technology with iBeta certified liveness detection that assesses micro-variations in fraudulent techniques and award-winning document-authenticity checks to catch presentation and injection attacks globally.

iDAKTO

idakto.com

iDAKTO enables secure and seamless digital identity for banks and financial institutions worldwide. Our iDCluster platform covers the entire identity lifecycle; from enrolment to wallet creation and secure authentication, enabling instant onboarding, automate eKYC, and global compliance.

With built-in biometrics, NFC document reading, and advanced AML/PEP screening, we deliver high assurance verification with a frictionless user experience. Trusted by central banks and retail banks alike, iDAKTO powers smart identity journeys that reduce complexity and accelerate digital transformation.

IDEMIA

idemia.com

Whether you're onboarding a new bank customer, verifying benefit eligibility for a local council, or enabling age-verified access to an online gaming platform, confirming who someone is and whether they're eligible is critical. IDEMIA helps organisations build trusted identity journeys that are seamless for users and rigorous for compliance.

Our modular identity verification tools support facial biometrics, document validation, age checks, liveness detection and adaptive MFA, at configurable levels of assurance. They integrate directly into your existing onboarding and authentication flows to reduce drop-off and accelerate time-to-serve, while safeguarding against spoofing, synthetic identities and regulatory breaches.

Idenfy

idenfy.com

iDenfy develops a market-leading all-in-one platform for identity verification, fraud prevention, and compliance—designed to create a safer and more sustainable world. It has created a global digital identity verification and fraud prevention platform helping organizations comply with the ever-evolving Know Your Customer (KYC), Anti-Money Laundering (AML) regulations.

Its innovative end-to-end fraud prevention ecosystem is designed to detect and prevent cybercrime in real-time without the hassle. It uses the power of liveness detection, biometrics, business verification, and an in-house expert team to support every business' needs – from small startups to high-end enterprises.

Identomat

identomat.com

Identomat innovates seamless identity verification solutions that ensure security and trust, enabling businesses and customers to connect with confidence. It revolutionizes identity verification using advanced tech to boost security and accessibility worldwide.

Its innovative solutions create a safer, more user-friendly online environment, fostering trust between individuals and businesses. It aims to make identity verification a seamless gateway to opportunities, promoting inclusivity and connectivity in the digital realm.

Identyum

identyum.com

Identyum is an all-in-one digital identity platform that helps businesses and individuals securely verify identities, sign documents electronically, and share data with confidence. Moreover, it simplifies every step of the digital identity process.

Identify is a remote identity verification service that fully complies with AML and GDPR requirements. At its core, it relies on secure biometric checks and document verification to confirm a person's identity. In turn, this allows businesses to onboard new customers digitally and meet KYC obligations without the need for face-to-face meetings.

IDnow

idnow.io

IDnow is a leader in digital identity and fraud prevention in Europe with a mission to transform trust into the most powerful asset in the digital world, empowering enterprises with AI-driven, SaaS-based identity solutions that deliver scalable security, adaptive compliance, and real-time fraud prevention. Through its broad portfolio of digital identity and fraud prevention solutions, IDnow ensures businesses can confidently and securely operate while leveraging digital identity to drive growth, security and scalability.

The company has offices in Germany, United Kingdom, and France and is backed by renowned institutional investors, including Corsair Capital and Seventure Partners.

Iidentifii

iidentifii.com

iiDENTIFii is an award-winning face authentication and identity verification platform that distinguishes itself through its use of 3D and 4D Liveness® detection. Purpose-built for enterprises, iiDENTIFii enables frictionless, scalable customer onboarding in seconds from anywhere and on any device.

Founded in 2018, iiDENTIFii has become a trusted and proven IDV partner for major banks across the continent. The technology integrates seamlessly into existing infrastructures, including mobile and web-based platforms.

Incode

incode.com

Incode is a global leader in trust and identity and is headquartered in San Francisco with offices in Europe and Latin America.

Incode's state of the art AI platform offers a highly secure and seamless AI-based experience that eliminates fraud and drives growth. With its mission to power a world of trust, Incode works with many of the world's largest banks, fintechs, hotels, governments, and markets.

Indicio

indicio.tech

Indicio delivers everything needed to build efficient, powerful, and simple decentralized solutions for a new era of digital trust. With Indicio Proven, customers in travel, hospitality, financial services, and enterprise can integrate portable, authenticated biometric credentials into workflows, enabling seamless border crossing, rapid remote KYC, and protection against synthetic fraud and deepfakes—without storing biometric data.

Proven Verifiable Credential technology provides instant interoperability, eliminating dependence on centralized databases, passwords, or third-party providers. Trusted identities extend to connected devices, robots, and AI agents for secure interaction. Indicio makes trusted data the engine of growth, reducing friction, cutting costs, and scaling markets.

Innovatrics

innovatrics.com

Independent EU biometrics provider Innovatrics develops high-performance, multimodal biometric solutions and industry-leading identity verification technology used by governments, businesses and law enforcement agencies to keep people safe, onboard new customers and build institutional trust.

Its full technology stack, developed in-house, includes biometric face verification, liveness detection and video injection detection, deepfake detection, document verification, autocapture components and mobile palm verification.

Intellicheck

intellicheck.com

Intellicheck, the industry leader in identity verification management, prevents the use of unauthorized IDs to stop identity-based fraud. Intellicheck is the only SaaS-based validation and proofing service that uses a unique and proprietary analysis of DMV-issued IDs to create trusted, real-time customer identity verification experiences across a wide variety of sectors, both in-person and digitally. Each year, we validate around 100 million identities across North America, providing a seamless, invisible ID verification with 99.975% decisioning in under a second.

Inverid

inverid.com

Inverid, known for its NFC-based identity verification solution ReadID, delivers identity proofing by securely reading and verifying the chip in passports and ID cards. Supporting documents from over 175 countries and compatible with more than 2,700 smartphone models, ReadID ensures authenticity, prevents fraud, and offers a seamless user experience. It is used in financial services, government, and other regulated sectors worldwide.

In 2025, Inverid joined Signicat, the pan-European digital identity leader. Combining ReadID with Signicat solutions like VideoID and eID Hub creates a comprehensive portfolio that enhances compliance, fraud prevention, and customer experience, while scaling seamlessly across local and international markets.

iProov

iproov.com

iProov provides biometric identity verification trusted by the UK Home Office, U.S. Department of Homeland Security, NHS, GovTech Singapore, UBS, and more. Our fully managed Liveness service protects against presentation, injection, and deepfake attacks while delivering fast, inclusive user experiences. It's the only liveness solution conformant to WCAG 2.2 Level AA for accessible authentication.

iProov analyzes device metadata, imagery, and traffic patterns to detect threats in real time, with expert teams mitigating risks. The SDK offers two options: Express Liveness for instant verification and Dynamic Liveness for higher assurance, FIDO-certified for remote face verification.

J

Jumio

jumio.com

Jumio unites powerful identity verification with connected intelligence so you can stop sophisticated fraud, instantly recognize trusted users, and deliver a frictionless experience in seconds.

Jumio solutions are powered by the Jumio Platform and leverage biometrics, AI and the latest technologies to establish and maintain trust, from onboarding throughout the entire customer lifecycle.

L

LexisNexis Risk Solutions

risk.lexisnexis.com

LexisNexis Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe.

Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers.

Luciditi

luciditi.co.uk

Luciditi is a privacy-first digital identity platform delivering rapid, secure verification for remote users. Its mobile and web-based solution combines liveness detection, facial matching, and ID document validation (including NFC chip read) to meet UK's DIATF for Right to Work, Right to Rent, Disclosure and Barring Service (DBS) as well as AML, and KYC standards.

Designed for seamless integration, Luciditi enables frictionless identity verification for regulated sectors including finance and HR. With encrypted data sharing, passwordless authentication, and compliance-ready architecture, it empowers businesses to onboard users confidently, without compromising experience or trust.

M

Mitek

miteksystems.com

Mitek Systems protects what's real across digital interactions in a world of evolving threats. Mitek helps businesses verify identities, prevent fraud before it happens, and deliver secure, seamless digital experiences in the face of rapidly advancing AI-generated threats.

From account opening to authentication and deposit, Mitek's technology safeguards critical digital interactions. More than 7,000 organizations rely on Mitek to protect their most important customer connections and stay ahead of emerging risks.

Mobai

mobai.bio

In Mobai, we help banks, eIDs, identity providers, and their IT vendors to create greater customer journeys in multiple use cases, from onboarding to ongoing authentication of users. We tailor technology and solutions for regulated industries in need of biometrics.

With Mobai's fully remote identity proofing, users can verify their identity from anywhere using their smartphone, eliminating the need for in-person visits. For industries requiring additional security, we also offer physical ID proofing solutions. Our technology leverages biometric face matching, liveness detection, and ID document validation to ensure compliance with global security standards and prevent fraud.

O

OCR Studio

ocrstudio.ai

OCR Studio provides comprehensive AI-driven solutions for instant scanning and authentication of ID documents in 100+ languages. Using powerful OCR technology, it streamlines data extraction from passports, ID cards, driver’s licenses, and other identity documents, enabling fast verification while ensuring global compliance (GDPR and beyond).

All OCR Studio’s technologies are designed with privacy in mind. They run entirely on the user’s device, with no transfer of data to external servers or third parties. No images or personal details ever leave the device. Developers can easily integrate ID scan via SDK into web, mobile, desktop, and server environments.

Ondato

ondato.com

Ondato is a global identity and age verification provider dedicated to preventing fraud and ensuring compliance in a complex regulatory landscape, addressing challenges from client onboarding to comprehensive databases for ongoing customer monitoring.

Recognized by the Financial Times as one of the top 1,000 fastest-growing companies in Europe, Ondato leverages AI technologies to verify users globally by checking identity documents, biometrics and liveness in seconds.

P

Paravision

paravision.ai

Paravision builds trusted Identity AI building blocks for face recognition, liveness, deepfake detection and age estimation.

Based in the U.S., the company delivers ethically developed AI software used globally for identity, security and authentication, running seamlessly across cloud, edge and embedded environments.

Persona

withpersona.com

Founded in 2018, Persona is headquartered in San Francisco and is available in 200+ countries and territories. Persona’s platform offers the building blocks businesses can use to collect and verify users’ identities.

Persona develops micromodels to detect different types of deepfakes during government ID, selfie, and document checks. It incorporates these into multi-modal ensemble models to create a layered defense.

Plaid

plaid.com

Plaid powers the tools millions of people use to lead healthier financial lives. Our mission is to build a more inclusive, competitive, and resilient financial system by simplifying payments, transforming lending, and advancing the fight against fraud.

Plaid Identity Verification (IDV) lets you verify the identity of your customers and seamlessly stitches together verification methods. Using Identity Verification, you can verify identification documents, phone numbers, name, date of birth, ID numbers, addresses, and more. Identity Verification also integrates directly with Monitor for an end-to-end verification and KYC solution.

R

Regula

regulaforensics.com

Regula is a global pioneer in developing forensic devices and identity verification solutions. With 30+ years of expertise in forensic research and the world's largest identity document template database, Regula leads in document and biometric verification technologies.

The company collaborates with border controls, law enforcement, international organizations, and businesses to define and maintain compliance standards. Its hardware and software solutions handle up to one billion verifications annually across 252 countries and territories. Regula empowers over 1,000 organizations and 80 border control authorities to verify 100 million online users worldwide, delivering seamless, secure, and reliable identity verification at scale.

S

Shufti

shuftipro.com

Shufti, founded in 2017 and headquartered in London, is a unified identity and compliance platform powering secure onboarding and continuous monitoring worldwide. Trusted by 1,200+ customers across 240+ regions and 150+ languages, it verifies 10,000+ document types and screens against 100,000+ AML data sources through a single API.

Shufti's advanced AI delivers sub-30-second verifications, detects deepfakes and injection attacks, and enables transaction-level orchestration with perpetual KYC/AML. Certified to iBeta Level 2 PAD, SOC 2 Type II, and GDPR, with a 4.8/5 rating from 3,000+ consumers, Shufti helps fintech, gaming, crypto, and enterprises fight fraud, stay compliant, and build lasting trust.

Signicat

signicat.com

Signicat is a pan-European leader in digital identity solutions, offering a comprehensive platform that covers the entire digital identity lifecycle: from identity verification and authentication to electronic signatures.

With Norwegian roots and global reach, the company offers the industry's most comprehensive suite of electronic identifications, with 36 eID integrations and expanding throughout Europe. Its Trust Orchestration capabilities enable organisations to create and customise workflows by combining identity verification, authentication and electronic signature solutions. This integrated approach enables secure, compliant and seamless digital onboarding experiences, positioning Signicat as the trusted infrastructure provider for any cross-border identity needs.

Smile ID

usesmileid.com

At Smile ID, we are helping to accelerate digital Africa by making it easy to verify and onboard customers across the continent. In the eight years since we started we have verified over

150 million identities. Improve your onboarding metrics and protect your customer's accounts with biometric authentication.

Our artificial intelligence and identity verification tools have been specially designed for African faces and have a 99.8% accuracy rate. Our technology is used by fast growing companies in a wide range of industries across Africa including Chipper Cash, Paga, Paystack, YellowCard and many more.

Socure

socure.com

Socure is a leading platform for digital identity verification, compliance and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust and mitigate risk.

Socure Verify offers precise, accurate and inclusive identity verification. Automate the customer onboarding process with unrivaled data coverage and industry-leading technology that delivers exceptional customer experiences with uncompromised compliance. Its triangulated data approach leverages artificial intelligence and machine learning to verify an identity across 400+ trusted sources, and then correlates thousands of identity data points—online and offline—to resolve to a single best-matched entity.

Sumsub

sumsub.com

Sumsub is a full-cycle verification platform that enables businesses to achieve secure, scalable compliance while preventing fraud. Its adaptive, no-code solution manages identity and business verification as well as ongoing monitoring, allowing it to respond effectively to evolving risks, regulations, and market demands.

Recognized as a Leader by Gartner, Liminal, and KuppingerCole, Sumsub combines seamless integration with advanced fraud prevention to provide consistent, industry-leading performance. Over 4,000 clients, including Bitpanda, Wirex, Avis, Bybit, Vodafone, Duolingo, Kaizen Gaming, and TransferGo, rely on the platform to streamline verification, reduce risk, and support growth, following global AML standards and engaging with institutions such as the UN, Statista, and INTERPOL.

T

Thales

thalesgroup.com

Thales offers leading capabilities in the Defense, Aerospace and Cyber & Digital sectors, including developing secure polycarbonate identification documents and investing in digital products and research. Working closely with customers and local partners, Thales meets the most complex requirements for every operating environment.

In the United States, Thales has a strong history of more than 130 years, employing 5,000 people around the country. Thales Canada combines over 50 years of experience with the talent of 1,400 skilled people from coast-to-coast.

U

Unico

unico.global

Unico is the largest identity verification network in the world and a pillar of trust in digital society. With solutions based on facial biometrics, machine learning, and reinforced security layers, Unico validates with 100% certainty who is performing a transaction and the associated identity risks.

In this way, it fights frauds, protects data, and promotes trust between people and companies, contributing to building a safer and less bureaucratic world. Globally renowned funds such as SoftBank, General Atlantic, and Goldman Sachs trust and invest in Unico.

V

Veridas

veridas.com

Veridas is a global leader in identity and biometrics, delivering trusted solutions that stop fraud while enabling secure, seamless interactions between people and organizations. Headquartered in Spain and operating worldwide, Veridas provides a proprietary, AI-powered Identity Verification Platform that prevents identity fraud at scale across banking, telecom, government, and beyond.

Our end-to-end platform combines document verification, facial recognition, and liveness detection to ensure real customers are verified on the first try, across any channel. Built to the highest security and regulatory standards, Veridas empowers enterprises to safeguard trust, accelerate growth, and deliver exceptional user experiences.

Veriff

veriff.com

Veriff is a global identity platform that helps businesses build trust online. Its AI-native technology combines automation with human feedback to rapidly and accurately verify identities across 230+ countries and territories, supporting over 12,000 government-issued IDs. By analysing thousands of data points, Veriff ensures users are who they claim to be with minimal friction.

Trusted by leading companies like Blockchain, Bolt, Deel, Monzo, Starship, Trustpilot, and Webull across Finance, Marketplaces, Mobility, Gaming, and other industries. Our trust infrastructure helps businesses stay compliant, prevent fraud, protect users and scale globally, enabling a safer, more transparent internet for everyone.

W

Wink

wink.cloud

Wink connects identity with commerce to eliminate theft and payments fraud, improve usability, and empower individuals as their own authenticators. Our modular platform delivers identity verification through multimodal biometrics—face verification, palm recognition, voice authentication, and advanced liveness detection—built into login, fraud prevention, checkout orchestration, and a payment gateway with a zero-chargeback guarantee.

As agentic commerce accelerates and AI agents initiate more transactions, Wink equips partners with the tools to ensure every interaction is secure and verifiable. Anchored in Identity, Commerce, and Intelligence, Wink delivers device-agnostic solutions that scale across retail, e-commerce, financial services, and beyond.

Y

Yoti

yoti.com

Yoti's identity verification service allows your customers to remotely prove who they are with just an identity document and selfie. No matter your company's size, we're here to make verifying customers more accessible for you. Our customisable identity verification tools give you the flexibility you need to deliver the perfect balance of speed and fraud detection at exactly the right time.

Our simple UI makes identity verification a seamless process for your customers. Whether you're after our core identity verification or additional checks for enhanced security, you can be confident only genuine customers are verified.

Youverse

youverse.id

Youverse enables organizations with secure, seamless, and privacy-preserving authentication where individuals control their data and businesses control their processes, all while upholding robust security.

With Youverse, businesses can seamlessly verify customer identities, protect their operations, and enhance customer experiences. With its seamless integration and industry-wide applicability, its solutions can empower businesses across diverse sectors, from banking to hospitality.

BIOMETRIC
UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS