EBOOK

The Compliance Manager's Guide to Identity Verification for KYC

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

Know your customer (KYC) and anti-money laundering (AML) processes are integral to any financial services onboarding journey. But in an online setting, it's become harder for companies to build an accurate picture of their customers to satisfy the ever-evolving global compliance landscape.

At the same time, it's no longer enough to simply tick a compliance checkbox. Customers are demanding seamless experiences across all industries. Players like Amazon, Netflix, and Apple have raised the bar when it comes to customer experience by offering instant access to services across multiple channels.

Business priorities are now stretched across financial crime and compliance, fraud risks, and scalable growth. Financial institutions face the challenge of balancing security, compliance, and user experience while increasing operational efficiencies.

Table of Contents

Digital Identity Verification: The Business Enabler

Identity verification is a non-negotiable requirement within any KYC and AML program. However, just because businesses need to verify customer identities before they grant access to their services, it doesn't mean they need to sacrifice the customer experience throughout the onboarding journey.

In today's complex cyber landscape, identity verification solutions aren't simply an add-on. Businesses no longer need to treat verification as an afterthought or tack checks onto the end of their sign-up flow. Instead, if done right, digital identity verification acts as a business enabler — setting businesses apart from the competition by supporting secure, near-instant, and scalable real-time verifications.

This allows businesses not only to remain compliant and fight fraud but also to scale quickly into new markets while enhancing operational efficiencies.

Today's Compliance Landscape

Interpreting global KYC and AML requirements is no small feat. Financial services — one of the world's most highly regulated industries — faces a constantly evolving compliance landscape. Regulatory bodies across different geographies are aligning with new supranational regulations, frameworks, and technical standards, further expanding the list of requirements.

In turn, navigating global compliance has become increasingly complex, especially with ever-growing legislation. Plus, these new requirements vary by location, only adding to the challenge. As a result, the pressure to stay compliant has never been greater.

United States

The history of U.S. AML legislation dates back to the **Bank Secrecy Act (BSA)** of 1970. It establishes the required recordkeeping and reporting practices for banks and other financial institutions. The BSA mandates that financial institutions must identify customers conducting transactions and maintain appropriate records of those transactions.

However, the BSA was enacted before digital banking became widely accepted. To keep pace with innovation and stay ahead of fraudsters, the U.S. Congress, along with the National Institute of Standards and Technology (NIST), has introduced additional legislation and guidelines. NIST, as a federal agency, promotes American industrial competitiveness by advancing technology, standards, and best practices.

KEY LEGISLATIVE UPDATES INCLUDE:

- Money Laundering Control Act (1986)
- Anti-Drug Abuse Act (1988)
- Annunzio-Wylie Anti-Money Laundering Act (1992)
- Money Laundering Suppression Act (1994)
- Money Laundering and Financial Crimes Strategy Act (1998)
- USA PATRIOT Act (2001)
- Intelligence Reform & Terrorism Prevention Act (2004)
- NIST Special Publication (SP) 800-63: Digital Identity Guidelines

The Anti-Money Laundering Act of 2020 (AMLA 2020), the most significant reform to U.S. AML legislation in decades, became law on January 1, 2021. It allows for more effective efforts in combating financial crimes, emphasizing the importance of identifying and managing risks over merely reporting suspicious activity.

One of NIST's key contributions to AML and identity verification is the development of the SP 800-63 Digital Identity Guidelines, which outline a framework for identity proofing and authentication. These guidelines aim to increase assurance levels, recommend rigorous verification measures, and reduce fraud risk — particularly in digital environments. A **second draft** of the fourth version of the guidelines was released in August 2024 to reflect new trends in the digital landscape.

In recent years, the **Financial Crimes Enforcement Network** (FinCEN) has acknowledged the need to modernize current AML and counter the financing of terrorism (CFT) regulations to ensure compliance with the BSA is more effective and efficient.

The Anti-Money Laundering Act of 2020 (AMLA 2020), the most significant reform to U.S. AML legislation in decades, became law on January 1, 2021. It allows for more effective efforts in combating financial crimes, emphasizing the importance of identifying and managing risks over merely reporting suspicious activity.

AMLA 2020 has led to a variety of rulemaking initiatives by FinCEN. In June 2021, FinCEN published its **first list** of AML/CFT priorities, highlighting key threat trends and resources. This list is expected to be updated every three to four years. Financial institutions should pay close attention, as these priorities will shape future regulatory changes. To date, FinCEN has started the **rulemaking process** in several areas, including real estate, beneficial ownership information, and antiquities.

United Kingdom

U.K. AML regulation is outlined in several key legislative acts:

The Proceeds of Crime Act (POCA) 2002: This is the U.K.'s primary AML legislation. Under POCA, banks and financial institutions must take necessary steps to detect money laundering activities. These steps include customer due diligence (CDD), transaction monitoring, and suspicious activity reporting.

The Terrorism Act 2000: This act mandates that financial services take steps to prevent terrorist financing, including CDD, transaction monitoring, and reporting. It has since been amended through the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007.

The Money Laundering, Terrorist Financing, and Transfer of Funds Regulations 2017: Often referred to as MLRs 2017, this regulation transposes the EU's 4AMLD into U.K. law and was later amended by the 5AMLD through the Money Laundering and Terrorist Financing (Amendment) Regulations 2019. It introduced the requirement for firms to conduct written AML and CFT risk assessments. In 2021, HM Treasury initiated a review of further amendments to bolster the regulation's effectiveness and optimize the supervisory regime. These changes were codified in the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022, which took effect on September 1, 2022.

These updates aim to help U.K.-based businesses meet international AML standards, particularly in the areas of virtual assets and proliferation financing risk assessments. The government concluded in June 2022 that the existing framework was largely fit for purpose, requiring no sweeping reforms at that time.

EU Landscape

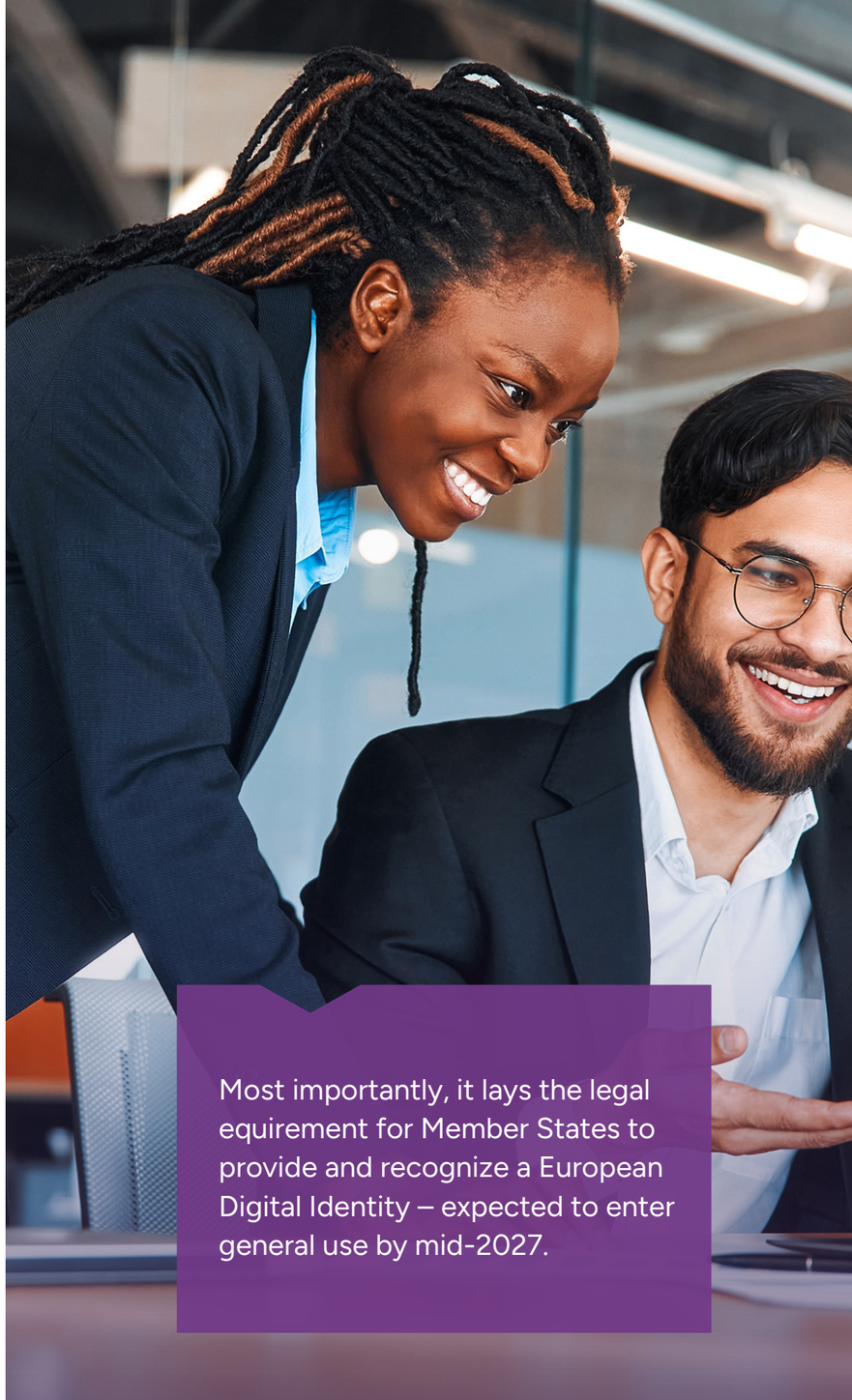
The EU Anti-Money Laundering and Financing of Terrorism Directives are designed to protect the financial system from abuse by criminals using it for money laundering or terrorist financing.

eIDAS 910/2014:

eIDAS — short for electronic Identification, Authentication, and Trust Services — is a regulatory framework introduced by the European Union to standardize how electronic identification and trust services are used across Member States to support KYC processes with enhanced security and compliance.

eIDAS 2.0 1183/2024:

In 2024, the EU passed amendments to Regulation 910/2014 to establish the European Digital Identity Framework, also known as eIDAS 2.0. The updated regulation creates new rules for electronic identification and trust services.



Most importantly, it lays the legal equirement for Member States to provide and recognize a European Digital Identity – expected to enter general use by mid-2027.

Global Regulations

Outside of the U.S., U.K., and EU, a variety of international regulations and standards help shape the global compliance landscape for AML and identity verification.

NIST: While primarily a U.S. agency, NIST's guidelines influence global practices because of their thorough and structured approach to cybersecurity and identity proofing. NIST's Digital Identity Guidelines offer a framework for verifying identity in digital transactions, and they are widely respected across industries — even outside the United States. These guidelines emphasize layered identity proofing and high-assurance methods to reduce fraud.

Financial Action Task Force (FATF): The FATF is an intergovernmental organization that sets global standards to combat money laundering and terrorist financing. It urges member countries to establish AML/CTF frameworks that align with its recommendations. Countries like Japan, Canada, and Australia have incorporated FATF principles into their national legislation. Key pillars include customer due diligence (CDD), riskbased approaches, and beneficial ownership transparency.

ISO Standards (ISO/IEC 27001): The International Organization for Standardization plays a major role in compliance through ISO/IEC 27001, which offers a framework for managing information security risks. Recognized across various industries — particularly finance and telecommunications — ISO/IEC 27001 is often a requirement in AML and KYC frameworks. Compliance with this standard helps organizations demonstrate their commitment to protecting sensitive customer data.

Regional regulations: In Asia-Pacific, countries like Singapore and Hong Kong have introduced local regulations that incorporate global standards while tailoring requirements to the regional market. Singapore's Payment Services Act mandates rigorous identity verification and CDD for transactions involving digital payments and virtual assets, aligning with FATF principles. Similarly, Hong Kong's Anti-Money Laundering and Counter-Terrorist Financing Ordinance requires financial institutions to implement robust identity verification processes, positioning the region as a leader in digital finance compliance.

Anatomy of KYC/AML Programs

Complying with AML regulations involves several different processes. Much of the compliance legwork occurs at the beginning of a customer lifecycle: onboarding. This is what sets the stage for AML measures and CFT practices. While specific requirements for compliant onboarding processes vary by geography, market, and customer profile, the key elements are generally the same.

Identity Verification (IDV)

This step typically includes verifying a government-issued ID, such as a passport, driver's license, or national ID card.

KYC and CDD

Businesses must perform KYC checks to confirm that customers are who they say they are. At a minimum, this includes collecting data like name, date of birth, and address. In many countries, additional information — such as an ID or tax number — is required. Businesses often begin forming a financial profile during this stage, identifying customer activities, industries, or geographic regions where they operate.

This information helps define what "normal" activity looks like for that customer, which aids in detecting anomalies later on.

Screening

Businesses must screen customers to determine whether they are politically exposed persons (PEPs) or appear on sanctions lists/watchlists.

Customer Risk Assessments (CRAs)

Using the collected information, businesses determine each customer's level of financial crime risk. Risk profiles may be based on occupation and income, location, type of financial services used, or transaction type. Depending on the results, businesses may need to conduct enhanced due diligence (EDD) before completing onboarding.

Entrust Identity as a Service

Businesses can extend the value of the identity verified on day one by leveraging Entrust's Identity as a Service (IDaaS). This enables stepup authentication at critical points, whether securing a user's bank account or ensuring workforce security. It also provides ongoing protection well beyond onboarding.

Considerations and Assessments

What to Consider When Building Out an Onboarding Tech Stack

The following questions offer a set of criteria businesses can use to assess identity solutions for KYC/AML programs. They should consider a combination of the following when making decisions regarding their tech stack.

Internal Considerations

Current Regulations

- What regulations do we currently need to satisfy?
- What approach is required for onboarding and ongoing monitoring?

Future Regulations

- Where is the future of regulation headed?
- What solutions will help me meet requirements both now and in the future?
- How does any vendor we consider stay on top of policy trends?
- How are the regulations evolving in regions your business wants to expand into?

Geography

- What is required in each region where my business operates?
- What are our expansion plans as a business?
- How suitable is our approach to verification in other regions?
- Will any solution we onboard make future expansion easier?

Risk Tolerance

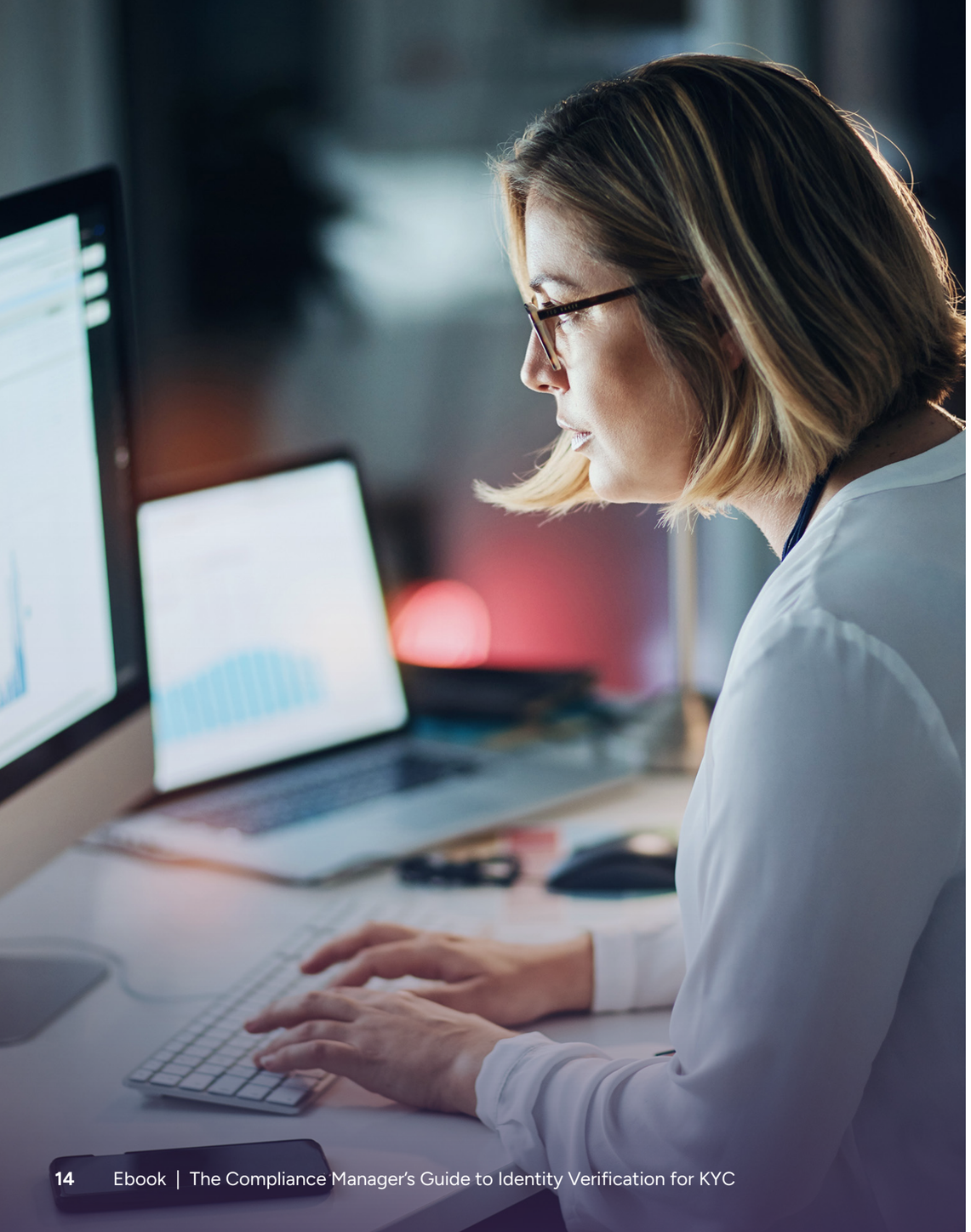
- How does our risk tolerance vary by customer, market, or region?
- Can a solution support different risk-based approaches?

Competition

- What approach are other companies in the industry taking when it comes to identity verification?
- How does our approach to verification/KYC compare?
- Are we ahead of the competition or behind?
- Are we providing a good onboarding experience or a bad one?

Implementation

- Should we build in-house or integrate a third-party solution?
- What are the orchestration requirements?
- Will managing this system strain internal resources?



Internal Stakeholders

Who else within the company relies on using this solution? What are their use cases? What questions will other teams be asking?

Product

- How will it impact conversion rates?
- Does it offer a good user experience?
- What level of friction does it create?
- Does it support expansion into new markets?
- What are the results like?
- How easy is it to integrate?

Operations

- Will it help improve efficiencies?
- Does the solution allow straight-through processing?
- Will it help reduce costs?
- Is it fast, and can it scale?
- How easy is it to use?
- What is the granularity of results?

Fraud

- What are the fraud detection capabilities?

Vendor Capabilities

Who else within the company relies on using this solution? What are their use cases? What questions will other teams be asking?

Product

- Does the vendor have global support for watchlist screening databases?
- Does the vendor support a global range of governmentissued IDs for document verification?
- Does the vendor offer the ability to configure different verification journeys for users of different risk profiles (e.g., limited verification for low-risk users, step-up verification for higher-risk users)?
- Does the vendor provide a portal to review and follow up on customer verifications?
- How does the vendor fit in with my acquisition channels? Is there support for web-based journeys and mobile journeys?
- Does the vendor and their product platform conform with relevant security and compliance certifications (e.g., ISO 27001, SOC 2, ETSI, NIST) and local KYC regulations (where required)?
- Does the vendor provide detailed analytical breakdowns on why a verification check was passed or failed?
- Does the vendor provide an easy way for me to download all relevant results and data to meet my recordkeeping obligations?

- **What's the integration process like?**
- Is there comprehensive API documentation?
- Is there support for off-the-shelf software development kits (SDKs)?
- What documentation do you provide?

Metrics

Performance

- What are the “false acceptance” (% of fraudsters that slip through verification) and “false rejection” (% of genuine customers that are rejected at verification) rates?
- How long does it take to receive a yes/no verification response?
- What percentage of users can you approve without the need for manual intervention?
- What’s the cost per acquired customer (CAC)?

User Experience

- How many steps does the compliance process require a user to go through?
- What is the percentage drop-off for customers at each stage of the process?

Identity Verification Vendor Capabilities

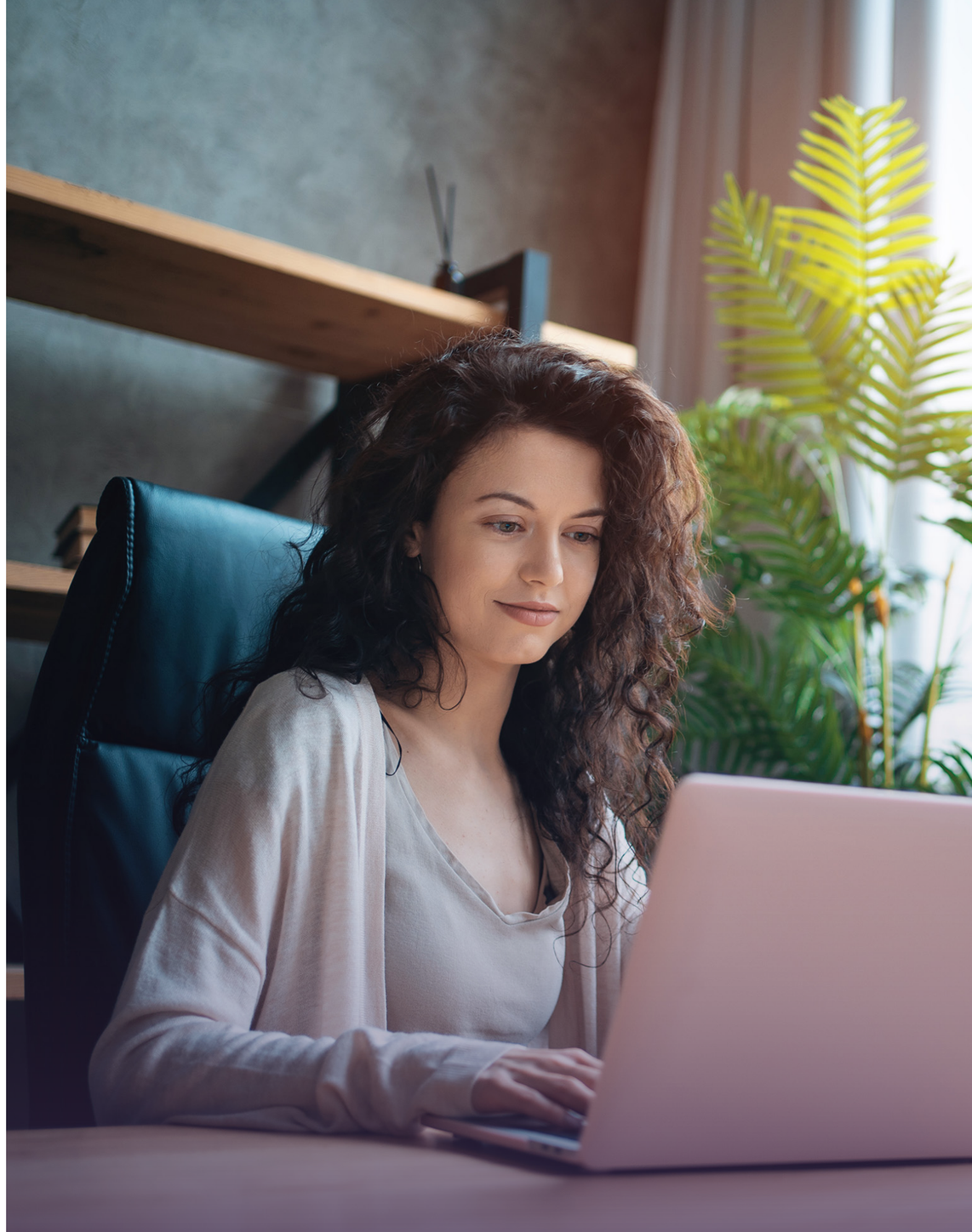
Entrust offers its users a portfolio of verification tools, no-code orchestration, and powerful artificial intelligence (AI) to help businesses meet their specific compliance needs.

Verification Suite

Entrust's Verification Suite includes a library of global checks and fraud signals to minimize friction, catch sophisticated attacks, and help address compliance needs at scale.

By combining verification tasks into Workflow Studio, clients can increase the overall assurance that a given user is:

- A real person presenting genuine government-issued ID and/or valid supplementary evidence
- Using a trusted device, network, and SDK to capture all required attributes and evidence



Document Verification

Automatically verify identity documents like government-issued photo IDs. Our award-winning AI classifies documents in milliseconds and supports more than 2,500 document types from 195 countries.

Biometric Verification

Ensure identity documents are presented by their rightful owners. Our biometric verification matches a photo ID to facial biometrics captured in the same flow. Clients can choose verification using a selfie, video, or motion. Selfie requests a static photo and passively checks for liveness. Video and motion request a video selfie to protect against more sophisticated attack methods.

Data Verification

Help fulfill regulatory compliance requirements such as AML with a suite of financial crime and compliance signals — from PEPs and sanctions to adverse media and proof of address. Clients can choose trusted data sources that make sense for them and convert users in seconds.

Fraud Detection

Unleash the power of phone and device intelligence to accurately distinguish between trusted and fraudulent behavior at onboarding and beyond. Harness intelligence related to devices, locations, identities, and threats without impacting the experience of genuine users.

Workflow Studio

Workflow Studio is a mission control orchestration layer that allows businesses to automate tailored experiences and build no-code workflows with a drag-and-drop approach.

Tailored Workflows

Workflows shouldn't be a one-size-fits-all approach, as different customers will have different risk levels. Workflow Studio allows businesses to tailor and optimize verification flows that respond to changing market conditions, enabling them to move each user through the right verifications at the right time. They can also easily introduce new verification methods, data sources, and fraud signals to help address global regulatory compliance requirements at scale. In turn, Workflow Studio empowers organizations to:

- Expand into new geographies
- Align with internal policy changes
- Adjust for risk tolerance
- Navigate new compliance requirements

Analytics and Dashboard

Businesses can manage the outcomes of verification checks via the centralized dashboard. With the help of comprehensive results and intuitive insights, organizations will know why decisions have been made at every stage of the workflow. This dashboard also allows them to define custom logic to automate decisions and eliminate the need for manual review. Plus, they can:

- Analyze workflow performance
- Access granular results
- Retrieve results in a dashboard or through an API

Award-Winning AI

We've built an award-winning AI that's fair, fast, and accurate.

Fair
We trained our AI using global, diverse datasets to reduce bias regardless of race, gender, and age, so all your customers are treated fairly.

Fast
With results returned in seconds, you can make confident decisions without keeping good customers waiting.

Accurate
Our AI is purpose-built to catch fraud before it impacts your business, protecting you and your customers.

The Benefits of Seamless Orchestration

Workflow Studio doesn't just simplify onboarding. It transforms how compliance and fraud teams operate. By bringing identity verification, fraud detection, and policy logic into one centralized, user-friendly interface, Workflow Studio empowers teams to orchestrate secure, scalable experiences with minimal lift.

With this solution, organizations can:

- Accelerate time to market by launching compliant onboarding flows faster.
- Reduce engineering dependency with drag-and-drop configuration.
- Adapt quickly to regulatory changes, policy updates, and fraud patterns.
- Support global scale with region-specific workflows and multilingual UX.
- Minimize manual review through automated decisions based on risk thresholds.
- Improve audit readiness by embedding traceable logic and decisions into every flow.

Workflow Studio empowers compliance teams to go from reactive to proactive — building onboarding systems that aren't just compliant, but competitive.

Ready to Make Compliance Your Competitive Advantage?

One provider, one unified onboarding flow, multiple markets. Entrust can help your business meet complex local regulatory needs and remotely onboard customers globally with an off-the-shelf compliance solution. It combines ETSI-certified identity verification with a qualified electronic signature and one-time password to offer simple, seamless, and eIDAS-compliant onboarding.

Contact our team today to get started.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

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

ENTRUST

SECURING A WORLD IN MOTION