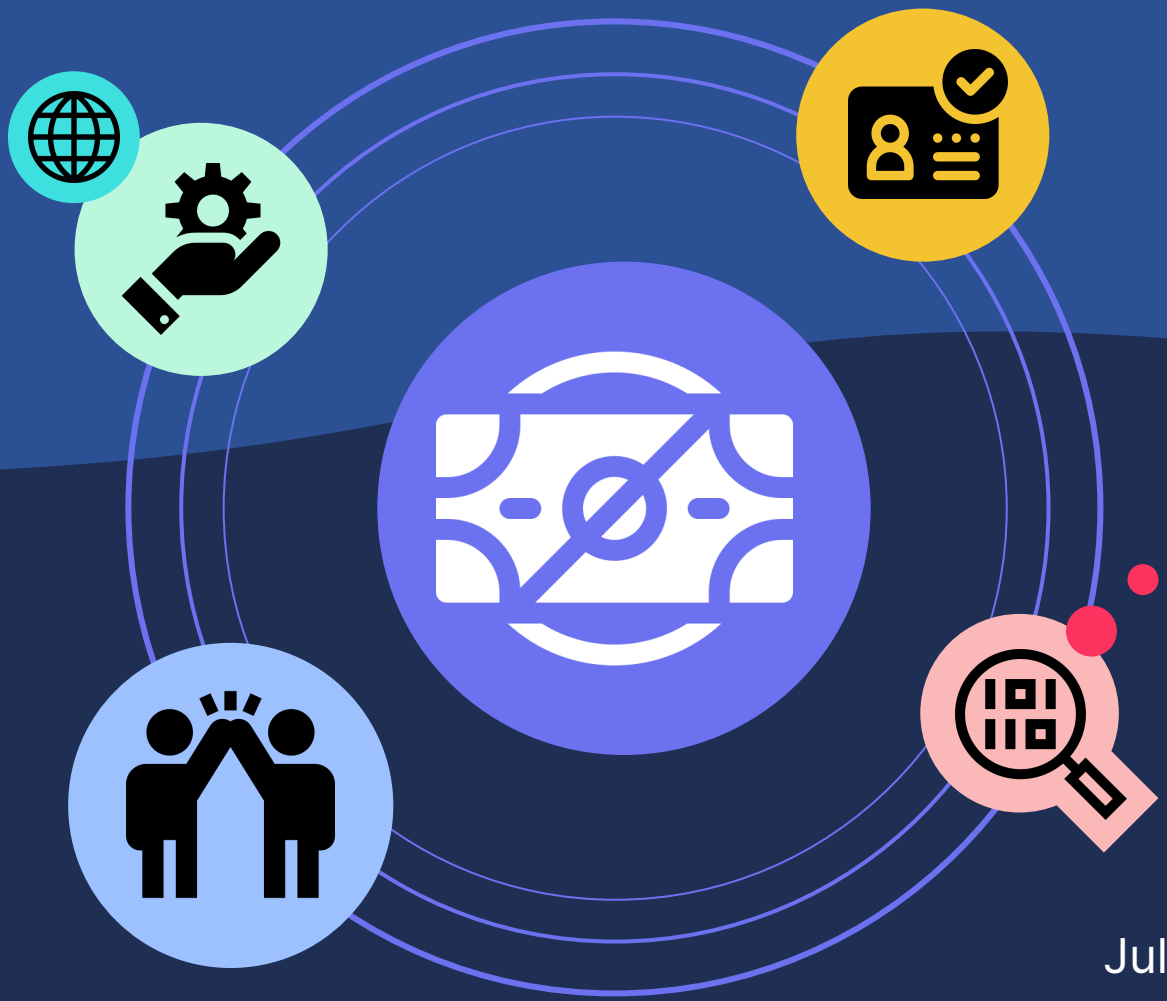
transmit security

TECHNICAL WHITE PAPER

Simplifying Compliance with AML & KYC

Technical white paper



July 2023

Executive summary

Although anti-money laundering (AML) regulations to prevent money laundering have a long history, laws have become increasingly complex over time — resulting in a corresponding increase in fines and penalties. In 2022, $8 billion in fines for AML-related infractions were collected from financial institutions globally — an increase of more than 50% from 2021.[1]

And for digital transactions and account opening, establishing customer identities poses considerable challenges, requiring agile policies capable of quickly adapting to changes in the regulatory landscape and the evasive tactics used by criminals to commit online fraud.

This white paper is designed to help enterprises understand how Transmit Security can help them overcome challenges with AML and KYC through secure digital onboarding and how to orchestrate, monitor and maintain frictionless journeys throughout the customer lifecycle with natively integrated identity security services.

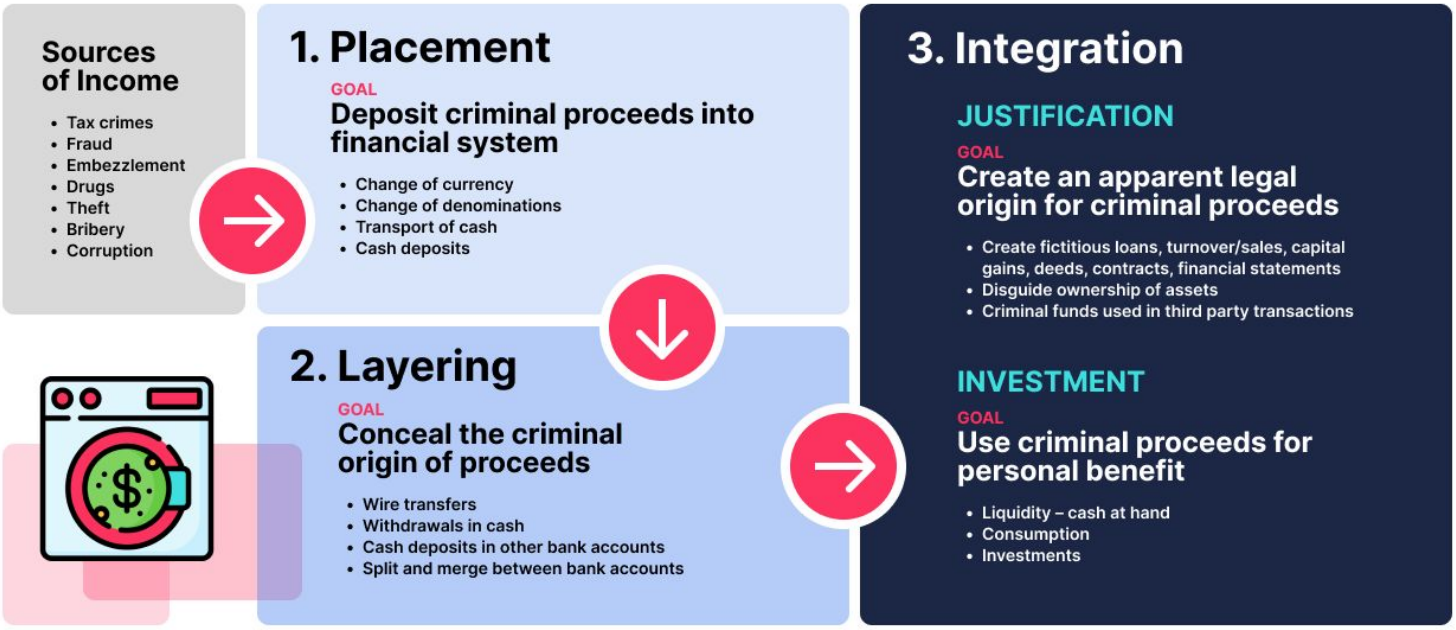
[1] Financial Times

Table of Contents

Understanding AML & KYC

Money laundering is a process used by criminals to deposit, receive or transfer funds from illicit activities like terrorist financing and human trafficking. In an attempt to make these transactions appear legitimate, criminals take steps such as moving funds around to disguise their source, breaking up large sums into multiple small deposits to evade scrutiny or conducting transactions in countries with less stringent monitoring of financial activity.

Overview of Money Laundering



Source: Organisation for Economic Co-operation and Development, ***Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*** (OECD, 2009), www.oecd.org/tax/crime

AML laws and regulations are processes that businesses handling large or significant financial transactions must abide by in order to prevent money laundering, In the process, AML regulations make it more difficult to profit off of criminal activity.

While specific AML laws vary by region, the basic components of these regulations include:

- Pre-onboarding ID verification checks and checks against AML databases
- Assessment and monitoring of customer risk
- Record keeping for auditing
- Policies and training to keep employees up to date

Although AML is traditionally considered the purview of banks and credit unions, global and regional regulations apply to a wide range of businesses to monitor customers for signs of money laundering and financial crimes, including:

- banks & credit unions
- insurance companies
- digital wallet providers
- cryptocurrency exchanges
- gambling entities
- payment processing companies
- lending platforms & wealth management services
- high-value retail businesses

Secure customer onboarding with KYC

Know Your Customer is a specific component of AML that regulates how businesses verify customer identities and assess risk prior to onboarding. By implementing thorough pre-onboarding background checks, KYC aims to prevent criminals from opening accounts that could be used for illicit transactions and stop money laundering before it can begin.

To maintain compliance with KYC, regulated enterprises must:

- Identify and verify all customers and beneficial ownerships through a Customer Identification Program
- Understand customer relationships and their risk profiles during Customer Due Diligence
- Perform verification with various data sources throughout the process
- Continue ongoing monitoring of customers and their transactions

A complex and evolving landscape

AML laws are established and enforced by a variety of global and country-specific organizations. These regulations change over time to address new industries, evolving risks, digitalization and fraud innovation, especially with regard to the rapidly changing online threat landscape.

To ensure compliance with frequent changes to AML laws enacted by regulatory bodies around the world, businesses must continually assess and adapt their AML policies. For example, in 2023, multiple updates to AML policies are in the works worldwide, including:

1. Regulations set by the Financial Action Task Force (FATF) to align with 2022 priorities set by the new Singapore presidency.[2]
2. Changes to U.S. policy designed to modernize regulatory frameworks, especially in the cryptocurrency space.[3]
3. Additional initiatives from the European Union targeting environmental crime and action on a rising number of cross-border money laundering cases.[4]

Because of these rapidly changing requirements, which are regulated by both international and country-specific laws and governing bodies, businesses must have clear visibility into customer activity, easily understand decisioning rules and be able to rapidly deploy updates to customer journeys to comply with various AML regulations.

[2] FATF, "Objectives for the FATF during the Singapore Presidency 2022-2024"
[3] White House Executive Order
[4] European Parliament Report

Challenges of digital AML & KYC programs

Implementing strong AML & KYC programs can be a challenge for any enterprise, but developing digital processes to verify customer identities and assess risks online can be especially complex. New technologies and an increase in organized crime are making it harder than ever to spot instances of online identity fraud, and with sophisticated criminals, even large-scale campaigns can go unnoticed.

Further adding to this challenge is the need to facilitate online experiences for legitimate customers that are not only secure, but minimize friction that can lead to dropoffs. Unlike in-person account openings, where individuals anticipate wait times and need to physically leave a branch in order to open an account with another provider, online users are only a click away from competitors and will often abandon account opening in the face of long wait times or cumbersome registration procedures.

To maintain compliance, prevent fraud and improve customer conversion rates, businesses must look for identity security solutions capable of overcoming the key challenges of digital AML and KYC programs, which are outlined in this section.

Customer Identification Program

Within KYC, online Customer Identification Programs are intended to collect information from customers to confirm their identity and ensure that they are who they claim to be.

Online Customer Identification Programs are generally composed of four key elements, each of which present their own unique challenges:

1. **Collecting customer information:** Businesses are required to collect each customer's name, date of birth, address and tax ID number. This information can be entered by the customer manually or extracted automatically from a scanned ID.

   A key challenge during this step is identity fraud that leverages the widespread availability of customer data on dark web marketplaces. With a low barrier for entry, fraudsters may steal legitimate customers' identities by using leaked data in full or by mixing stolen data with fabricated information — a technique known as synthetic identity fraud.

2. **Validating customer-provided data with third-party databases:** To quickly detect synthetic identity fraud and the use of stolen identities, customer-provided data must be verified with third-party sources to ensure that it is valid and strongly associated with the user's claimed identity.

   However, because different information is validated by different services, creating online processes to validate all the customer data needed for AML compliance requires extensive vetting and licensing, as well as complex third-party integrations in order to aggregate global data sources. This leads to high overhead, increases time-to-market and requires expertise to design, deploy, update and maintain.

3. **Assessing the validity of IDs and other necessary documents:** Strongly identifying users under KYC also requires assessing the authenticity of one or more official documents provided by customers, typically a driver's license or passport, to ensure the ID is unexpired and exhibits no sign of forgery or tampering.

   But whereas in-person assessment gives experts the ability to physically examine documents for signs of tampering, using manual inspections to review documents online is time consuming, difficult to scale and eliminates the ability to touch and feel documents for signs of alteration or view missing elements such as holograms and fine-line patterns that are only visible in certain light.

In addition, organized crime such as online marketplaces for stolen IDs or high-end forgeries lowers the bar for fraudsters to obtain realistic IDs, whereas high-end printers give cybercriminals the ability to copy advanced security features that were previously difficult or even impossible to replicate.

4. **Biometric authentication and liveness detection:** To verify the physical presence of the customer and ensure their identity is aligned with the document owner, electronic KYC programs must perform biometric authentication with liveness checks, typically by requiring customers to submit a selfie as part of the ID verification process.

   However, fraudsters can circumvent liveness checks by using printouts, masks, cutouts, or digital photos of the ID owner to fool standard liveness screenings — a technique known as a presentation attack.

   In addition, companies that use machine-learning systems to match and assess user selfies are often black boxes that do not explain the rationale behind their judgements and are prone to bias, which can result in discrimination against certain genders, age groups or races — requiring vendors to implement anti-bias measures to ensure a positive and fair user experience for all users.

Customer Due Diligence

Once customers have been identified and their personal information has been validated, businesses must assess the individual's risk level through a process known as Customer Due Diligence and determine if additional screenings — known as Enhanced Due Diligence (EDD) — are required. After the onboarding process is completed, continuous monitoring is also needed to trigger re-verification during suspicious or high-risk activities, or in the event of changes to the individual's business or account that impact their risk profile.

As with Customer Identification Programs, each of these stages present unique challenges for businesses to ensure that their digital onboarding and monitoring processes comply with KYC and AML requirements:

1. **Risk Assessment:** The first step in Customer Due Diligence is to assess the customers' risk profile by checking government watchlists for sanctions against them and determining if there are other factors that might impact their risk level with regard to money laundering. This includes high-net worth individuals and politically exposed persons (PEP), who are required to undergo additional screenings for KYC compliance.

   But performing these checks one at a time or manually can lead to long customer wait times and dropoffs. And because PEP is defined according to the government position that the individual holds — rather than their name — information stored in static databases and PDFs can quickly go stale, making it all the more crucial that businesses validate this information with dynamic, up-to-date sources.

2. **Enhanced Due Diligence:** Individuals that fit into a higher risk profile must undergo Enhanced Due Diligence, which may include gathering further customer information, performing checks with additional sources or gaining more information about the nature of the customer's business relationships.

   However, creating workflows to automate these subjourneys is a complex task as regulations may vary from country to country and depend on the specific risk profile of the user. As a result of this complexity, identity decisioning — already complicated through the use of multiple IDPs and databases — can result in a patchwork of overlapping rules that are hard to understand. This makes it difficult to see how new rules might impact other areas of business, hinders collaboration with stakeholders and adds overhead due to the time and expertise needed to build and maintain decisioning logic.

3. **Ongoing monitoring and re-verification:** After customers are safely onboarded, AML compliance requires ongoing monitoring to spot changes to each customer's risk level and anomalies that might indicate a compromised account — requiring reverification of the customer's identity and, if needed, Enhanced Due Diligence steps such as verifying the source of funds to address increased risk levels.

   Common reverification triggers include:

   - Large and high-volume transactions
   - Occupational changes or newly available information about the customer
   - Changes to the nature of the customer's business with the organization
   - New parties added to a customer's account
   - Overseas transactions, especially with high-risk countries that do not maintain strict AML screening requirements
   - Transactions with individuals that are deemed high risk

However, orchestrating these reverification triggers can be difficult for businesses, as it requires the creation of complex journeys and subjourneys. And when these journeys require significant custom code to stitch together various IDPs and databases where customer information is stored, decisioning logic becomes even more complicated, making it hard for risk, fraud and other teams to update or even understand EDD journeys.

Record keeping and documentation

As with any regulations businesses must abide by, AML and KYC compliance requires record keeping and documentation for auditing purposes. For AML compliance, businesses must maintain records of each customer's identifying information, descriptions of the ID used to verify their identity and the methods and actions taken to verify the customer's identity and perform due diligence, along with their results.

However, maintaining centralized records can be a challenge for modern enterprises, who often rely on multiple IDPs, third-party solutions and customer databases. In addition, explaining the specific risks and anomalies that triggered reverifications or Enhanced Due Diligence can be difficult or even impossible when using machine-learning algorithms that deliver opaque risk assessments without sufficient explainability into the anomalies or behaviors that were deemed risky.

How Transmit Security solves AML & KYC challenges

How Identity Verification works on the Transmit Security Platform

Transmit Security's Identity Verification Services meet AML & KYC challenges using a fast, accurate and user-friendly process with broad support for documents worldwide and automatic scaling designed for planet-scale enterprise workloads.

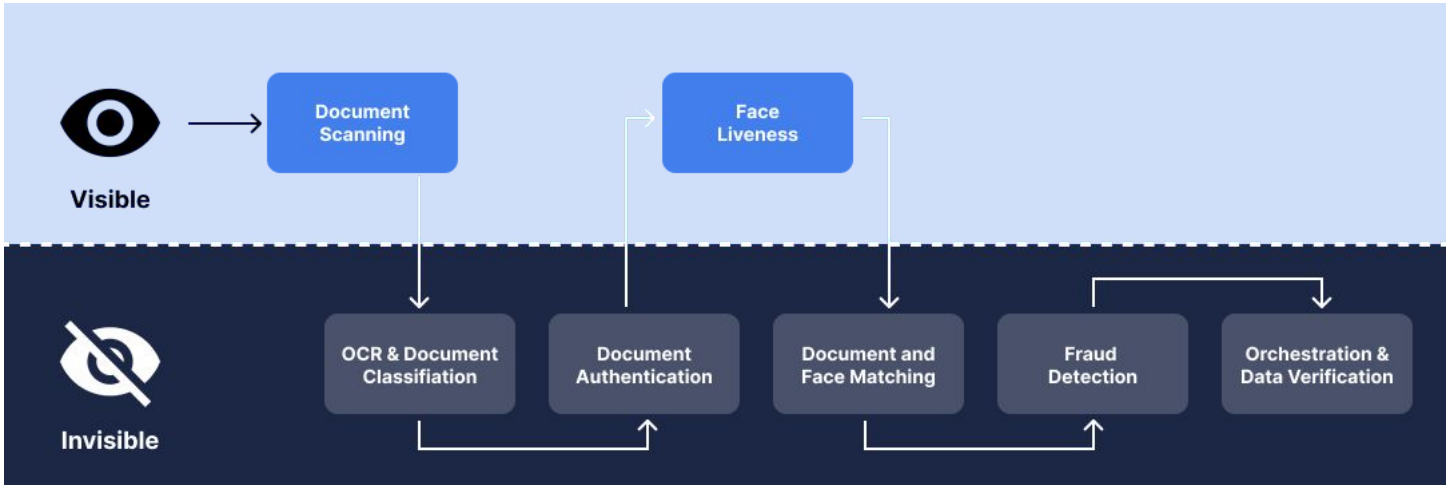
Key performance metrics include:

- Support for more than 10,000 supported document types worldwide
- 3.6s median response time
- 99.5% accuracy

The process streamlines the user experience by automatically extracting user data to complete registration forms, and the process is fully automated, with an option to include human overview from in-house analysts or third-party experts that are available 24/7 and typically complete the process in 12-47 seconds.

While end users only need to complete two steps, third-party data verification with pre-integrated sources and multi-method fraud detection is performed passively, enabling the highest level of assurance in user identities without the need for additional user interaction.

The visible and behind-the-scenes processes can be visualized in the diagram below.



Customer Identification Program

Identity Verification helps businesses overcome challenges in establishing Customer Identification Programs at each step of the process:

- **Collecting customer information:** Identity Verification uses OCR (optical character recognition) and state-of-the-art (SOTA) deep learning techniques to automatically extract the customer's information from their scanned ID, reducing the steps customers need to take in order to complete the process.

  At the same time, Detection and Response Services begin running in the background, using multiple detection methods such as device reputation, bot detection, behavioral biometrics, user activity, network reputation and threat intelligence to detect risk signals that could indicate synthetic identity fraud.

- **Validating customer data:** On the Transmit Security Platform, Data Validation Services validates customer information through vetted and pre-integrated third-party databases, which run concurrent checks to check for individuals that have reported identity theft and ensure that the data provided is strongly associated with the customer.

- **Assessing document authenticity:** Identity Verification maps the ID to the correct country and version to check for formatting anomalies and security features on the ID, as well as other signs of ID fraud, such as glued or stamped elements, incorrect printing technologies or wrong dimensions.

  Customer information extracted from the visual inspection zone is also cross-checked against machine readable elements, such as the MRZ and NFC chips, in order to detect inconsistencies that indicate fraud or tampering.

- **Biometric authentication and liveness detection:** Liveness detection is performed to ensure the customer is present and to match their ID photo while checking for presentation attacks, including masks, cutouts, photos and video replays. To mitigate demographic bias that can result in false positives, Identity Verification uses large and diverse datasets that are dynamically weighted to reduce disparities in error rates across age groups, genders or races.

Customer Due Diligence

During the Customer Due Diligence process, native integration with Data Validation, Identity Orchestration and Detection and Response Services help businesses orchestrate workflows to assess customers' risk profiles, perform EDD when necessary and provide ongoing monitoring to detect changes that require re-verification.

- **Risk assessment:** To assess customers' risk profiles, Data Validation enables businesses to instantly and automatically perform concurrent checks against PEP, sanctions and other watchlists. This lets them assess customer risk with the most up-to-date info to prevent delays that could occur with manual review or outdated information that can lead to error when using static info stored in PDFs and spreadsheets.

- **Enhanced Due Diligence:** Native integration with Identity Orchestration Services lets teams orchestrate EDD and other advanced checks needed for business or regulatory needs using no-code and low-code drag-and-drop journeys that are easy for teams to understand, deploy and update.

To further simplify decisioning, Identity Orchestration leverages pre-built integrations and can sit on top of any third-party service or IDP and incorporate sophisticated policy enforcement into decisioning with serial, parallel or sequenced calls.

- **Ongoing monitoring:** Detection and Response monitors customers throughout the entire end-to-end lifecycle, building a profile of trusted behavior for each customer that is used to detect anomalies that might indicate ATO or other fraudulent behavior. Low-code and no-code workflows enable teams to quickly create customer journeys and subjourneys to trigger re-verification for events such as transactions above a certain threshold or transactions with high-risk countries.

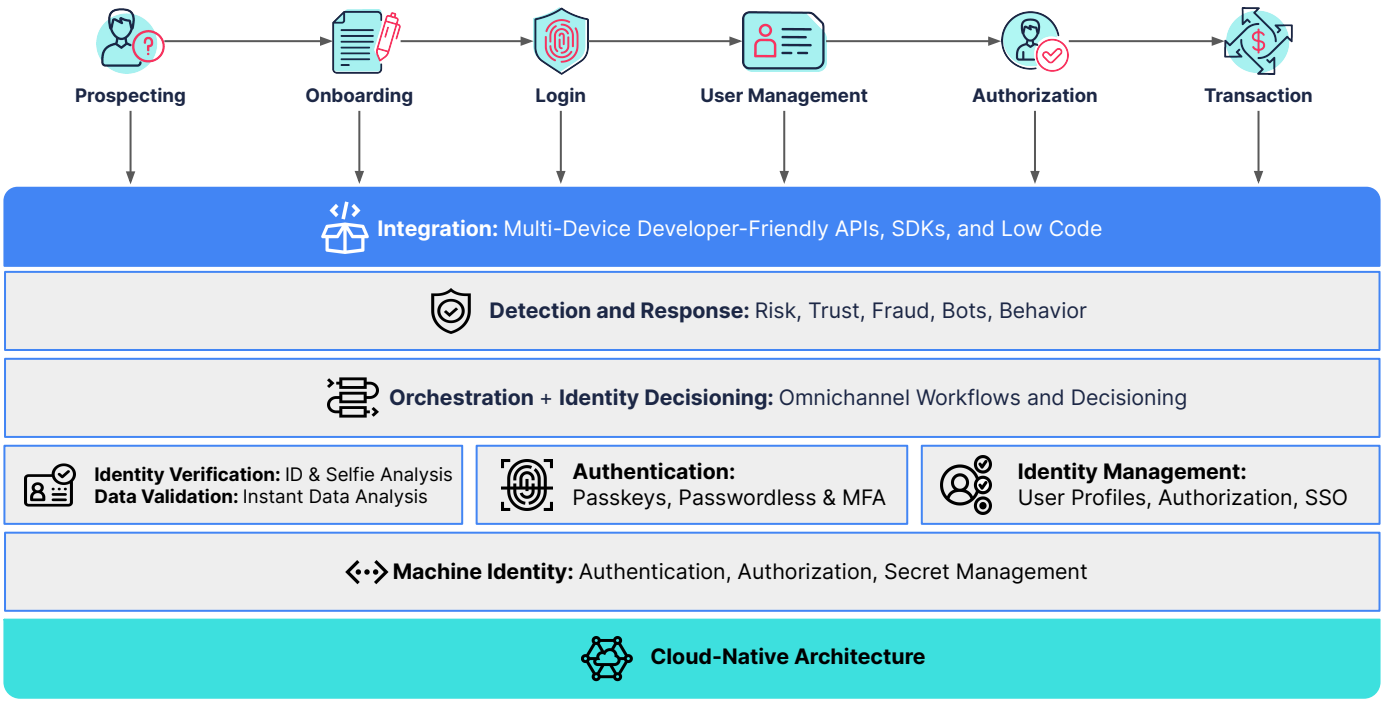
In addition to these capabilities, Transmit Security's Decisioning Rules integrate with Identity Verification, Data Validation and Detection and Response, allowing teams to quickly adapt to changing regulations with no-code custom decisioning logic that can be easily updated and safely deployed through an easy-to-use UI or API.

Record keeping and documentation

To simplify record keeping and documentation needed for auditing and compliance, all Detection and Response risk signals, Data Validation checks and Identity Verification results are stored centrally, enabling businesses to easily access everything they need in one place.

Model explainability for Detection and Response's machine-learning-based risk engine is provided through the use of SHAP values, which provide transparency into the top factors that trigger Trust, Allow, Challenge and Deny recommendations — enabling businesses to not only explain anomalies in customer activity that triggered re-verification for auditing purposes, but understand the model's decisioning logic and easily tune it to optimize results.

In addition to natively integrated services for Data Validation, Identity Orchestration and Detection and Response, Transmit Security is the only vendor that offers platform-native identity verification woven into the fabric of a complete identity platform, including modular, API-first services for Authentication and Identity Management Services, enabling unified experiences and a holistic view of customers across applications and channels.



All services can all be accessed through a centralized portal, enabling businesses to further simplify record keeping and documentation through IDP consolidation.

Conclusion

Establishing and maintaining digital KYC and AML programs can be a difficult task for modern enterprises, but combining identity Verification Services with natively integrated Identity Orchestration, Data Validation, Detection and Response and other identity services provide a way forward.

And with Transmit Security's advanced identity security capabilities, enterprises can overcome many of the common challenges with KYC and AML to reduce the risk of identity fraud, money laundering and regulatory fines — all while ensuring a positive customer experience that minimizes friction to reduce dropoffs.

About Transmit Security

Transmit Security gives businesses the modern tools they need to build secure, trusted and end-to-end digital identity journeys to innovate and grow. CX-focused, cybersecurity-conscious leaders rely on the Transmit Security Platform to provide their customers with smooth experiences protected from fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers, and other leading brands, collectively responsible for more than $1.3 trillion in annual commerce.