EBOOK

The Compliance Manager's Guide to Identity Verification for KYC

onfido
an Entrust Company

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.

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.

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 and 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 to not only remain compliant and fight fraud but to also 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 — face 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 record-keeping and reporting practices for banks and other financial institutions. The BSA established that financial institutions must identify customers conducting transactions and keep appropriate records of financial 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

One of NIST's key contributions to AML and identity verification is the development of the SP 800-63 Digital Identity Guidelines, which outlines a framework for identity proofing and authentication. These guidelines focus on achieving higher levels of assurance in identity verification by recommending rigorous identity proofing measures, improving security protocols, and reducing fraud risk, particularly in digital environments. NIST released **the second draft** of the fourth version of the SP in August 2024, which updated the text in response to the changing digital landscape.

In recent years, the **Financial Crime Enforcement Network (FinCEN)** has acknowledged the need to modernize current AML and Counter-Terrorist Financing (CTF) regulations to ensure financial services 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 versus strictly reporting suspicious activity.

AMLA 2020 has led to a variety of rulemaking by FinCEN. FinCEN published its **first list** of anti-money laundering and countering the financing of terrorism (AML/CTF) priorities in June 2021, highlighting key threat trends and informational resources. The list of priorities is expected to be updated every three to four years. Financial institutions should pay close attention to these priorities because they will feed into 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 the following legislation:

The Proceeds of Crime Act (POCA) 2002

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

The Terrorism Act 2000

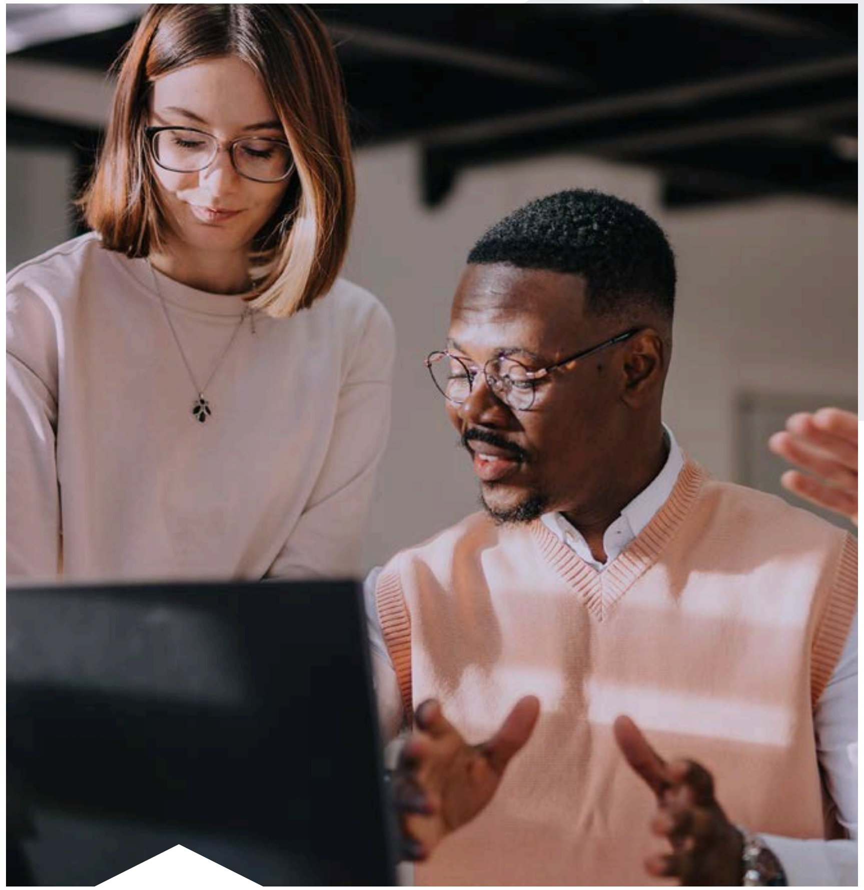
This act mandated that financial services must take steps to prevent terrorist financing, including CDD, transaction monitoring, and reporting. It has since been amended through subsequent legislation, including the Terrorism Act 2006 and the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment)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

The Money Laundering, Terrorist Financing, and Transfer of Funds Regulations 2017

This regulation (often referred to as MLRs 2017) is another key piece of AML legislation in the U.K. and transposes the obligations set out in the EU's 4AMLD, and subsequently, 5AMLD via The Money Laundering and Terrorist Financing (Amendment) Regulations 2019. It also introduced the requirement that firms implement a written AML and CTF risk assessment. In July 2021 the HM Treasury initiated a review of amendments to the MLRs 2017 to bolster their effectiveness and optimize the U.K. supervisory regime. The amendments will be made in draft secondary legislation entitled Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022, which took effect from 1st September 2022.

The amendments look at changes to help businesses operating in the U.K. comply with international AML standards on virtual assets, plus examine the requirement to perform risk assessments on proliferation financing.

The government published its response in June 2022. It also issued a forward-looking review of AML in June 2022, concluding that the current regime is broadly fit for purpose and required no wholesale changes for the time being.



EU landscape

The EU Anti-Money Laundering and Financing of Terrorism Directives are designed to protect the financial system from criminals who misuse them for money laundering and financing terrorism.

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 EU member states to support KYC processes for 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 new regulation creates and updates rules for electronic identification and trust services.

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

Global regulations

Outside the U.S., UK, and EU, various international regulations and standards shape the compliance landscape to address global AML and identity verification needs.

NIST

While primarily a U.S. agency, NIST's guidelines influence global practices due to their rigorous approach to cybersecurity and identity proofing. NIST's Digital Identity Guidelines provide a framework for verifying identity in digital transactions, widely respected by organizations across sectors, including those outside the U.S. The guidelines recommend multi-layered identity proofing, emphasizing high-assurance methods to reduce fraud.

Financial Action Task Force (FATF)

The FATF, an intergovernmental organization, sets global standards to combat money laundering and terrorist financing, urging member countries worldwide to establish aligned AML/CFT frameworks. Many countries, including Japan, Canada, and Australia, have adopted FATF's recommendations, incorporating them into local legislation to drive consistent compliance measures across financial systems. FATF's guidelines emphasize key practices like customer due diligence (CDD), risk-based approaches, and beneficial ownership transparency to protect the global financial network.

ISO Standards (ISO/IEC 27001)

The International Organization for Standardization (ISO) plays a significant role in global compliance through standards like ISO/IEC 27001, which provides a structured approach to managing information security risks. This standard is recognized across industries and regions, including financial and telecommunications sectors, and is often a core requirement in AML/KYC frameworks. By adhering to ISO 27001, institutions demonstrate commitment to protecting sensitive customer data, an essential aspect of compliance that builds trust in cross-border operations.

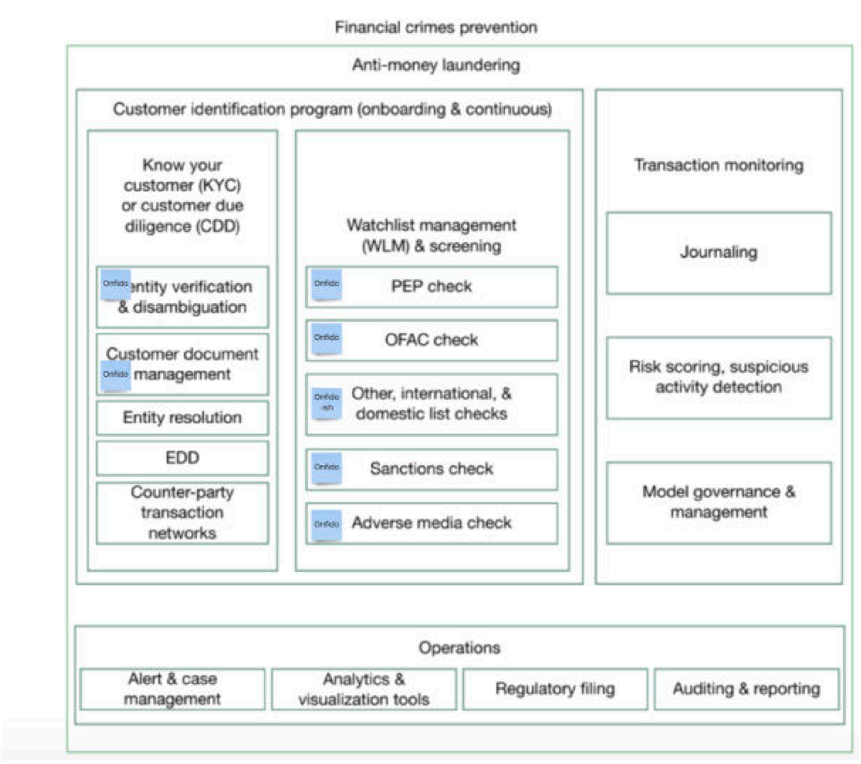
Regional Regulations

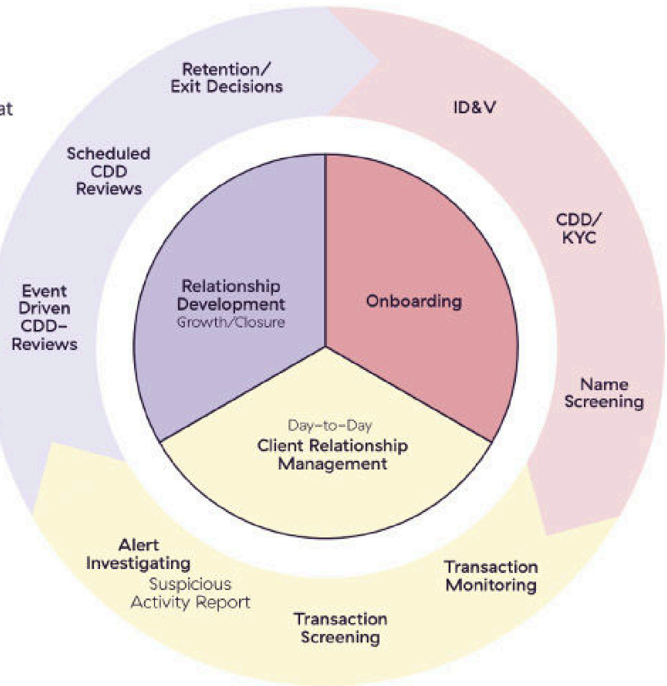
In Asia-Pacific, countries like Singapore and Hong Kong have introduced local regulations that incorporate global standards while tailoring requirements to the regional market. Singapore's Payment Services Act mandates rigorous identity verification and CDD for transactions involving digital payments 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.

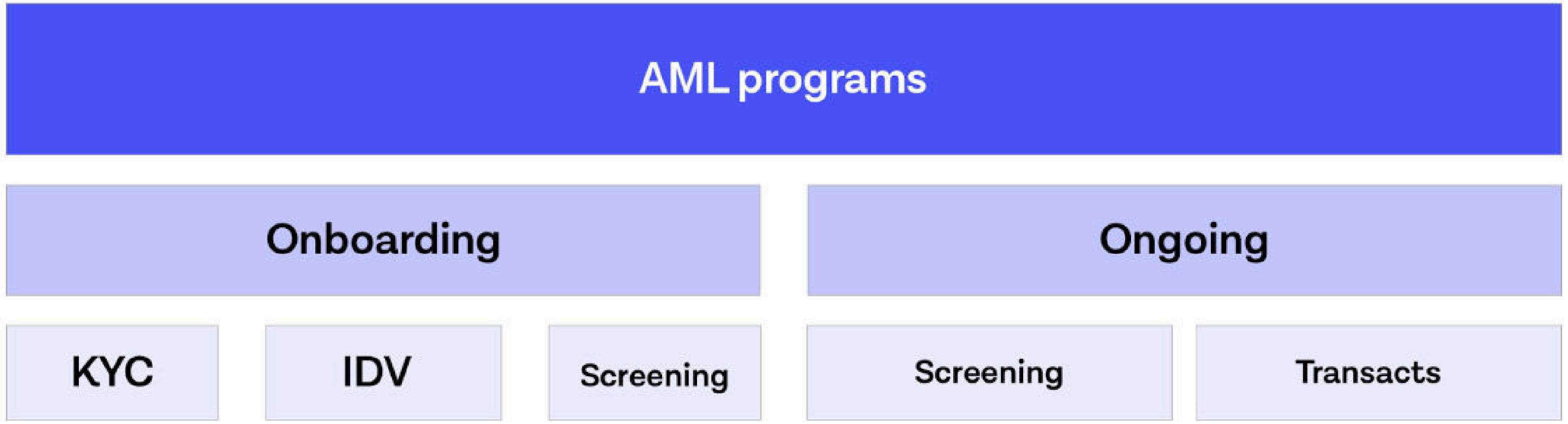
Anatomy of KYC/AML Programs

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 CTF practices. While specific requirements for compliant onboarding processes vary by geography, market, and customer profile, the key elements are generally the same.

FIGURE 1 Anatomy Of AML Programs







Identity verification (IDV)

This step usually involves checking a government-issued ID, such as a passport, driver's license, or national ID card.

KYC and CDD

Businesses need to perform KYC checks to ensure customers are who they say they are. Providers must collect a blend of customer data points for KYC — including, at the minimum, name, date, and address. Many geographies also require additional data verification such as an ID number or tax ID.

At this stage, businesses will often start building a picture of customers' economic activities and financial status — such as what markets they're active in and entities they usually do business with.

This helps create a customer profile, helping businesses understand what normal activity looks like for that customer.

Screening

This step involves identifying sanctioned individuals or customers who are considered a higher financial crime risk, such as Politically Exposed Persons (PEPs). Businesses screen customer names against a series of relevant watchlists and sanctions lists.

Customer risk assessments (CRA)

At this point, businesses can use the information available to them to determine the financial crime risk of the customer. This risk profile is typically built on the following information: a customer's occupation and income, their location and area of operation, what services they use (credit, foreign exchange, etc.), and the types of transactions they conduct.

Depending on the customer risk level, a business might conduct further due diligence (such as enhanced due diligence, or EDD) before allowing them to complete the onboarding process.

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 as a business need to satisfy now?

What approach will we need for each part of the onboarding and ongoing monitoring processes?

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 market, region, and customer?

Will any solution we consider support different levels of risk tolerance?

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?

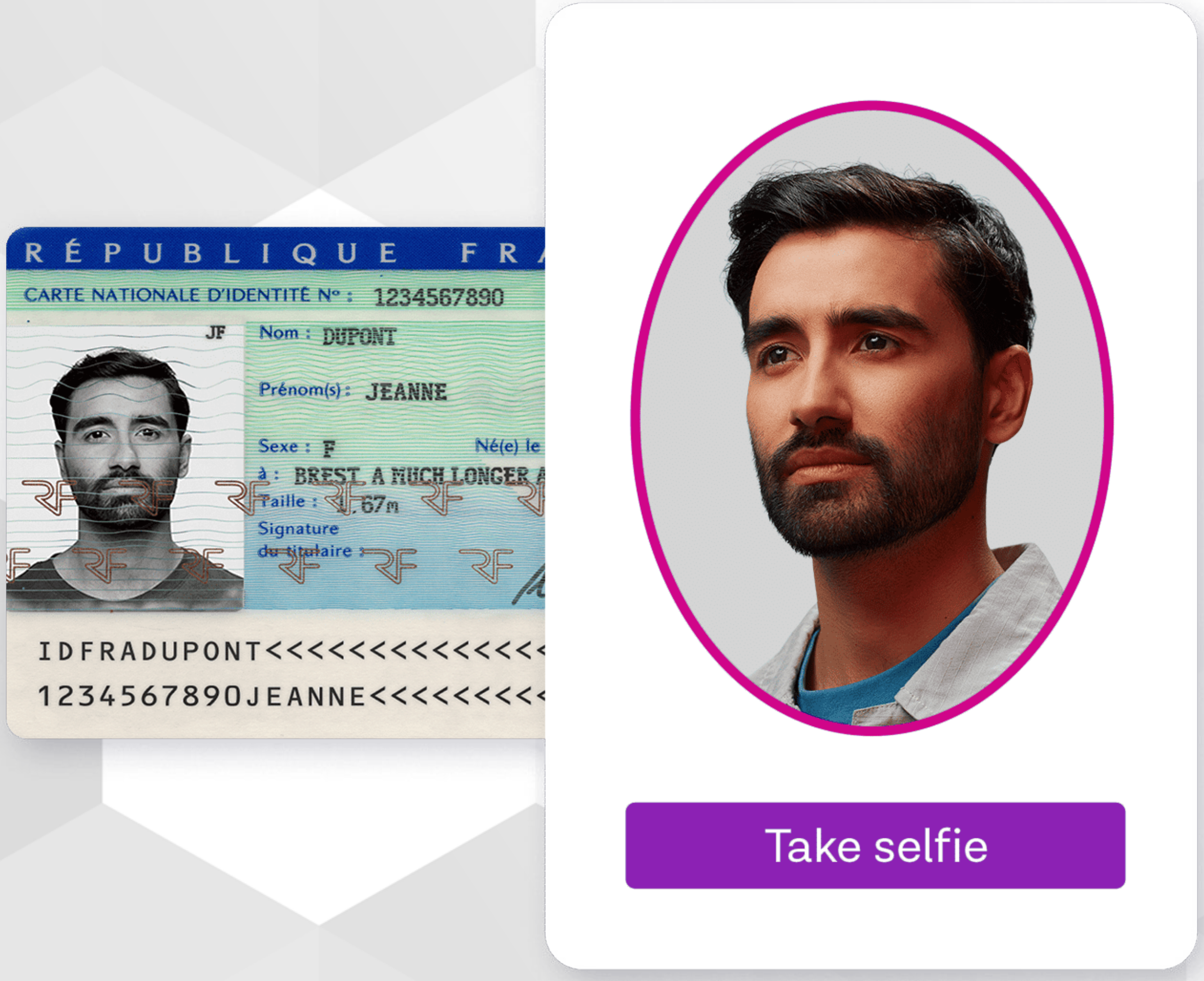
Are we providing a good onboarding experience or a bad one?

Implementation

How easy is it to integrate a vendor versus build and operate in-house?

What is our orchestration plan?

- *Do we need to manage this in-house?*
- *How much of a drain will this be on 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

Product

- Does the vendor have global support for watchlist screening databases?
- Does the vendor support a global range of government-issued 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)?
- 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, ESTI, 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 record-keeping obligations?
- **What's the integration process like?**
  - » Is there comprehensive API documentation?
  - » Is there support for off-the-shelf 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

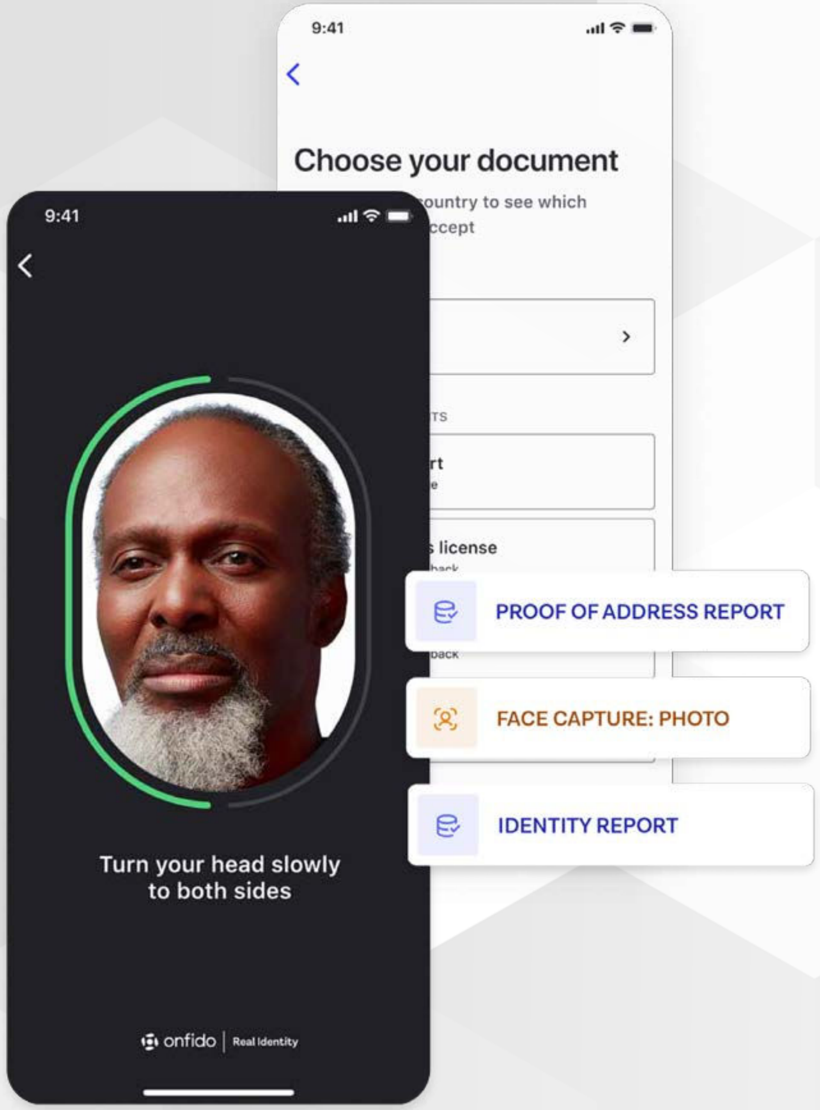
Onfido, an Entrust company, offers its users a suite of verifications, no-code orchestration, and powerful artificial intelligence (AI) to help businesses meet their specific compliance needs.

Verification Suite

A library of global verifications and signals to verify identities with minimum friction, catch sophisticated fraud attacks, and address compliance needs at scale.

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

- Is a real person presenting genuine authoritative evidence of their own identity through government-issued ID (and/or genuine supplementary evidence)
- Is using a trusted device, network, and Onfido SDK to capture all required attributes and evidence.



Document Verification

Verify identity documents such as a government-issued photo ID. Our automated analysis, powered by award-winning AI, classifies documents in milliseconds and supports over 2,500 documents in 195 countries.

Data Verification

Fulfill compliance regulations 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.

Biometric Verification

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

Fraud Detection

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

More information can be found at **Verification Suite** and in our Developer Hub's **Product Guides.**

Studio Workflow Builder

Studio workflow builder 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.

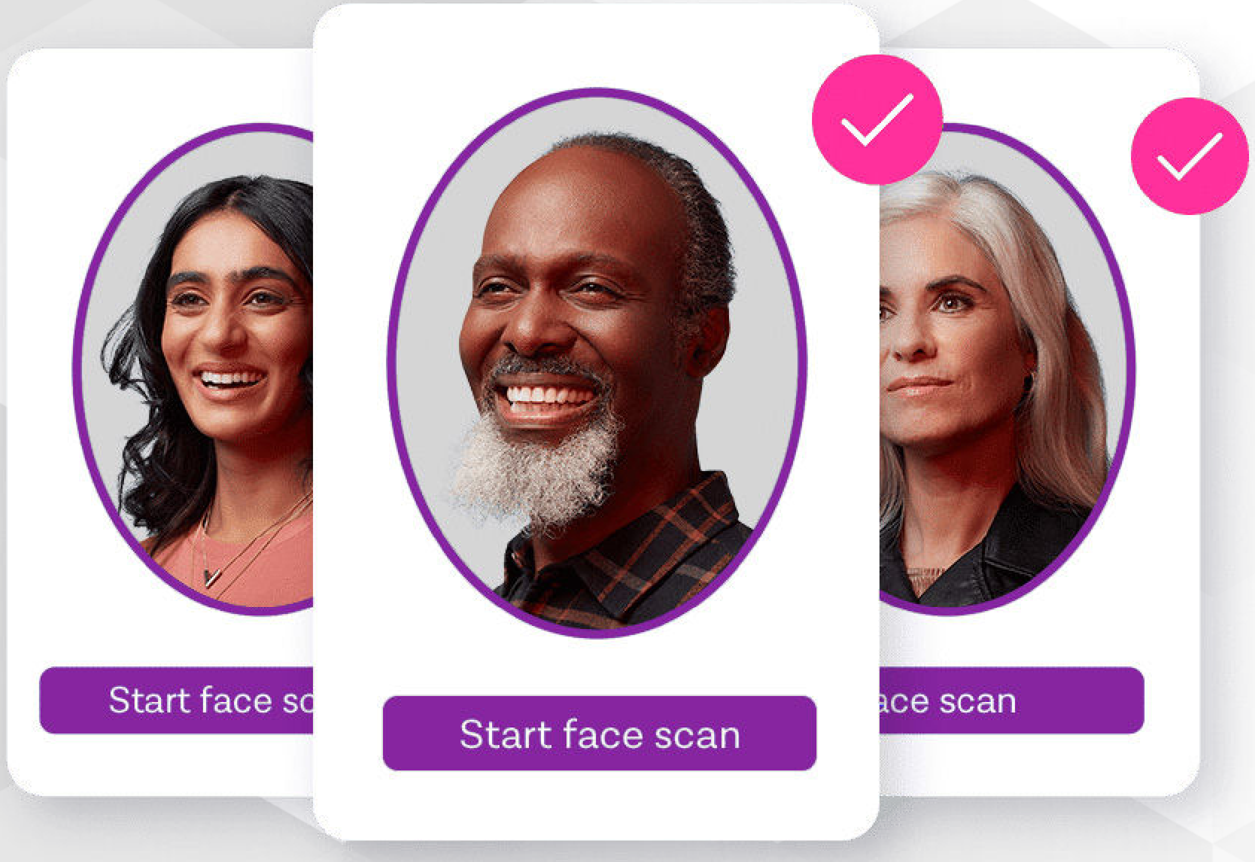
Studio allows businesses to tailor and optimize verification flows that respond to changing market conditions, enabling them to move each user through the right verifications at the right time. They can also easily introduce new verification methods, data sources, and fraud signals to address global regulatory compliance requirements at scale. In turn, Studio empowers organizations to:

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

Analytics and dashboard

Businesses can manage the outcomes of verification checks via the Onfido 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

Onfido, an Entrust company, builds an award-winning AI that's fair, fast, and accurate.

Fair:

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

Fast:

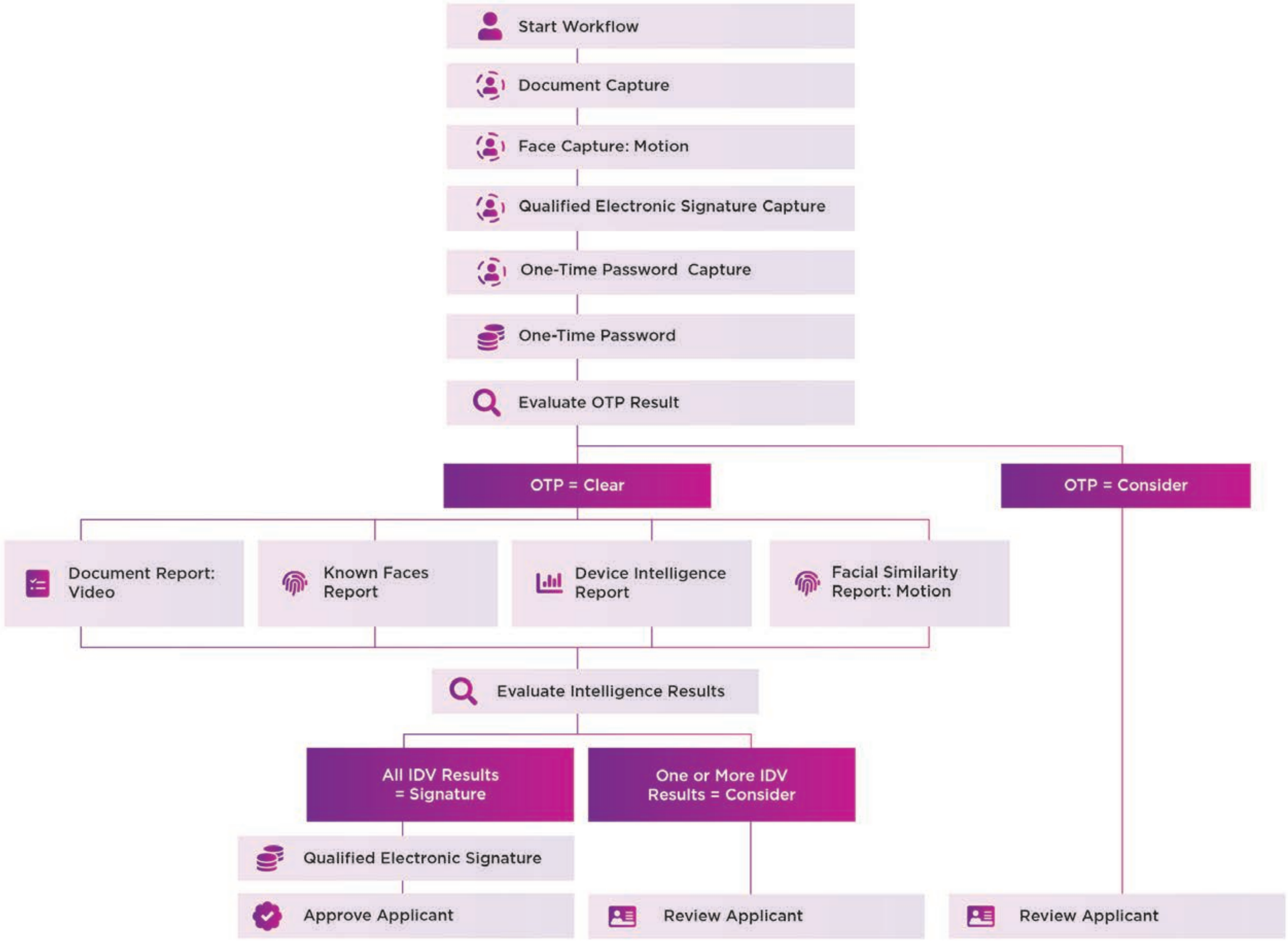
With results returned in seconds, you can make confident decisions without keeping good customers waiting.

Accurate:

It's purpose-built to catch fraud before it impacts your business, protecting you and your customers.

Building and Optimizing Your Onboarding Flow

This section runs through what an example onboarding journey could look like using Studio. The setup is optimized for both KYC/AML compliance (ensuring the business collects and verifies the right data points) and the end customer's experience.



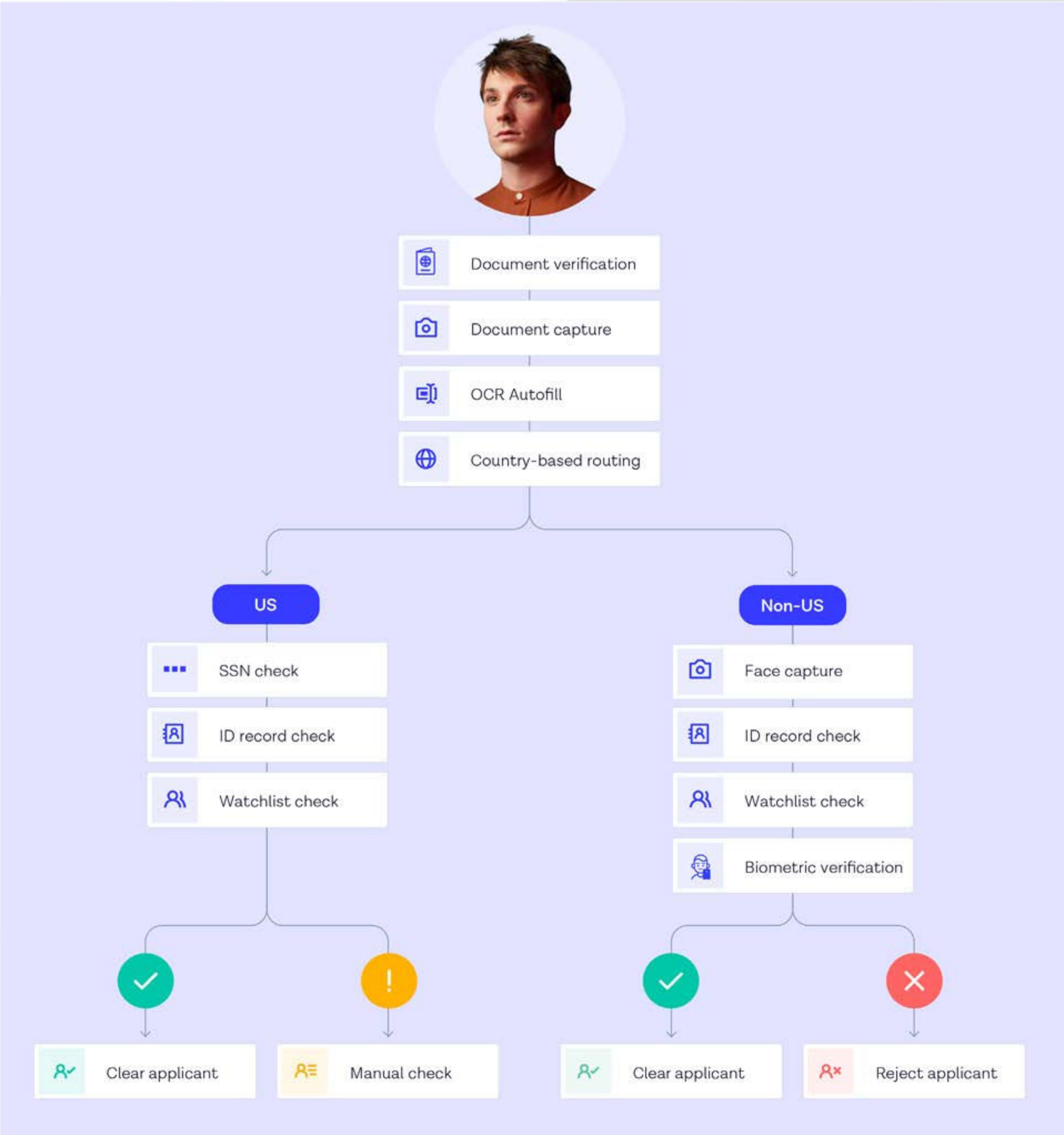
STEP 1

Build Your Onboarding Flow

On the back end, customers can map out their onboarding flow and build it in Studio. No-code, drag-and-drop workflows mean you can build tailored, automated workflows based on market, geography, and customer profile. That's the beauty of Studio — businesses can create sophisticated and automated decisioning minus the complexity.

This example (right) shows a basic onboarding flow that funnels U.S. customers through one workflow, and rest-of-world customers through another. First, we ask a customer to submit their document. We can perform OCR on the ID to extract key information about the user such as their name, date of birth, and the issuing country of their document. For customers with a U.S. document, you might want to run a quick Social Security Number (SSN) check, and for all other customers, you want to run the usual databases and an additional biometric check. If all looks good, the customer may continue with their account opening. If there are issues with any of the database results, you might choose to reject that customer. Or in some cases (such as a name mismatch), simply manually review them internally.

No-code, drag-and-drop workflows mean you can build tailored, automated workflows based on market, geography, and customer profile.



STEP 2

Create the Customer Onboarding Experience

As you build out the flow on the back end, you'll also want to build out the user experience on the front end, considering how this will work for the end user. Below is an example verification experience for the end user as they go through a sign-up flow:

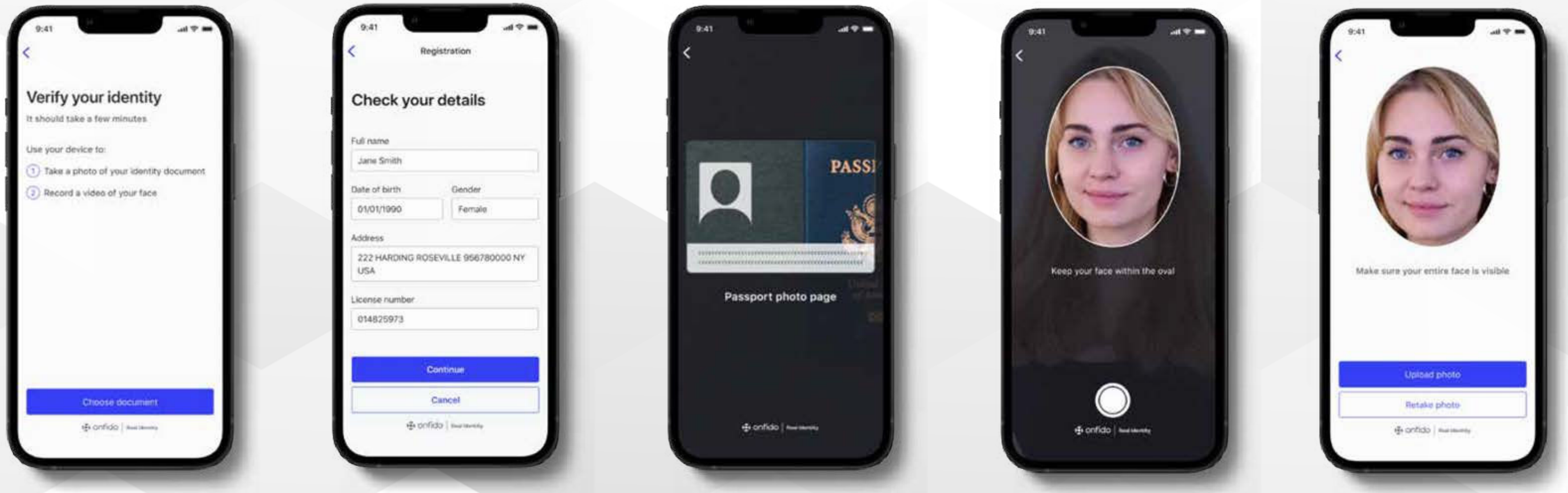
Capturing attributes: The customer starts by entering their personal details.

Identity screening: The business collects the necessary customer information for KYC verification. In the background, identity screening (watchlist, PEPs, and sanctions checks) happens concurrently.

Document verification: The customer takes a photo or video of their government-issued ID. In the background, we check for signs of fraud and that it's a genuine document. If the business uses Autofill, the document's information automatically populates the sign-up fields — saving this customer time and reducing the risk of input errors.

Biometric verification (Selfie or Motion): The customer takes a selfie or captures a video, turning their head. We compare this against the ID to ensure it's a genuine human signing up for the account. We also check for a range of fraud including presentation and injection attacks.

Fraud detection (ongoing checks and passive signals): In the background, we can also conduct passive fraud checks (for example, checking the customer's IP address and geolocation).



STEP 3

Tweak and Test

The dashboard breaks down all the results so you have a clear picture of customer verifications and can understand why decisions have been made at every stage of the workflow. Businesses can automate decisioning and define custom logic to eliminate the need for manual review.

They can also analyze workflow performance and granular results in the dashboard to tweak and test flows in response to market feedback.

Establishing a strong, trusted identity at onboarding is just the first step for businesses. Unfortunately, many institutions treat IDV as a one-time process, overlooking the opportunity to utilize this identity beyond the initial onboarding. This can create friction for end-users during high-risk moments, like transactions, account log-ins, or password resets. With Entrust, Onfido allows businesses to extend the value of the identity verified on day one by leveraging Entrust's Identity as a Service (IDaaS). This enables step-up authentication at critical points, whether securing a user's bank account or ensuring workforce security. This provides ongoing protection well beyond onboarding.

Ready to Make Compliance Your Competitive Advantage?

Discover the Compliance Suite

One provider, one unified onboarding flow, multiple markets. The **Compliance Suite** helps businesses 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.

Get in touch

About Onfido

Onfido, an Entrust company, makes digital identity simple. The platform allows businesses to tailor verification methods to individual user and market needs in a no-code, orchestration layer — combining the right mix of document and biometric verifications, trusted data sources, and passive fraud signals to meet their risk, friction, and regulatory requirements. Partnering with over 1,200 businesses globally, Onfido helps millions of people access services every day — from billion-dollar institutions to hyper-growth start-ups.

About Entrust

Entrust, a global leader in trusted payments, identities, and data security, completed its acquisition of Onfido, a global leader in identity verification in April 2024. Onfido is now a wholly owned subsidiary of Entrust Corporation. Entrust Corporation's leadership and board information can be found here.

Explore platform

Start free trial