The Dawn of END-TO-END AML COMPLIANCE

jumio

Introduction

The history of anti-money laundering (AML) regulations began in 1970 with the creation of the Bank Secrecy Act (BSA). Its mission was to "safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity."

Since then, numerous laws have enhanced and amended the BSA to provide law enforcement and regulatory agencies with the most effective tools to combat money laundering, including the Money Laundering Control Act (1986), the Money Laundering Suppression Act (1994) and the USA PATRIOT Act (2001), among others.

Each amendment and law adds a layer of complexity and burden to the compliance teams of regulated institutions. The complexity is aggravated by the number of different solutions that need to be managed and orchestrated to satisfy different aspects of these regulations. These include:

- **Know Your Customer (KYC)**
- **AML screening (sanctions, politically exposed persons, adverse media)**
- **Transaction monitoring**
- **Investigations and case management**

Collectively, AML regulations and their different components have resulted in specializations and silos. There are often separate teams that oversee their own piece of the AML puzzle, each managing different software programs and implementing their own sets of processes. Unfortunately, this has led to operational inefficiencies where data is lost and threats are not properly identified.

Additionally, firms face huge challenges with tuning their compliance rules. Tight thresholds can drown your compliance teams with way too many false positives, while loose thresholds can allow nefarious activity to go undetected. The challenge is to find the right balance, and there is no single right answer. Regulators have made it clear that compliance departments must be adequately staffed to address the resulting case volume, and it is not acceptable to simply relax thresholds to meet compliance staffing constraints.

The aim of an AML compliance program is to expose and correctly react to money laundering, terrorist financing and fraud-related risks. If your technology stack and internal processes are efficient and integrated, you improve your chances of identifying these risks without overburdening your teams.

AML Challenges of Fintechs and Marketplaces

Fintechs and marketplaces face their own set of challenges. They are subject to the same regulations, sanctions and fines as traditional financial institutions, but they don't have the compliance infrastructure and labor resources of their larger counterparts. They typically don't have any face-to-face interaction with their customers, which complicates the ID verification process. And many of these organizations must meet the compliance requirements of a sponsor bank that lacks visibility into the fintech's business data. Other organizations such as sharing-economy platforms face similar challenges, even though they don't engage in any financial services.

Repeating the Same Mistakes

Failures in compliance processes cause firms to face heavy penalties. Yet AML fines continue to rise each year because many financial institutions continue to make the same mistakes.

While the AML fines in 2018 were about $4 billion globally, they doubled to approximately $8 billion in 2019. When we examine some of the data announced in 2020, we see that the AML penalties in the first half of 2020 are close to $6 billion … on pace for another significant increase (source: Fenergo, August 2020).

AML Fines by the Numbers

Swedbank

€360 million

Deutsche Bank

$216.1 million

SEB

$107 million

Commerzbank

£ 37.8 million

Guotai Junan Securities

$25.2 million

The most recent penalties stem from compliance lapses highlighted since 2015, including insufficient due diligence on new clients, improper management of AML programs, poor transaction monitoring and a failure to ensure adherence to the rules.

Financial institutions face strict regulatory scrutiny due to their frequent use by money launderers. They need to comply with a regulatory landscape that is in a constant state of change. Non-compliance can lead to hefty fines, criminal proceedings and sanctions. Unfortunately, many firms keep making the same compliance mistakes and struggle to meet their regulatory obligations despite the repeated messages in these enforcement cases. The enduring problems reflect a lack of resourcing and the reliance on legacy systems that can't keep up with the changing trends in financial crimes.

Key AML Failings

In their Global Enforcement Review (August 2020), global advisory firm Duff & Phelps highlighted the four key AML failings from 2015-2020 that regulators across the world have consistently identified through the fines they imposed:

KYC/customer due diligence	115 significant cases
AML management	109 cases
Suspicious activity monitoring	82 cases
Compliance monitoring and oversight	62 cases

Know Your Customer

What is Know Your Customer?

Know Your Customer (KYC) is the process of gathering data, verifying the identity and understanding the risks associated with doing business with a particular customer. In practice, this means obtaining key customer data such as name, address, date of birth and an official document with their photograph that confirms their identity. They must also be screened to ensure that they are not on any sanctions lists and are not a politically exposed person (PEP). KYC also encompasses customer due diligence (CDD), which is the process of assessing the risk both during the onboarding process and on an ongoing basis.

Key Ingredients

At the heart of KYC are three processes designed to thwart the growing threat of money laundering:

Identity Proofing

According to Gartner, identity proofing describes a set of tools that provide confidence in the genuine presence of the identity owner. For example, requiring an online user to take a photo of their government-issued ID and a corroborating selfie (with some embedded liveness checks to ensure the person is physically present) qualifies as identity proofing. Unfortunately, many regulated institutions still rely exclusively on data-centric methods (e.g., pinging a credit bureau) that do not provide the same level of identity assurance.

Screening

Financial institutions and fintechs must check their customers against global/regional watchlists for sanctions, PEPs and adverse media. Often this step is performed when a new user creates an account, at which point the individual is screened. Regulated companies also need to stay on top of changes in risk status of existing customers. This means being alerted if any of your existing customers end up on a watchlist.

Risk Scoring

With the growing sophistication of money laundering schemes, a robust risk scoring framework is required to effectively capture customer risk — not just during onboarding but on a continuous, dynamic basis. Unfortunately, a one-size-fits-all approach no longer makes sense. Firms must develop risk scores for various customer categories (e.g., individuals, corporations, government bodies), as every customer type has different risk parameters. For example, the source of wealth and nationality would be risk factors for an individual customer whereas the ownership pattern and products offered would contribute to a corporation's risk score.

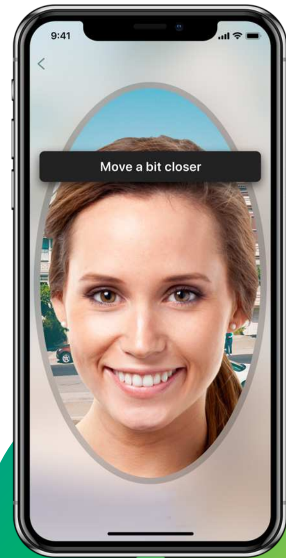
How KYC Works

ID Proofing Check

Is the ID document authentic and valid?

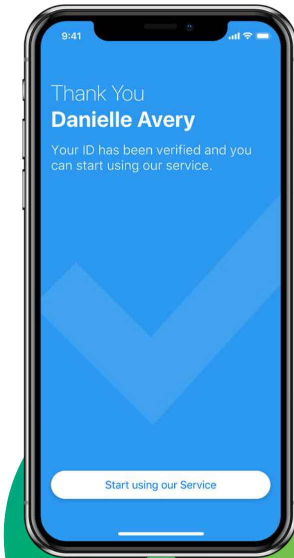
Similarity Check

Is the person holding the ID the same person shown in the ID photo?



Liveness Check

Is the person holding the ID physically present during the transaction?



Definitive Answer

Jumio instantly delivers a definitive yes or no answer.

"By 2022,

80%

of organizations will be using document-centric identity proofing as part of their onboarding workflows, which is an increase from approximately 30% today."

Gartner, 2020 Market Guide for Identity Proofing and Affirmation

Transaction Monitoring

What is Trandsaction Monitoring?

Transaction monitoring refers to monitoring customer accounts and activity for illegal behavior, and it is a primary tool in helping to detect and prevent money laundering and terrorist financing. It involves assessing historical/current customer information and interactions to provide a complete picture of customer activity. In addition to traditional transaction types like deposits, withdrawals and wire transfers, transaction monitoring should include P2P transfers, currency exchanges and even profile updates such as an address change.

AML laws state that when suspicious transactions occur, the financial institution must act quickly to investigate. The firm must confirm that nothing illegal has taken place or perform a regulatory filing with the proper authorities, such as filing a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN) in the United States.

How it Works

An advanced AML transaction monitoring solution will create a profile of each customer's financial habits and history and then track transactions to identify patterns and trends. It looks for anomalies or deviations in transaction types, amounts, frequencies and more. When the solution discovers suspicious activity, it sends an alert so that the financial institution can take the necessary steps.

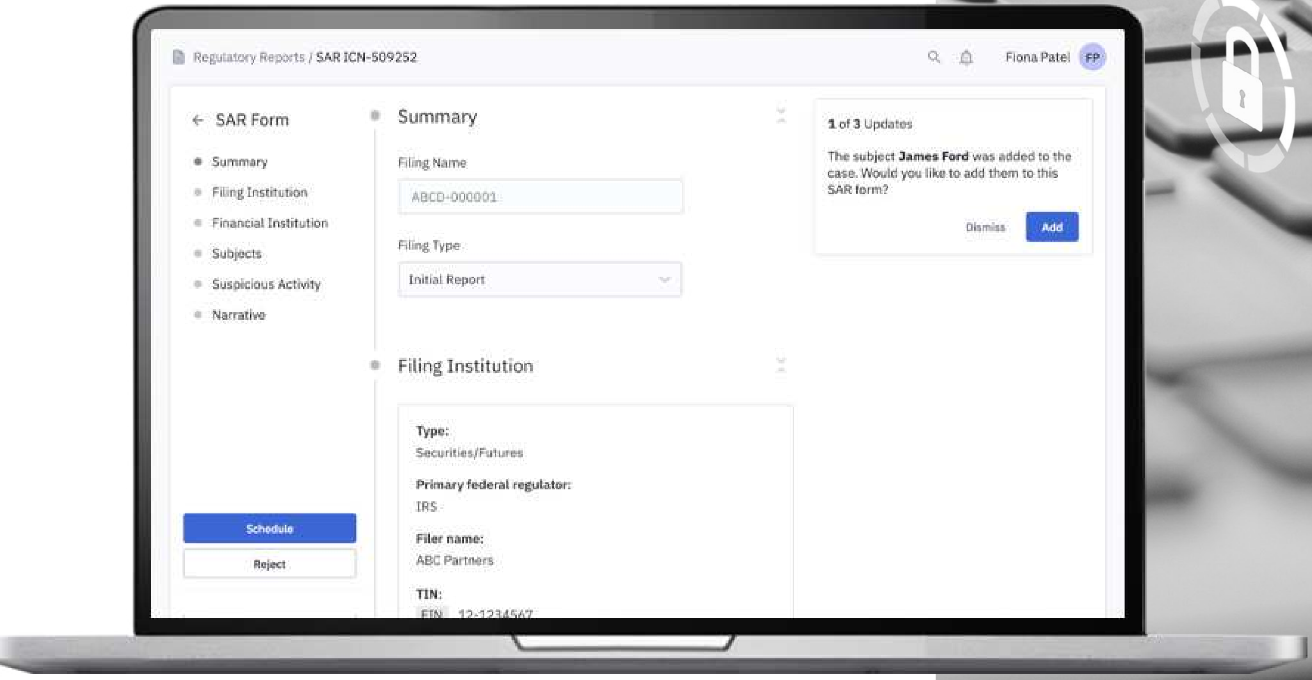
Over time, the system can refine customer profiles using their ongoing transactions and other financial activity. This allows suspicious activity to be flagged faster and more effectively.

AML Compliance is Moving to the Cloud

The transaction monitoring space has long been dominated by legacy, on-premises solution providers. Historically, traditional client-server software was selected by IT departments that wanted to have total control over the implementation.

However, these types of deployments often take a year or more to go into production and consequently suffer from slow time-to-value. Furthermore, the IT staff will have to develop expertise in maintaining compliance software, and the overall cost of this approach is prohibitive for many companies.

Solutions that take advantage of cloud infrastructure can be deployed much more rapidly than on-premises solutions and are ideal for distributed investigation teams. Plus, they're increasingly adept at withstanding regulatory scrutiny thanks to their enterprise-class security safeguards, audit trails and advanced reporting capabilities. The result is a compliance solution that's more efficient and effective … at a significantly lower cost.]



Key Ingredients of Transaction Monitoring

A robust transaction monitoring solution includes these key ingredients:

Advanced Detection

Legacy systems based on static rules can only identify the most basic money laundering vectors. Modern AML detection incorporates machine learning to analyze vast amounts of data and adaptively search for subtle trends and patterns. Another way to improve detection is to establish different rules or thresholds for various populations based on factors such as risk level, geography or account type.

Reducing False Positives

One issue for both regulators and regulated institutions is excessive volumes of false positive activity alerts. False positives can undermine the efficiency and efficacy of a compliance program, and they can erroneously disguise actual illegitimate activity. The more modern approach leverages machine learning algorithms to learn from the results of every investigation. This allows the system to identify ways to improve detection, such as adjusting a threshold or adding an additional data factor, so your detection models constantly improve.

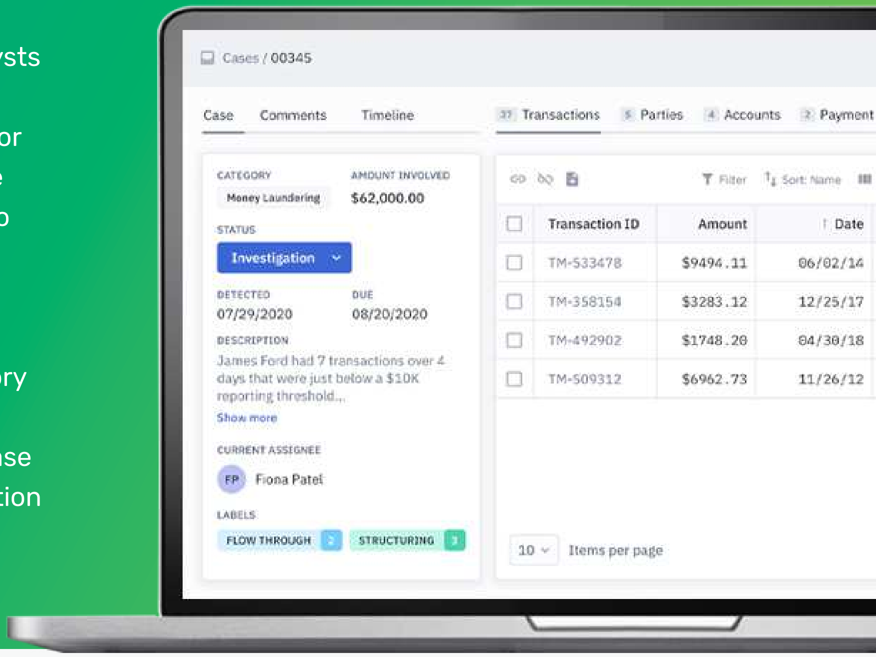
Data Enrichment

Advanced solutions allow firms to embed their own data sets in the transaction monitoring solution and leverage online sources like social media to enrich the data and flag suspicious activity. For example, if a customer is applying for a loan, it's prudent to ensure that the loan amount isn't greater than the value of the home, that the customer's stated income is typical for their profession and that their stated profession matches their social media profiles. Regulated institutions also routinely integrate with third-party services that specialize in identity verification through various channels, such as a customer's device settings and geolocation, to give analysts all the information needed to satisfy KYC requirements.

Case Management

What is Case Management?

Case management is the critical step where analysts at regulated organizations review and investigate suspicious activity that was detected by the KYC or transaction monitoring system. Increasingly, case management functionality is being integrated into those detection solutions in order to streamline compliance operations and help investigators organize, prioritize and manage investigations while creating a permanent audit trail for regulatory review. For example, in Jumio Transaction Monitoring, all relevant information related to a case can be stored and easily updated as new information and evidence is uncovered.



How it Works

The detection rules in an AML system flag all the suspicious transactions that meet specific criteria. The system then groups those transactions into a case. Case management involves these three basic steps:

Case Analysis

The system provides the analyst with all the relevant information about the suspicious activity. The analyst can review this data and drill down to view related data and historical activity that might provide additional context. This enables the analyst to gain a comprehensive understanding of the suspicious activity.

Investigations

The analyst records their findings by adding notes, attaching supporting documents and recommending the next steps. A workflow is often utilized to ensure a consistent process is followed across the organization, which may include escalating to a manager for further review.

Regulatory Filing

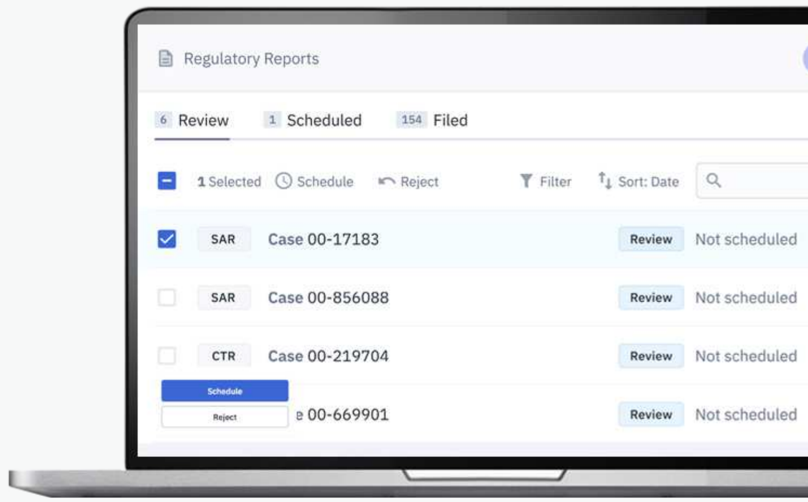
Most jurisdictions require certain suspicious activity to be reported to a regulatory agency. These reports must document all the details of the activity including what issues were identified and who was involved.

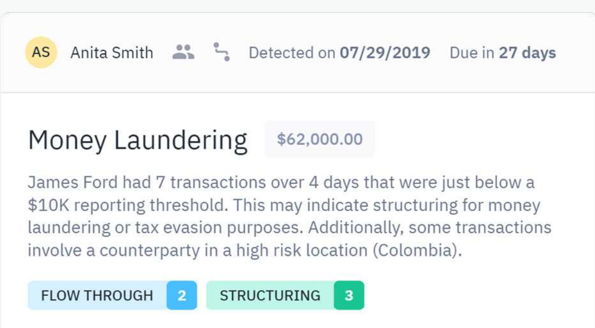
Key Ingredients of Case Management

An integrated case management solution enables compliance teams to efficiently conduct and document investigations. Advanced solutions offer highly configurable capabilities, provide flexible case management workflows, create defensible audit trails, streamline regulatory filings and, most importantly, reduce the risk of money laundering. They should also include the following:

Consolidated View

A case should show you a consolidated view of the relevant parties, accounts, transactions and more. This efficiency can help teams investigate cases more effectively with intelligent data aggregation and a collaborative, role-based workflow. Relationship diagrams and other visualizations can make it easier for the analyst to make sense of complex activity. The analyst should be able to easily review the history, add notes and send the case over to other team members for review.





Simple and Intuitive User Experience

If the workflow is too simplistic or hard to use, doesn't provide powerful case management or slows down your analysts' investigations, your team won't benefit from using it. Every extra click adds up to lost productivity, so choose a solution that has a streamlined, intuitive, modern interface that will enhance your compliance team's effectiveness and efficiency.

Automated SAR Filing

FinCEN has made some improvements to the SAR form in recent years, but it's still a challenge to fill out correctly and consistently, and the narrative is notoriously difficult to write. Modern case management systems pre-populate the forms and electronically file them with a regulator. The capability to file the SAR directly with FinCEN saves your team a lot of time and hassle while helping to ensure your reports adhere to FinCEN's strict requirements.

End-to-End Compliance

Up until now, fintechs, banks and credit unions, broker-dealers, lenders, cryptocurrency providers, marketplaces and other regulated organizations have had to cobble together several different point solutions — sometimes 10 to 20 of them — to combat financial crime and meet compliance mandates.

But in September 2020, Jumio acquired Beam Solutions' AML platform, creating **the first end-to-end identity verification and compliance solution.** Now, firms can use Jumio's KYX Platform to manage compliance throughout the entire customer journey, from onboarding to ongoing customer due diligence, transaction monitoring, case management and reporting.

Jumio's KYX Platform uniquely addresses these challenges:

Detect Suspicious Activity

This entails analyzing vast amounts of financial data and adaptively searching for subtle trends and abnormal activity that may suggest a pattern of money laundering.

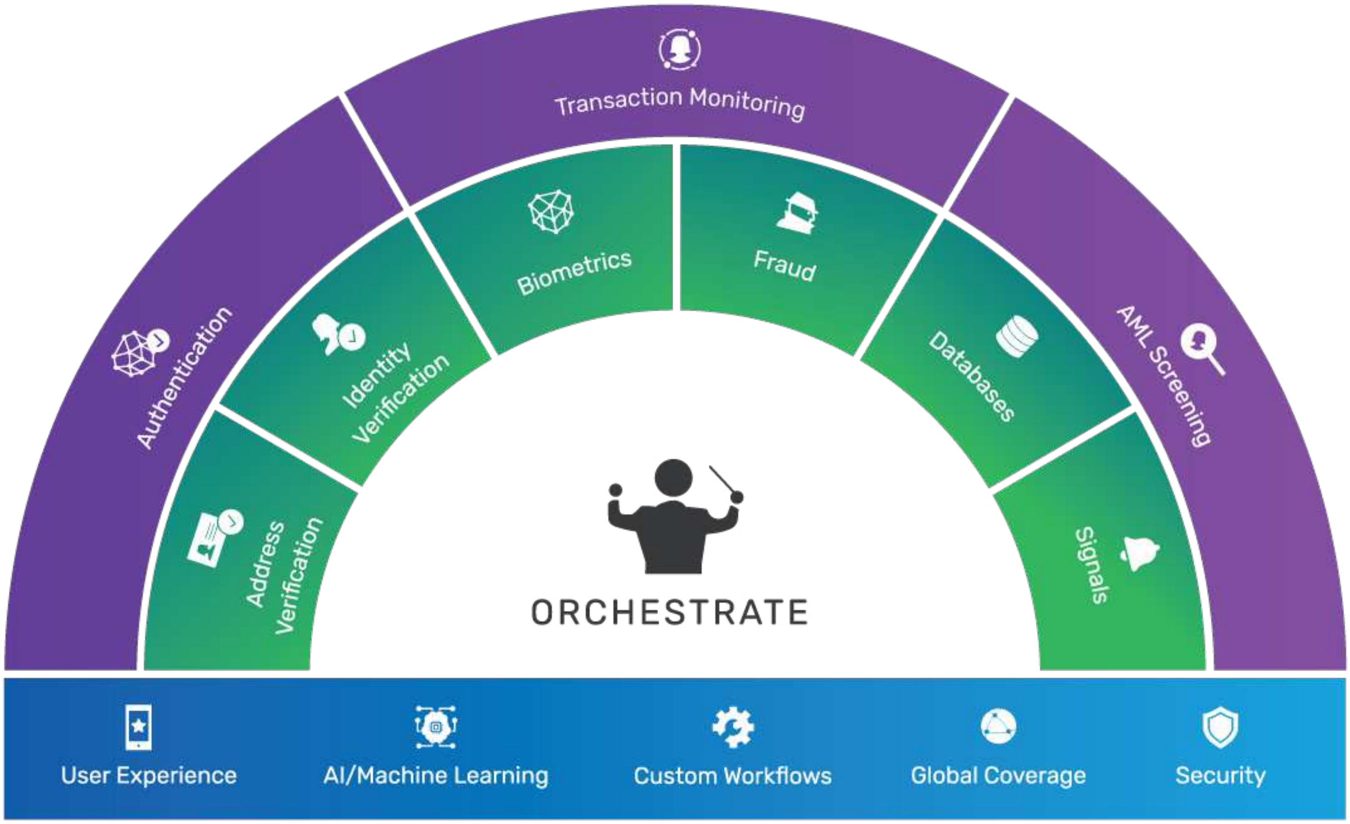
Simplified Case Management

A streamlined platform to investigate suspicious activity, document finding, complete a workflow and submit regulatory filings, all from a single interface.

A More Holistic Approach

Organizations need to have a more comprehensive and holistic view of the risk associated with each customer, which includes performing AML and KYC processes both upfront and on an ongoing basis.

The Solution: Jumio's KYX Platform



The KYK Engine

The engine behind Jumio KYX Platform includes a number of interwoven features, including an award-winning UX, state-of-the-art AI/ML, custom workflows, global coverage and bank-grade security.

Identity Proofing and Corroboration

Organizations often utilize a number of identity services to increase the level of identity assurance and answer the fundumental questions: is the user who they claim to be online and is it safe to start doing business with them?

AML Screening and Monitoring

Beam's detection engine analyzes vast amount of financial data and adaptively searches for suspicious activity and trends. It uses machine learning to significantly reduce false positives and yields higher catch rates.

As both financial crimes and regulations have evolved, the task of compliance has become a massive burden. With the advent of Jumio's KYX Platform and the dawn of end-to-end compliance, firms can now leverage the very best compliance solutions in a unified, secure platform.

About Jumio

When identity matters, trust Jumio. Jumio's mission is to make the internet a safer place by protecting the ecosystems of businesses through a unified, end-to-end identity verification and eKYC platform. The Jumio KYX Platform offers a range of identity proofing and AML services to accurately establish, maintain and reassert trust from account opening to ongoing transaction monitoring.

To avoid exorbitant AML fines, today's financial institutions and other regulated entities need a smart solution that enables their compliance teams to be responsive, adaptable and efficient. This is what Jumio now offers by integrating Beam's AML screening, transaction monitoring and case management solutions into its KYX Platform.

Leveraging advanced technology including AI, biometrics, machine learning, liveness detection and automation, Jumio helps organizations fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including KYC, AML and GDPR. Jumio has verified more than 250 million identities issued by over 200 countries and territories from real-time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, digital currency, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in North America, Latin America, Europe and Asia Pacific and has been the recipient of numerous awards for innovation. For more information, please visit www.jumio.com.

jumio.com