EBOOK

A Guide to Digital Identity Verification

The technology and trends

ENTRUST

SECURING A WORLD IN MOTION

Introduction

Businesses are under increasing pressure to create frictionless experiences for their customers. Providing always-on, digital services has opened up the pathway to growth — allowing businesses to serve customers better and, in return, increase customer loyalty.

On the flip side, fraud is growing in scale and sophistication; plus, it's never been harder to keep up with an ever-expanding list of compliance requirements. There's a growing tension between two priorities — knowing who a business is interacting with and providing fast, frictionless access for customers.

Businesses have accelerated their approach to identity verification (IDV). The identity industry itself has also made huge strides in enabling remote, digital-first interactions. But as capabilities have evolved, identity verification, fraud detection, and user experience have converged. It's no longer possible to do one without the other.

This report examines the importance of identity verification processes and their role in facilitating key business objectives: preventing fraud and enabling risk management, increasing operational efficiencies, and satisfying compliance requirements, all while meeting customer expectations and driving long-term growth.

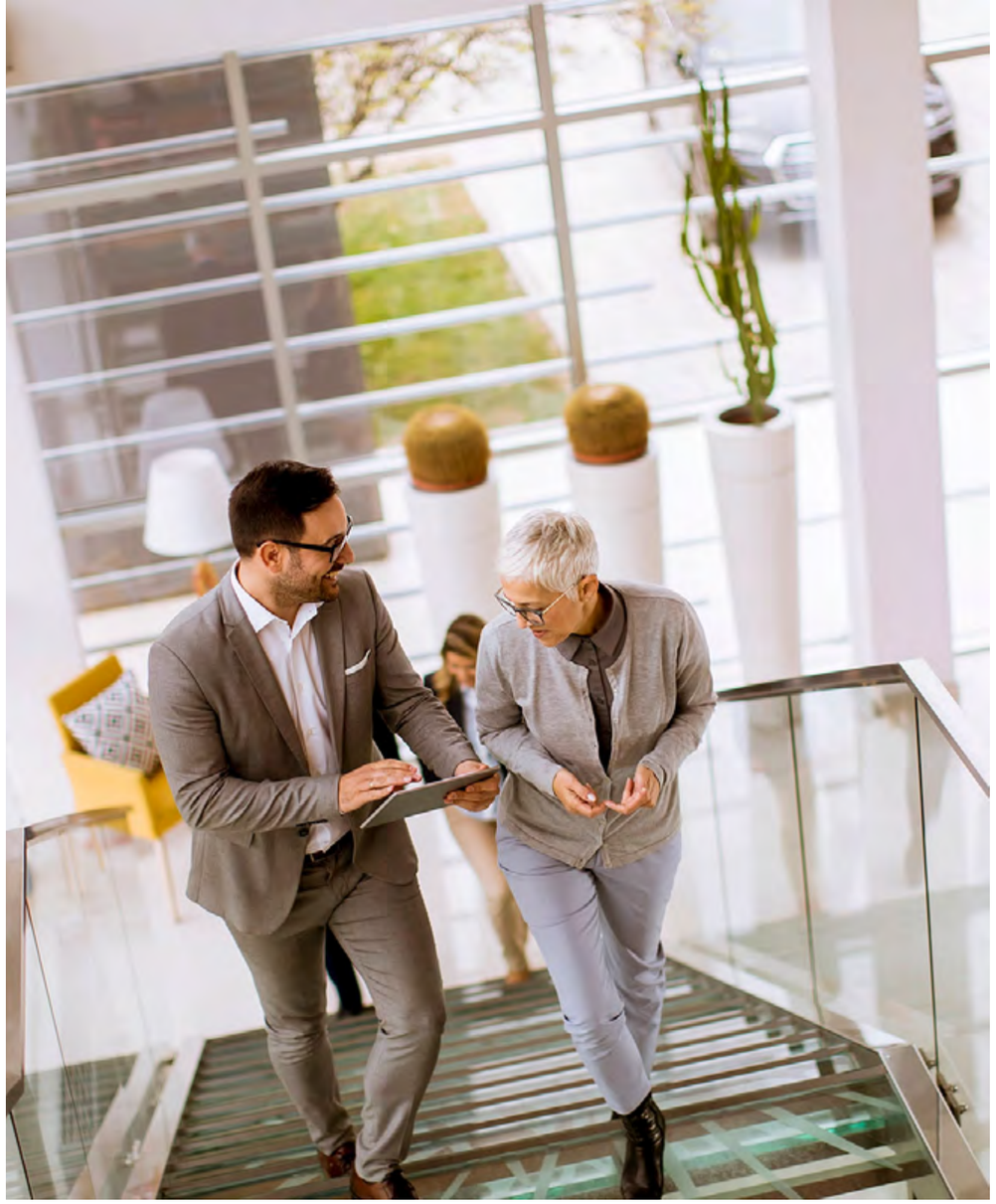


Table of Contents

The Identity Verification Landscape

Identity verification as a sector has seen immense change over the last 10 to 20 years.

It's hard to imagine there was a time when all verification was performed in person. Traditional methods typically involved multiple forms, paper files, manual compliance checks, and in-person identity verification performed in the back office, often by an untrained or inexperienced staff member.

There are several reasons why the industry moved away from manual approaches and adopted digital alternatives. The development of new technologies, the rise of smartphones, and customer willingness to embrace a digital-first way of life all created the demand for remote solutions to identity verification. Today, businesses are routinely using newer solutions — such as online form filling, data validation, document and biometric verification, and even issuing digital identity cards — to streamline their onboarding processes.

Protecting the Entire Identity Lifecycle

Digital transformation has changed how we interact, transact, and verify identity, but it's also created new opportunities for fraud. Threats like deepfakes, synthetic identities, and credential theft are no longer isolated events — they span the entire customer journey.

That's why organizations need more than point solutions. They need identity security: a holistic, AI-powered approach to securing every interaction across the identity lifecycle. Modern identity security must be:

Proactive
Anticipating threats and preventing fraud before it occurs

Adaptive
Adjusting dynamically to user risk, context, and behavior

Continuous
Spanning onboarding, authentication, and monitoring

KEY ELEMENTS OF A LAYERED IDENTITY SECURITY STRATEGY INCLUDE:

Digital IDV
Establishes trust from day one using biometrics, document checks, and passive signals

Risk-based Authentication
Applies the right level of assurance at every access point

Biometric and Passwordless Access
Reduces friction and vulnerability

Ongoing Monitoring
Uses AI to detect anomalies and prevent account takeovers

In the pages that follow, we'll take a closer look at digital IDV — the crucial first step in building trusted, secure, and scalable identity systems.

Digital Identity Verification Explained

Identity verification is how businesses confirm that a customer is who they say they are, using unique information about an individual. Today, identity verification is nearly always done in a digital setting. It's no longer scalable or competitively viable for businesses to rely on in-person verification alone.

Businesses usually conduct verification (or at least partial verification) at onboarding during the account creation or sign-up process. For regulated industries such as financial services,this is not negotiable. Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations mandate that customer identification and verification must happen at onboarding.

Common Use Cases for Identity Verification

- Verification for new account opening
- KYC and AML compliancefor financial services
- Age verification for age-restricted products/services
- Player verification for iGaming
- Fraud detection and prevention
- Onboarding remote workforces
- Driver verification for transport
- Reverification for high-risk moments and transactions

Drivers for Change

Simplifying Business Operations

Regulatory requirements are constantly evolving. It's hard for businesses to stay on top of a changing compliance landscape, especially if they operate in more than one geography. Businesses must invest a high allocation of resources and dedicate departments to implementing KYC and AML requirements, but relying on manual processes is a huge resource drain. It's expensive, slow, and can restrict business growth.

Adding to this complexity, businesses often onboard multiple vendors to support different parts of the onboarding flow. One might specialize in database checks, another in document verification, and another in fraud protection. So even as businesses develop more sophisticated approaches to verification and onboarding, they're forced to orchestrate their own onboarding flows, building custom code to bring the elements together. It's time-consuming and expensive, and as different vendor checks don't talk to each other, it becomes much harder for businesses to get a clear picture of their customers' identities.

A New Generation of Customers

Competition for today's customers is tough. They're used to having access to everything at their fingertips, at the touch of a button, and they have a low tolerance for complex, outdated, or manual experiences at onboarding. Put unnecessary or high-friction roadblocks in their way, and they'll simply switch to a competitor. Research shows that up to 20% of customers will abandon an onboarding experience if it's too confusing or time-consuming.[1]

If today's customers are this demanding, what can businesses expect from consumers? Consider that most Millennials got their first smartphone at around age 20, whereas Gen Z has never known life without the internet or smartphones.[2] And they use both to do practically everything. To keep customers loyal, businesses have to meet increasingly high standards regarding digital experiences.

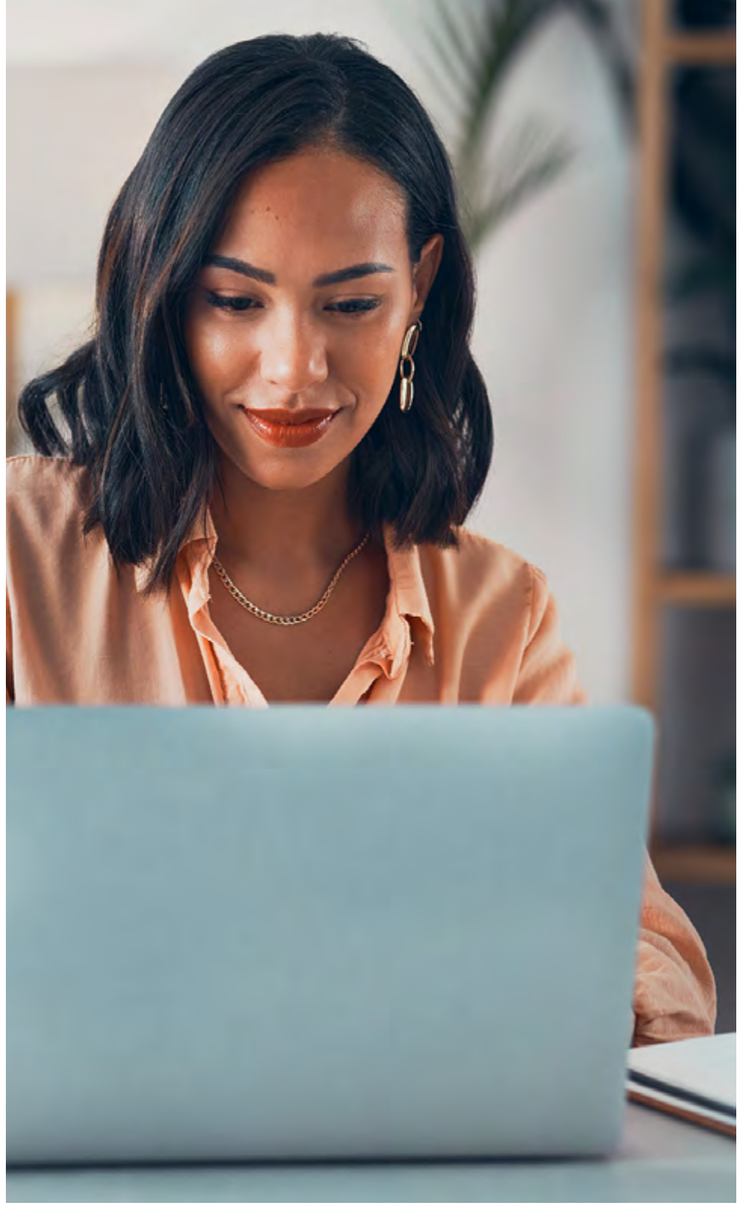
Increase in Fraud Sophistication

The rise of digital technologies hasn't just benefited businesses. It's also helped fraudsters advance. A deepfake fraud attempt happens every five minutes, according to the 2025 Identity Fraud Report, marking deepfakes' emergence as a significant threat to identity verification processes.[3]

Today's fraudsters also don't take days off — it's an increasingly global and scalable industry. Fraudulent activity used to mirror the typical 9-to-5 working week, but weekends are now the peak time for fraud, possibly an outcome of fraudsters attacking businesses when they're thought to be most vulnerable and under-resourced. A reactive approach to fraud will forever leave businesses one step behind, playing catch-up. In the long run, swallowing the cost of fraud only impacts revenue and company reputation.

The Future of Onboarding

Given these pressures, the future of identity verification and onboarding will focus on two key elements: flexibility and adaptability. When it comes to the identity process, businesses want to be able to do more, scale faster, and adapt quicker with less complexity. This is where identity orchestration will play a vital role.



Digital identity is made up of many things, including:

- Government-issued identity documents (such as birth certificates and passports)
- Digital identity documents (such as eIDs)
- Mobile data and device signals
- Identifiers such as phone numbers and email addresses
- Database checks (such as credit bureaus)
- Transaction history
- Biometric information (face, voice, and fingerprints)
- Social media information

And that list is only growing. Businesses will increasingly need to factor in a range of different checks and signals to build accurate pictures of who their customers are.

Different industries, markets, and risk tolerances demand different types of verification. In scenarios where reducing friction is top priority (such as social media or e-commerce), businesses might only want to use one type of verification, such as phone number verification.

Organizations that require a medium level of assurance or need to meet regulatory requirements might leverage several verification types, such as databases combined with document verification. In high-risk scenarios, or for highly regulated industries such as financial services that must satisfy KYC/AML requirements, they might layer watchlist checks with document and biometric verification and digital signing.

Identity Verification Benefits

Identity is the connecting thread that helps businesses build cohesive, accurate, and trusted pictures of their customers.

Stand-alone data signals or checks offer little insight. Until those insights are brought together, businesses are left with a mishmash of information that does nothing to tell them who they're interacting with or what that customer's behavior looks like.

IDENTITY VERIFICATION ENABLES BUSINESSES TO:

- Increase operational efficiencies
- Satisfy compliance requirements
- Convert more customers at onboarding
- Prevent fraud and enable risk management
- Add assurance during high-risk moments and transactions

41%

of businesses experience over $1 million in direct fraud-related costs annually, with the average organization losing $7 million.[5]

Increase Operational Efficiencies

Businesses must verify that customers are who they say they are for regulatory purposes, but interpreting global KYC and AML requirements is no small feat. Regulations constantly change, and complexity increases when a business operates in multiple geographies. Also, they must offer a low-friction user experience that allows customers fast access to their products.

Reliance on complex, manual, or inconsistent onboarding processes is time-consuming and increases friction and customer drop-off. Meanwhile, reliance on different providers pressures businesses to build their own orchestration engines. This limits the time onboarding teams have to dedicate to existing and potential customers and increases a business's operational costs.

For a global bank, you might onboard customers across geographies and have a team manually reviewing documents and biometrics for customer due diligence. In cases where there isn't a clear match, you have a team requesting follow-up documents such as proof of address. Your aspirations for growth are limitless, but your team's capacity is far from that.

Automated ID verification allows businesses to speed up turnaround times, removing friction for customers so they can access services faster. Replacing manual form fills with automatic document extraction and population reduces the likelihood of errors. With automation, businesses can grow their business and their customer base without increasing their internal team's size or overtime hours.

Satisfy KYC/AML Requirements

For regulated industries, KYC and AML checks are essential to onboarding. But in a digital world, it's harder than ever to verify identities while maintaining a seamless user experience. Today, security and compliance must coexist with low-friction, customer-friendly interactions.

That's where identity verification comes in. From government ID checks to layered data validation and screening, IDV helps businesses confidently meet KYC/AML requirements.

By automating these processes, organizations can reduce compliance risk, cut operational costs, speed up onboarding, and enter new markets more efficiently — all while allowing internal teams to focus on delivering value, not managing fines.

Convert More New Users at Onboarding

Converting more new users at onboarding is key to unlocking long-term value — but poor experiences, outdated verification methods, and clunky flows can drive users away. In fact, 90% of companies lose potential customers during the onboarding process.[4] A third of the time, it's because it takes too long or there are too many manual steps.

While regulated industries can't operate without verification, manual or in-person methods often lead to delays, frustration, and missed opportunities, especially during spikes in demand or when entering new markets.

To stay competitive, businesses are shifting toward automated, user-friendly, and scalable verification solutions that reduce friction and improve conversion.

IDENTITY VERIFICATION SHOULD OFFER:

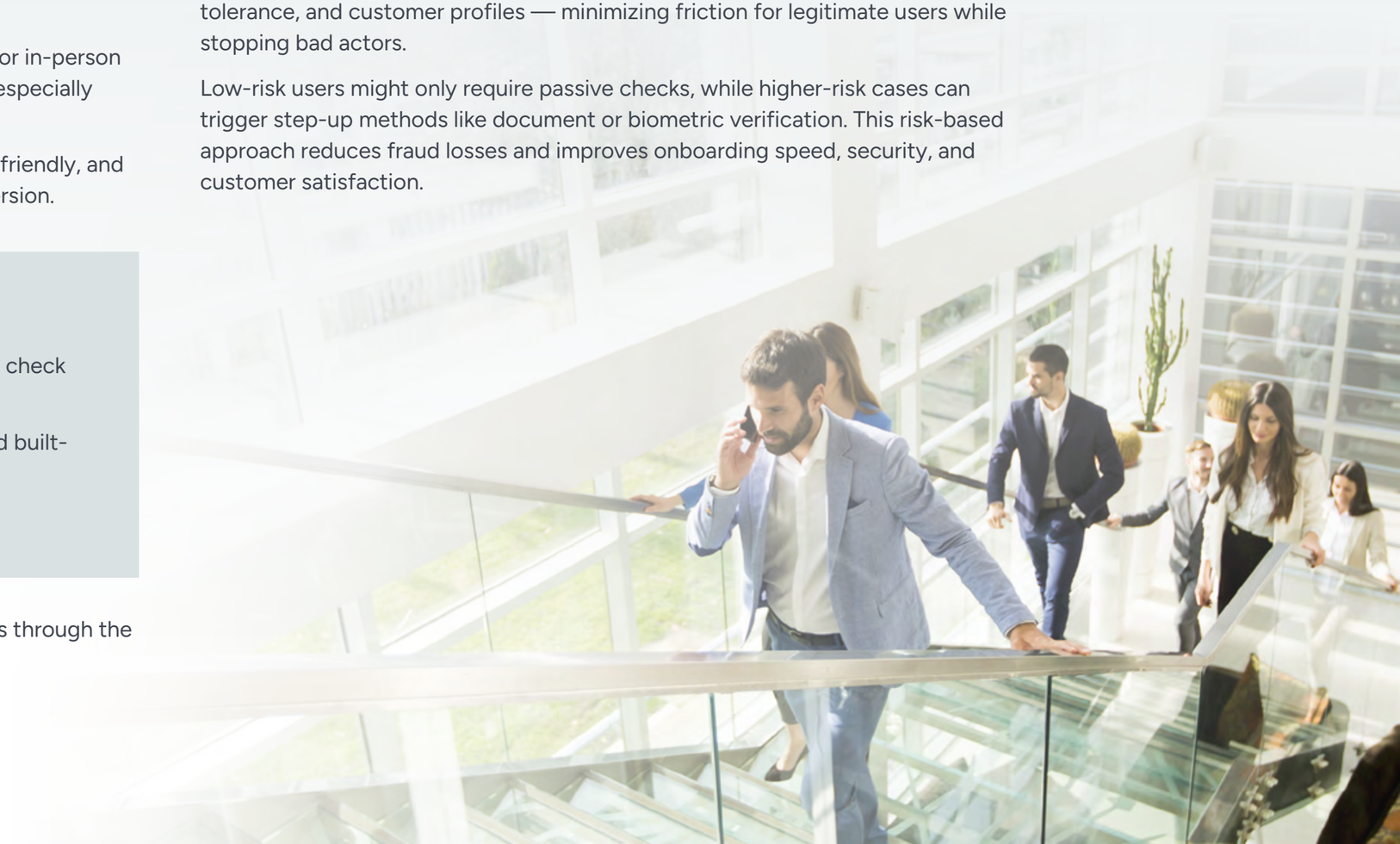
- A range of verifications so businesses can pick the right type of check for their specific goals
- Optimized capture experiences including NFC, accessibility, and built-in analytics features
- Sophisticated AI that boosts automation and decisioning

An optimized flow will ultimately help businesses get more customers through the door, driving long-term growth and revenue improvement.

Prevent Fraud and Enable Risk Management

Globally, 41% of businesses experience over $1 million in direct fraud-related costs annually, with the average organization losing $7 million.[5] Modern fraud prevention relies on layered, customizable workflows that use a mix of active and passive signals. This allows businesses to tailor identity checks based on geography, risk tolerance, and customer profiles — minimizing friction for legitimate users while stopping bad actors.

Low-risk users might only require passive checks, while higher-risk cases can trigger step-up methods like document or biometric verification. This risk-based approach reduces fraud losses and improves onboarding speed, security, and customer satisfaction.



Digital Identity Verification: Building a Strategy

The Customer Journey

A key consideration when implementing identity verification is how to integrate it into the wider customer journey. Traditionally, businesses often tacked an identity check onto the end of the sign-up flow and gave it a little more thought. However, this approach is only going to hold a business back long term. Here are some of the key moments to consider in a customer journey.

Onboarding

Verifying customers from day one sets the foundation for reverification later. It's also when users are most likely to abandon the process, so placement and expectation management are key.

High-risk Moments

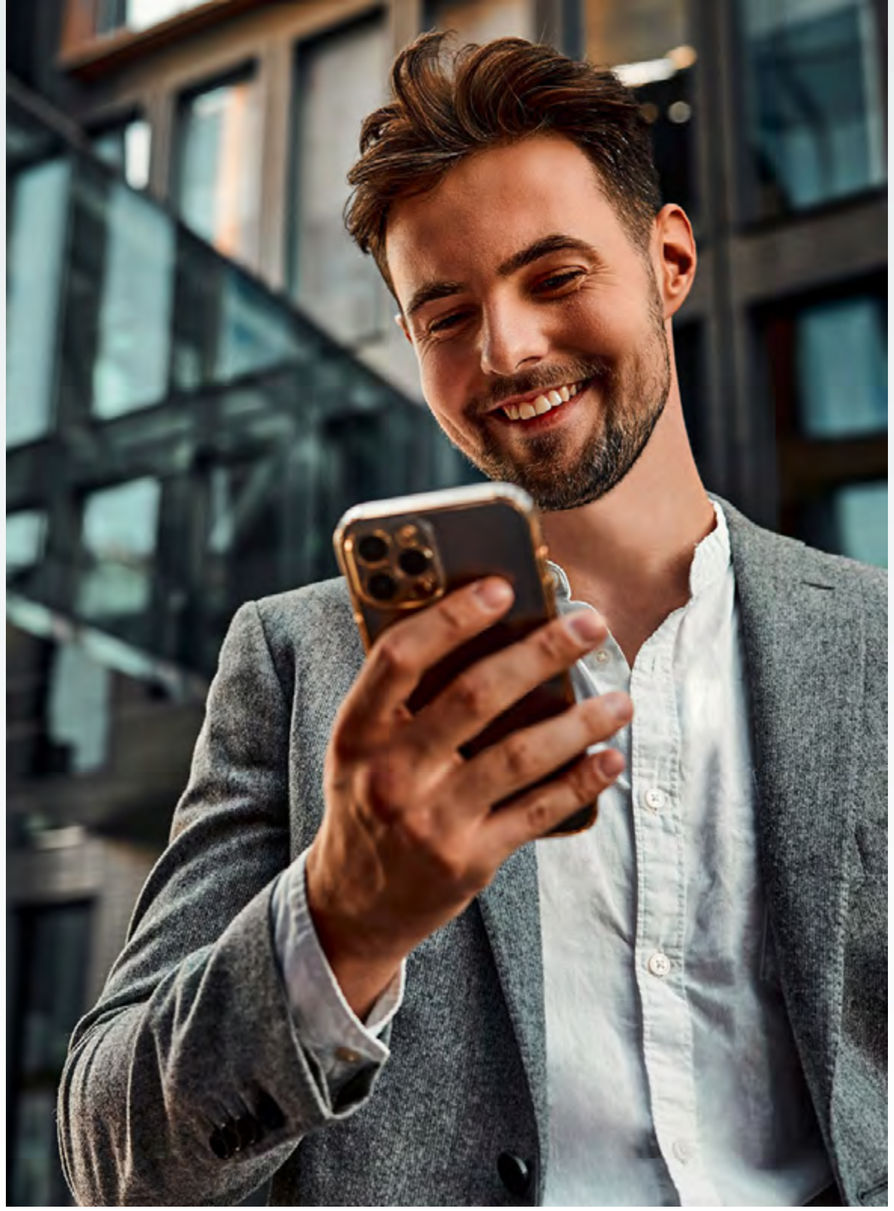
Businesses can use digital identity to re-verify or authenticate customers at risky moments — for example, when transferring large sums of money or resetting an account. Strong onboarding makes these later verifications more seamless and cost-effective.

Risk Management

Businesses should build risk management strategies around identity verification. This can help identify high-risk events and automate data-based responses.

At each stage of the journey, ask yourself:

- What information do I need from a customer?
- Is this the right moment to capture this information?
- Am I optimizing for fraud mitigation or a seamless UX?
- Can I use tools such as gamification to increase conversion?



Orchestrating Identity Flows

An effective identity verification solution depends on coordination — the ability to route the right checks and signals at the right moment in the customer journey. This is where orchestration plays a pivotal role.

Orchestration acts as mission control for verification. It ensures that all identity checks work together cohesively to create a complete, accurate picture of each user. A no-code, drag-and-drop orchestration layer removes the burden of building custom integrations and lets businesses quickly assemble tailored workflows for different geographies, risk levels, or customer types.

But verification is never a "set it and forget it" process. To keep flows performing at their best, businesses must continually test and optimize. Analytics help reveal:

- Where drop-off occurs in the funnel
- The percentage of customers converting at each step
- The number of customers rejected or unnecessarily flagged
- How often internal teams override verification outcomes
- The all-in cost of customer acquisition

By analyzing these metrics and making data-informed adjustments, businesses can continually improve conversion, reduce fraud risk, and deliver better customer experiences — all while staying compliant.

Future of Identity Verification

Identity verification is rapidly evolving, driven by advancements in technology and changes in global regulations.

One of the most significant shifts is the role of AI, particularly in fraud detection. AI-powered systems are becoming essential for combating sophisticated threats such as deepfakes, which can be used to bypass traditional identity checks. Deloitte predicts deepfake technology will have rapidly increased fraud of all forms by 2027, at which point losses in the U.S. will be triple what they were in 2023.[6]

At the same time, regulatory frameworks are moving toward greater standardization. The patchwork of requirements across regions is giving way to more cohesive standards, such as those established by ETSI, eIDAS, and NIST. This shift will simplify compliance for businesses operating in multiple regions, enabling more consistent and streamlined IDV processes.

eIDs are also playing a crucial role in shaping the future, with governments increasingly adopting digital identity schemes to facilitate secure, efficient access to services. As these systems become more widespread, they will likely drive greater adoption of digital IDV across sectors.

Deloitte predicts deepfake technology will have rapidly increased fraud of all forms by 2027, at which point losses in the U.S. will be triple what they were in 2023.[6]

Identity Verification Vendor Assessment

Selecting an identity provider is a daunting task. Below is a list of considerations businesses can use to help identify which partner is right for them.

Fraud Capabilities

What signals is the vendor assessing?

What are their false-positive and false-negative rates?

Turnaround Times

How long does it take to return results?

What steps does the vendor take to help reduce turnaround times?

Pass Rates

What are pass rates like across different documents?

How does the vendor increase pass rates?

Global Coverage and Performance

Does the vendor verify the documents and data sources from my priority regions?

Will they cover documents and data sources as we expand to new regions?

Flexible Identity Orchestration Capabilities

Do I need to orchestrate onboarding flows in-house?

Does the vendor allow me to create tailored workflows?

Accessibility

Does the vendor have industry-standard (e.g., WCAG) accessibility features?

AI Innovation

Does the vendor build their AI in-house?

Does the vendor take active measures to reduce bias in their AI?

Seamless Integration and Developer Support

Does the vendor have easy-to-follow developer documentation?

Is the product easy to integrate?

Entrust Digital Identity Verification Capabilities

Entrust Identity Verification is a flexible end-to-end identity solution, supporting both businesses and citizen needs. It provides a curated library of IDV services, including document and biometric solutions, trusted global data sources, and fraud detection signals.

Document and Biometric Verification
Our award-winning document and biometric tools give businesses confidence in customer identity at onboarding and beyond.

Data Verification
Our library of ID records, proof of address, and watchlist screening solutions allows you to navigate KYC and AML compliance at scale.

Fraud Signals
Passive signals identify fraud before it impacts businesses and can analyze geolocation, IP reputation, and device integrity while spotting repeat fraud across document and biometric solutions.

Entrust Workflow Studio

Build and optimize IDV flows using Workflow Studio Builder, a powerful orchestration layer that acts as the mission control for identity verification.

Workflow Studio
Create verification flows that take each customer on the right path. Allow low-risk customers to get fast access and direct riskier customers to more verifications.

Smart Capture Technology
Integrate with existing applications using our flexible, easy-to-integrate SDKs across iOS, Android, and web, offering accessibility features and intelligent end-user feedback to correct things like blurred or cropped images.

Full Automation
Set smart conditions within workflows to automate decision-making and improve turnaround times, clear rates, and fraud detection accuracy.

Award-Winning AI

Get fair, fast, and accurate AI-powered identity verification with a built-in risk engine and anti-bias capabilities.

Anti-bias AI
Our award-winning AI is trained on diverse datasets and tested to ensure it performs the same for everyone, regardless of race, gender, or age.

Built In-house
Our AI was built and refined in-house over the last 12 years in collaboration with leading privacy organizations, such as the Information Commissioner's Office in the UK.

Lightning-fast
Our AI delivers results rapidly, so genuine customers aren't kept waiting.

Pinpoint Accuracy
With over 10,000 micro-models that specialize in individual tasks, our AI is highly adaptive and accurate.

Contact our team today to get started.

Sources

1. https://www.entrust.com/resources/reports/user-research-report
2. https://explodingtopics.com/blog/gen-z-trends
3. https://www.entrust.com/resources/reports/identity-fraud-report
4. https://www.businesswire.com/news/home/20221115005637/en/90-of-companies-lose-potential-customers-during-the-digital-onboarding-process-according-to-ABBYY-State-of-Intelligent-Automation-Report-Q4-2022
5. https://go.entrust.com/docusign-future-global-identity-verification
6. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST

SECURING A WORLD IN MOTION