Identity Verification

Securely Onboard New Customers and Build Trust Across the Identity Lifecycle

ENTRUST

SECURING A WORLD IN MOTION

Identity is now at the center of every interaction – whether opening a bank account, issuing an identification card, approving a loan, completing high-risk transactions, onboarding employees or contractors, or granting access to critical systems. As a result, businesses must establish trust from day one to answer key questions: Is this person real? Are they who they claim to be? Should they have access?

The Challenge: Balancing Speed, Security, and Trust

Financial institutions face rising fraud, tightening regulations, and increasing customer demand for instant digital onboarding. Fraud continues to grow at double-digit rates, with businesses reporting an **18% increase in fraud losses in the past year**[1], as synthetic identities, deepfakes, and other AI-driven impersonation attacks challenge legacy verification methods.

At the same time, customer expectations are high. Every point of friction costs real revenue – **55% of customers have abandoned purchases or sign-ups due to poor digital experiences**[2]**.**

Global regulators are also tightening Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, with greater scrutiny than ever on digital identity proofing.

- In the U.S., FinCEN now recognizes digital identity credentials aligned to **NIST IAL2**
- In the EU, **eIDAS** establishes the framework for electronic identification and authentication and introduces EUDI wallets, in line with ETSI standards
- In the U.K., the **Digital Identity & Attributes Trust Framework** requires high-assurance digital identity checks to support KYC

The drive toward digital wallets, open banking, and eID ecosystems is increasing demand for interoperable, high-assurance identity in the next few years. The EU's Digital Identity Wallet initiative, for example, will require regulated industries to accept EUDI wallets by December 2027[3].

Financial services face increasing complexity and operational inefficiencies when scaling secure, compliant onboarding and authentication processes.

For years, enterprise organizations have focused on securing the network perimeter and now also face an identity crisis when it comes to Know Your Employee (KYE). With the rise of remote work and AI, the human employee has become the most targeted – and most vulnerable – entry point for sophisticated global threats.

Attackers are targeting the entire employee lifecycle:

- **Hiring:** Gartner® predicts that by 2028, 1 in every 4 job applicants worldwide will be fake[4].
- **Workforce Access:** Compromised multi-factor authentication (MFA), stolen credentials, and AI-assisted impersonation make it harder for security teams to determine who is actually behind a login attempt.

Finally, governments around the world are under increasing pressure to modernize identity systems for travelers and citizens, while maintaining the highest levels of security, privacy, and public trust. Many government agencies still rely on legacy identity systems that are vulnerable to impersonation, fraud, and cyberattacks. The rise of sophisticated AI-driven spoofing, deepfakes, and synthetic identities threatens traditional document checks and remote identity proofing methods, while offline or underserved populations risk exclusion if digital systems aren't built with accessibility and equity in mind.

At the same time, governments must balance cross-border interoperability, complex privacy regulations, and public scrutiny around data protection. The result: agencies are challenged to deliver trusted, high-assurance digital identity at scale.

Protecting a business is about protecting digital and physical people, devices, and data, and being 100% certain that the person logging in is real and is who they say they are.

[1] TransUnion's H2 2025 Fraud Trends Report
[2] Conviva's 2025 State of Digital Experience Report
[3] European Commission – European Digital Identity (EUDI) Regulation
[4] Gartner Survey – 1Q25

The Solution: IDV for Secure and Compliant Identity Journeys

Organizations need a reliable, scalable way to verify identities from day one and throughout the customer lifecycle. Entrust Identity Verification (IDV) empowers organizations to quickly and accurately confirm that individuals are real and are who they claim to be – whether opening an account, accessing critical systems, or applying for government services. By combining secure identity document validation, biometric verification, and layered fraud-detection intelligence, Entrust helps organizations reduce risk, streamline onboarding, and deliver trusted digital experiences.

Identity Verification for Financial Services: Verify customers quickly and accurately at account opening and beyond, increasing customer acquisition, ensuring KYC/AML compliance, and minimizing fraud risk.

Identity Verification for Enterprise Workforces: Fast, reliable identity checks for employees and contractors, enabling secure hiring and onboarding while ensuring privileged access by role, without slowing productivity or increasing risk.

Identity Verification for Government: Verify citizen identities with high assurance for high-risk services, fraud reduction, and seamless access to government services.

Entrust Supports Your Business Goals

Onboard More Customers, Employees, and Contractors Faster

Establish trusted identities from day one while balancing speed and security, ensuring legitimate customers are onboarded quickly and without unnecessary hurdles. With high-assurance, AI-powered document and biometric verification, convert more users through a combination of automation and speed. 95% of results are returned in less than five seconds.

Create Trusted Identities Across the Customer Lifecycle

Build on trusted identities established at onboarding for faster authentication and unlock lifetime value by providing access to additional services throughout the customer lifecycle. Secure high-risk moments beyond onboarding against account takeover using trusted biometric authentication and passkeys that tie users back to their trusted, day-one identity and protect every high-value action.

Prevent Fraud and Reduce Risk

Detect high-risk behavior to combat fraud, including impersonation, deepfakes, synthetic identities, and other emerging attack methods. Our document and biometric verification is designed to prevent fraud from day one – supported by passive fraud signals including device intelligence and repeat fraud detection, and backed by best-in-class machine learning models and in-house fraud expertise.

Simplify Regulatory Compliance

Meet local and global regulations including eIDAS 2.0, in line with trust frameworks such as ETSI TS 119 461, ETSI EN 319 401, and NIST 800-63-4. Easily scale to new markets with market-ready packages, selected partner integrations, and global identity coverage across 195 countries.

Powered by a Platform Built for Speed, Scale, and Adaptability

Accelerate time to market and optimize user identity journeys with a platform that creates a unified view of identity – all in one place. Access a full suite of IDV, digital signing, database, and authentication solutions; low-friction user experiences dynamically linked to a powerful workflow builder; partner ecosystem; and integrated testing and analytics tools.

Security and Compliance Certifications

ISO 27001	ETSI TS 119 461 Certified (remote identity proofing)	ETSI EN 319 401 Certified (trust service governance)
eIDAS Regulation EU 910/2014 Compliant	UK Digital Verification Services Trust Framework (DVSTF)	NIST 800-63-3 - Identity Assurance Level 2 Certified

Talk to an Entrust Expert

Learn how Entrust can help you verify, onboard, and authenticate users with confidence, securing every identity interaction across your digital ecosystem. Connect with an Entrust expert today.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION