The ABCs of eKYC

A How-To Guide for Identity Verification to Know Your Customer (KYC) Online

jumio

"The idea is that knowing your customers — verifying identities, making sure they're real, confirming they're not on any prohibited lists, and assessing their risk factors — can keep money laundering, terrorism financing, and more run-of-the-mill fraud schemes at bay.

"The key is finding a balance so that these efforts are effective without penalizing innocent consumers — or being so onerous that upstarts can't comply with them (and hence can't compete)."

FIN.PLAID.COM

The "Know Your Customer" Imperative

If the last decade has taught us anything, it's that a person's online identity isn't always what it appears to be. Data breaches, phishing schemes, identity theft, money laundering and other digital scams have wreaked havoc on organizations from every sector of the economy — from financial institutions to dating sites to players in the sharing economy.

Corporate losses from fraudulent online transactions are expected to reach $25.6 billion this year (2020), according to Juniper Research. Meanwhile, new research from the Internet Association indicates, "Consumers are spending more (money) than ever online, and they want to use online services across categories from shopping to transportation."

Whether it's contracting for a project on a freelance site, transferring funds via a financial app, or renting a vacation home, consumers expect that the people and institutions on the other end of the transaction are who they say they are and will handle their financial and personal details safely and securely.

The "new normal" of our digital world has made verifying the digital identities of online users and customers a business imperative, driven by several important factors.

1. Fraud Risk

The abundance of identity information housed online makes it a fraudster's goldmine. Digital identities act as a currency on the web, with specific data (e.g., Social Security numbers, email addresses, passwords, credit card numbers, medical records) fetching anywhere from 25 cents to $60 per record. Bad actors will exploit any opportunity available to obtain access to this data. In the first six months of 2019 alone, 4,000 publicly disclosed data breaches and 4.1 billion records were exposed.

To mitigate fraud risks, not to mention to protect their brand reputation, organizations have a clear financial incentive to accurately verify their users' online identities.

2. Trust

Customers and online users trust businesses to protect their data. They count on you to take the necessary precautions to keep their identities and personal data secure from fraudulent transgressions.

But there's another side to trust. In many industries, your online consumers are interacting with one another. They're renting vacation housing from each other, they're sharing rides, they're setting up dates and other social gatherings. Trust is also the foundation for these exchanges and users expect that players on both sides have been vetted. In fact, a recent Jumio Global Trust and Safety Survey found that a combined 64.4 percent of U.K. and U.S. consumers feel it's important for online sharing services to verify the identity of new users.

3. Compliance

In recognition of the huge risks involved, oversight bodies across the globe have begun instituting compliance mandates to bring digital identity verification to the forefront of the minds of businesses.

Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance mandates and associated customer due diligence (CDD) requirements are probably the most well-known of these regulations when it comes to online transactions, especially opening accounts. Others include California's CCPA compliance rules and Europe's GDPR mandates, both of which are driving companies to establish a strong link between the digital and real-world identities of their online customers.

There are also related directives from the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), Counter-Terrorist Financing (CTF), the 6th EU Anti-Money Laundering Directive (6AMLD), MLR 2017, the Bank Secrecy Act/ Anti-Money Laundering (BSA/AML), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Customer Identification Program (CIP), not to mention guidelines about Politically Exposed Persons and recommendations from the Financial Action Task Force.

What are KYC and eKYC?

KYC

Know Your Customer, referred to as KYC, refers to the process institutions use to verify the identities of their customers and to perform due diligence in determining the risks these individuals present in terms of illegal activity and financial crime. Their aim is to confirm, to a high level of assurance, that customers are who they say they are and that they are not likely to be engaged in criminal activity. KYC is mandated for some organizations — primarily financial institutions. For others, while not mandated, it is an important component of their operations and a signal that the business is trustworthy and that they care about protecting their customers.

One thing is clear: in the digital world knowing your customer is almost always a good idea! So while banks are required to comply with KYC regulations to limit fraud, KYC procedures are fundamental to protecting all types of organizations from fraud and losses at the hands of money launderers, fraudulent individuals or organizations, and even terrorists.

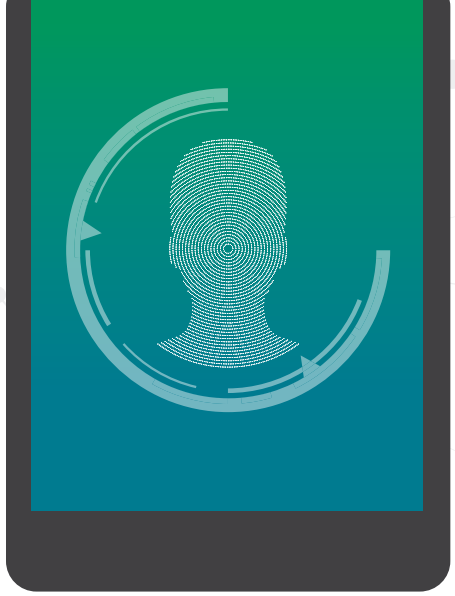
KYC procedures are usually employed when an account is created (either in person or online) or a customer starts doing business with an organization, as well as later, when the customer accesses that account. KYC includes three components:

- ✔ **Verifying the identity of the customer through a Customer Identification Program (CIP)**
- ? **Understanding the nature of the customers' transactions**
- 🔍 **Performing AML screening (due diligence)**

The first component — identity verification — entails having the customer (individual or business entity) provide relevant documentation (e.g., government-issued ID, articles of incorporation) to establish their identity and then subjecting that documentation to some type of formal verification process. When done in person, some pieces of that verification can be done manually, on the spot, such as comparing a person's face to their passport photo. Other times, accounts are created online, and therefore documentation must be validated through a third party or some other manner.

eKYC

eKYC refers to the process of performing identity verification and due diligence online/electronically. By bringing the KYC process online, businesses have an opportunity to improve the customer onboarding experience by reducing paper-based procedures and time spent on administration. They can also reduce the costs of and time spent on verification, making it more profitable for the organization.



Why Does KYC Compliance Matter?

Maintaining a Safe & Ethical Business Environment

By first verifying customers' identities and intentions and then understanding their transaction patterns, businesses are able to more accurately pinpoint suspicious activities. For example, money-laundering and terrorist financing often relies on anonymously opened accounts. The emphasis on KYC has led to increased reporting of these suspicious transactions among financial institutions. This doesn't necessarily mean there's more illegal activity happening in the world, just better detection of it.

Fines for Non-Compliance

Nearly $26 billion in fines were imposed against financial institutions for non-compliance with AML and KYC regulations in the last decade, according to research by Fenergo. Case in point? In 2018, Dutch bank ING was fined $900 million for failing to meet KYC and AML compliance. The investigation revealed that the bank failed to execute policies meant to prevent financial-economic crime. From 2010 to 2016, ING's Dutch branch did not meet due diligence standards when it neglected to report suspicious transactions in its system.

"It's no longer good enough for banks to simply accept the costs associated with inefficient processes — the consequences are now much more serious," said Steve Pannifer, author of The Cost of Compliance and How to Reduce It and chief operating officer at Consult Hyperion. "The biggest change in the past two years has been new EU rules around KYC related compliance. This has led to many more punitive fines for banks who fail to comply — and the size of the fines has grown in tandem. "The Financial Conduct recently issued fines to several major banks, amounting to £176 million. Then, even that fine was dwarfed by the €775 million fine handed to a single bank by Dutch authorities."

Loss of Reputation or Personal Liability

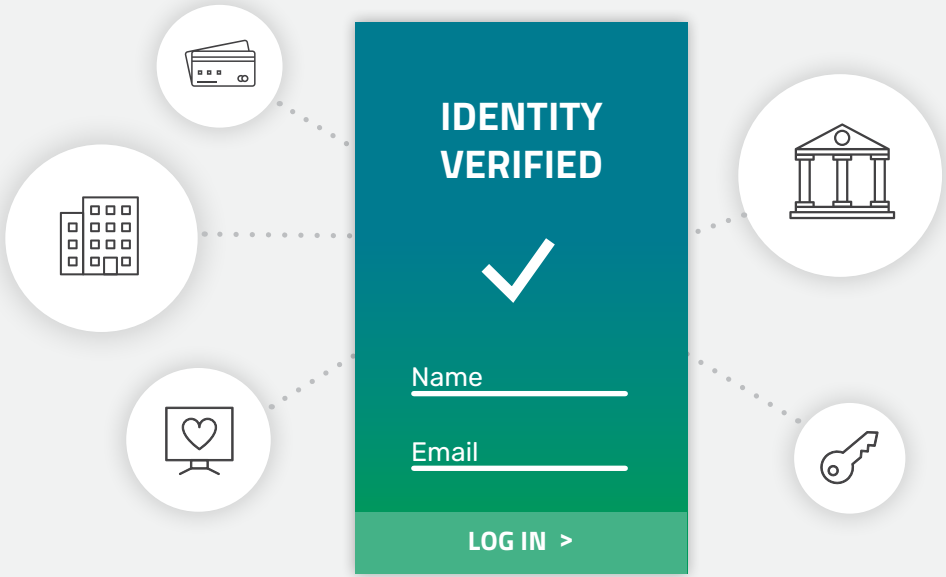
It's not all about the financial and business costs. Another strong incentive for compliance is that bank officials can be liable, not just civilly, but criminally. The risk of reputational loss, loss of operating licenses, and even personal liability of senior management are significant motivators for organizations to get KYC right.

Who Must Comply?

The U.S. Treasury has had legislation in place for decades directing financial institutions to assist the government in detecting and preventing money laundering. The Bank Secrecy Act of 1970, for example, specifically requires financial institutions to keep certain records (e.g., cash transactions exceeding $10,000) and to report financial transactions that might signify money laundering, tax evasion or other criminal activities. In an evolution of these regulations, KYC processes were introduced in 2001 as part of the Patriot Act, which was passed after 9/11 to provide a variety of means to deter terrorist behavior.

When KYC procedures were first introduced, regulators did not create specific standards for verifying customers. This was by design as regulators suspected that banks would only choose to meet minimum requirements if specific KYC and AML rules were put into place. Instead, the regulators wanted banks and other financial institutions to create their own systems for achieving compliance. Unfortunately, this lack of clear standards led to a convoluted system that has made compliance challenging.

So, while legislation has historically targeted financial institutions, there is good reason for many types of businesses — even those not subject to KYC — to follow KYC procedures. In fact, it is increasingly common for social platforms (e.g., dating sites, drivers, rental agents), credit card companies, insurance agencies and many other enterprise companies to require that their customers verify their identities in order to help ensure that they are not involved in fraudulent activities maintain trust within their ecosystems.



Focus on KYC in Banking

The Hudson United Bank of New Jersey was one of the banks used by the airplane hijackers who perpetrated the deadliest attack ever on American soil on Sept. 11, 2001. According to the 9/11 Commission, money-laundering safeguards at the time were not designed to detect or disrupt the type of deposits, withdrawals and wire transfers that helped facilitate the attacks. The resulting KYC legislation was passed as a means of deterring terrorist activity and financial crimes.

More recently in 2016, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a set of rulings to further clarify and strengthen customer due diligence (CDD) requirements and meet KYC in the financial sector. They outlined four minimum elements needed to effectively ensure banking customers are who they say they are. They include:

1. Identifying and verifying the identity of customers
2. Identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities)
3. Understanding the nature and purpose of customer relationships to develop a customer risk profile
4. Conducting ongoing monitoring for suspicious transactions and, on a risk basis, maintaining and updating customer information

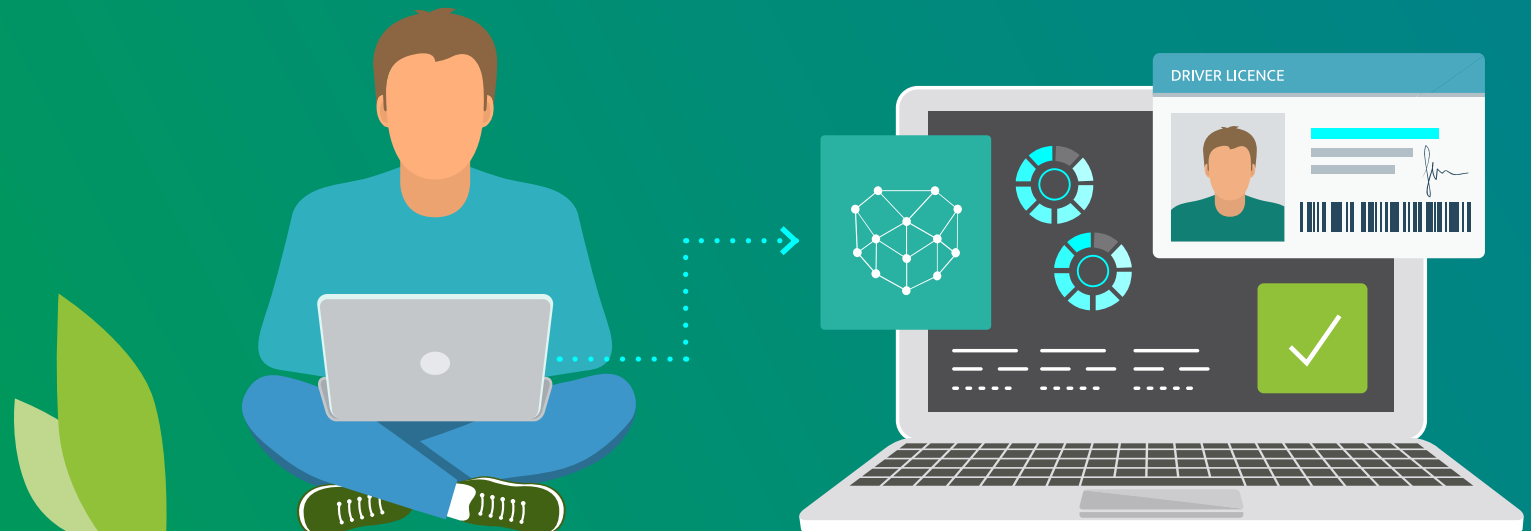
Customer Requirements

To meet these KYC requirements, financial entities must gather and verify identity information at the point of onboarding new customers. The requirements vary depending on whether the account is for an individual customer or a business customer.

Individual customers who visit a bank in person will bring some proof of identity, such as government-issued identification (e.g., driver's license, passport), proof of address and whatever else might be required for the transaction. The banker checks the customer's documentation to physically ascertain that they are who they claim to be. For business accounts, additional information verifying the identities of beneficial owners (e.g., articles of incorporation) and business activity (e.g., profit and loss statements) are required.

These processes are far more complex when customers create accounts online. Now, financial institutions must verify that the customers' digital identities match their actual, real-world identities. Establishing a trustworthy link between a digital identity and an actual person requires a robust identity verification process to prove the person is who they represent themselves to be. That process may include a combination of biometrics (e.g., facial recognition, fingerprints), machine learning and/or document or ID verification.

Outdated security models that ask users to provide passwords or answer security questions are no longer considered an effective paradigm for assuring that the digital identity of an online customer matches their real-world identity. Increasingly, organizations are looking to biometrics as a critical component to identity verification.



The Challenges of KYC Compliance

Cost

The costs of KYC compliance are astonishingly high. To satisfy KYC compliance and related mandates, banks spent more than $100 billion in 2016 and predicted those costs would rise from four percent to 10 percent by 2021.

Individuals financial institutions spend an average $60 million every year to meet regulatory requirements under KYC and customer due diligence — with some banks spending as much as $500 million, according to a global survey by Thomson Reuters.

Customer Experience

KYC adds friction to the onboarding process for businesses as customers go through the necessary identity verification steps. A Thomson Reuters study found that it takes financial institutions an average of four touchpoints and 26 days to onboard a new client, up from 24 days in its 2016 survey. Corporate customers, however, are contacted roughly eight times and must wait an average of 32 days.

These long wait times are expensive for banks and frustrating for clients, who expect quick and easy interactions. Research by Signicat found that more than 50 percent of retail banking customers in Europe abandoned their attempt to sign up for new financial services. The leading causes for this high level of abandonment were attributable to the process simply taking too long and being too cumbersome and onerous.

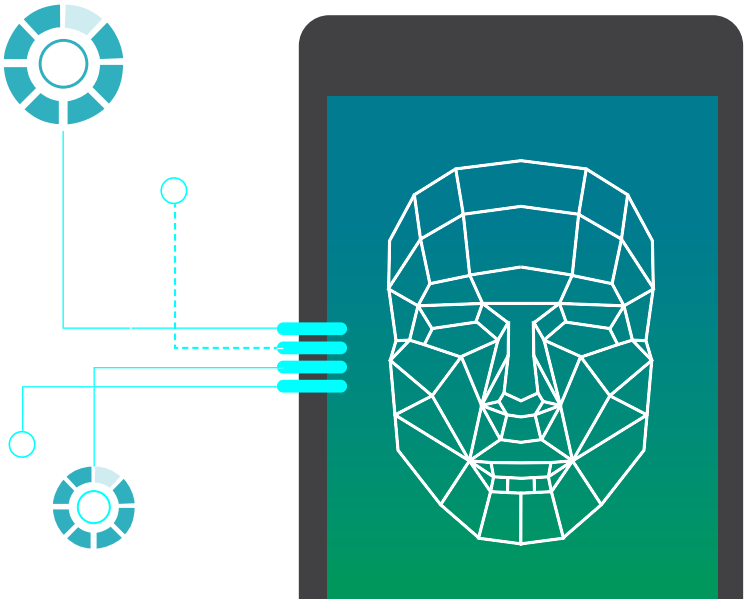
So the challenge that every business faces is how to balance KYC with the need for fast, efficient onboarding processes.

Complexity

Despite the fact that financial institutions had an average of 307 employees working on KYC adherence in 2017 (up from 68 in 2016), 34 percent of them report that a lack of resources remains the biggest challenge in conducting KYC and customer due diligence processes, according to Thomson Reuters.

And, because there is no standardization for complying with KYC, processes vary from institution to institution. To verify individuals' identities, some companies require Social Security numbers, national ID cards or driver's licenses, while others ask for passports or birth certificates. For business customers, the documentation and verification process are even more problematic.

These complexities are only amplified when onboarding happens online. Now, the challenge of verifying a digital identity enters into the equation.



Technologies

With so many — often disparate — systems available for identity verification and customer onboarding, organizations struggle to identify the specific suite of technologies and procedures they need to meet due diligence. There is already tremendous risk involved in modern commerce and electronic banking, which is why cybersecurity and IT infrastructure services are such big business today. The identity verification requirements of KYC introduce yet another technological risk element into the mix.

Biometric Authentication

In its 2019 Market Guide for Identity Proofing and Corroboration, Gartner recommends that organizations move away from traditional identity proofing and authentication technologies that rely solely on something a customer knows (e.g., a password or security question) or possesses (e.g., an ID badge).

Instead, they recommend organizations turn to biometrics for KYC identity verification. Biometric authentication technologies rely on what someone is, for example, by using their unique fingerprint or facial map to verify a customer's identity.

Banks are using biometrics, alongside more traditional ID verification, to strengthen their defenses against online fraud and maintain compliance with AML and KYC. These technologies not only build trust among customers, but they also create a seamless, efficient onboarding experience.

3 Keys to Successful KYC Compliance

With this historical (and complex) foundation of KYC as a backdrop, let's turn to the three core areas that businesses need to focus on to successfully implement KYC processes.

1. Verify the Identity of Your Customer

One of the requirements of KYC for financial institutions is that they establish a Customer Identification Program (CIP) in connection with the opening of an account to "form a reasonable belief that (they) know the true identity of each customer" (i.e., verify the identity of individuals wishing to conduct business them). The CIP requires U.S. financial institutions to develop a CIP "appropriate for its size and type of business" and designed to limit money laundering, terrorism funding, corruption and other illegal activities.

But the CIP requirement isn't just for the U.S. — more than 190 jurisdictions around the world have committed to recommendations from the Financial Action Task Force (FATF), a pan-government organization designed to fight money laundering. Every CIP must have a risk-adjusted procedure to verify the identity of a potential customer who wants to open an account. The minimum requirements to open an individual financial account are clearly spelled out in the CIP: name, date of birth, address and identification number.

The relevant risks may include the types of accounts in question, typical transaction size, the quality of the information offered by the customer, the characteristics of the organization as a customer, and the location(s) where the customer's transactions originate or end. To demonstrate compliance, financial institutions need to be able to record and retrieve customer information and account activity, including relevant transactions.

In addition to gathering this information during the opening of the account opening, the institution must verify the identity of the account holder "within a reasonable time." Procedures for identity verification include reviewing ID documents, non-documentary methods (e.g., comparing information provided by the customer with consumer reporting agencies, public databases), or a combination of both.

Because online identity verification is at the core of any CIP, the chosen service providers must not only be able to perform at the highest standards and enforce the strictest compliance and data privacy requirements (which are always evolving), but also successfully integrate with the company's back-end and front-end systems.

There are several technologies that can be brought to bear to perform eKYC, AML screening and online identity verification. For institutions that rely on a government-issued ID document and biometric verification, the online identity verification process generally consists of a few key components:

Optical Character Recognition (OCR) to extract data from the ID document

ID verification to ensure the ID is valid and unaltered

Selfie capture and comparison to ID document to increase identity assurance

Some institutions attempt to create their own homegrown KYC processes, particularly in the Asia-Pacific (APAC) region. There are significant risks to this approach, however, which is why we've created eKYC in APAC: How to Get It Right.

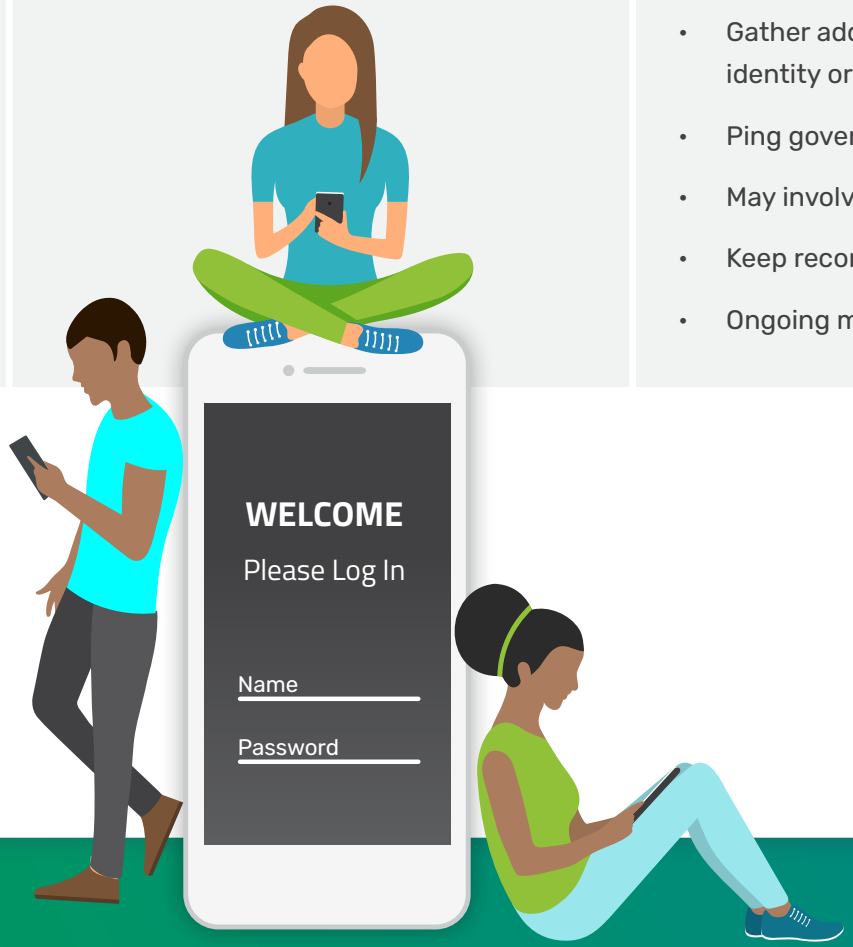
2. Perform Due Diligence

The cornerstone of a strong Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program includes comprehensive customer due diligence (CDD) policies and processes for all customers, combined with the adoption and implementation of internal controls. Financial institutions need to know their customers and the risks they represent, as well as protect themselves against criminals, terrorists, and politically exposed persons (PEPs) who might present a risk.

There are three levels of customer due diligence:

LEVEL	DEFINITION	CONSIDERATIONS
Simplified Due Diligence	Lowest level of due diligence where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing	• No requirement to verify your customer's identity • Appropriate for low value accounts • Business relationship should be continually monitored for trigger events which might create a requirement for further due diligence in future
Standard Due Diligence	These are generally situations where there is a potential risk, but it is unlikely that these risks will be realized	• Majority of cases • Requires identity verification • Must gather information to enable you to understand the nature of the business relationship • Keep records of diligence activities • Ongoing monitoring of potential trigger events that may result in further due diligence being required

LEVEL	DEFINITION	CONSIDERATIONS
Enhanced Due Diligence	Required where the customer and product/service combination is considered to be a greater risk for money laundering or terrorist financing	• Politically exposed persons (PEPs) • Based on a combination of risk factors, including the location and occupation of the person, the type of transactions and expected pattern of activity and dollar amounts in terms of transaction types • Gather additional information to verify the customer's identity or source of income • Ping government-issued sanctions or watchlists • May involve an adverse media check • Keep records of all diligence activities • Ongoing monitoring



The Right Level of Diligence

Because entities can vary in terms of typical types of transactions, customers, locations, scale and business lines, the KYC efforts can vary as well. In general, CDD will include verifying the identity of customers and understanding the monetary thresholds for required reporting and record retention, as well as the specific FinCEN rules governing specific types of transactions.

In determining what level of due diligence is appropriate (Simplified vs. Standard vs. Enhanced Due Diligence), a company should look for red flags relating to:

- Location of the business
- Occupation or nature of business
- Purpose of the business transactions
- Expected pattern of activity in terms of transaction types, dollar volume and frequency
- Expected origination of payments and method of payment
- Articles of incorporation, partnership agreements and business certificates
- Understanding of the customer's customers
- Identification of beneficial owners of an account or customer
- Details of other personal and business relationships the customer maintains
- Approximate salary or annual sales
- AML policies and procedures in place
- Third-party documentation
- Local market reputation through review of media sources

When to Undertake Customer Due Diligence

To help prevent money laundering and terrorist financing, it's becoming standard practice to complete due diligence prior to entering into a business relationship with a customer. This usually involves ascertaining the identity and location of the potential customer and developing a good understanding of their business activities. This can be as straightforward as requiring user documentation (e.g., capturing ID documents paired with utility or bank statements) that verifies the name and address of your customer.

Before storing this information or any additional digital documentation, organizations should classify the customer's risk category and define what type of customer they are when authenticating or verifying them. Once a customer has been identified and verified, there is no requirement to re-verify their identity unless a trigger event occurs. Potential trigger events can include:

- The product or service that you supply to the customer changes
- Concerns are raised regarding previous information collected and its validity
- Suspicions of money laundering are raised

Approaches to due diligence should be fluid and ongoing monitoring should be carried out to allow you to detect trigger events that may impact your risk and the level of due diligence that is required. Ongoing monitoring should include the nature of the business relationship as well as financial sanctions and PEP screening.

3. Conduct Ongoing Monitoring

Being able to identify customers who pose an increased risk as circumstances change reduces compliance blind spots and the need for bulk remediation projects further down the line. Ongoing monitoring is a process in which organizations implement a periodic review of all information regarding each of their clients. A "business relationship" is defined as having a client that holds an account with you or any person or entity that has conducted two transactions or activities, within five years, where you were required to verify the identity of the individual or confirm the existence of the entity.

The ongoing monitoring function includes oversight of financial transactions and accounts based on thresholds developed as part of a customer's risk profile. With the onset of FinCEN's CDD rule and MLR 2017, the emphasis is on organizations to develop clear, auditable processes to manage ongoing checks. What was once best practice has moved to law, reflecting an increasing expectation from both global regulators and stakeholders that firms should be more aware of customer risk at all times.

Comprehensive monitoring is only possible if you have a true picture of your customer and that means understanding the ultimate beneficial owners (UBOs). Having a reliable process in place allows firms to do better business and protect their reputations.

The primary objectives of ongoing monitoring are to:

- Detect suspicious transactions (e.g., spikes in activities)
- Keep client identification, beneficial ownership information and the purpose and intended nature of the business relationship record up to date
- Determine if your customers are included on PEP,

  sanctions or adverse media lists after the new account onboarding (i.e., when the initial vetting occurred)
- Unusual cross-border activities

In the United States, financial institutions must file a Suspicious Activity Report (SAR) if they think that an employee or customer has engaged in insider trading activity, there is evidence of computer hacking or a consumer is operating an unlicensed money services business. They must also file a SAR if they detect potential money laundering or violations of the Bank Secrecy Act.

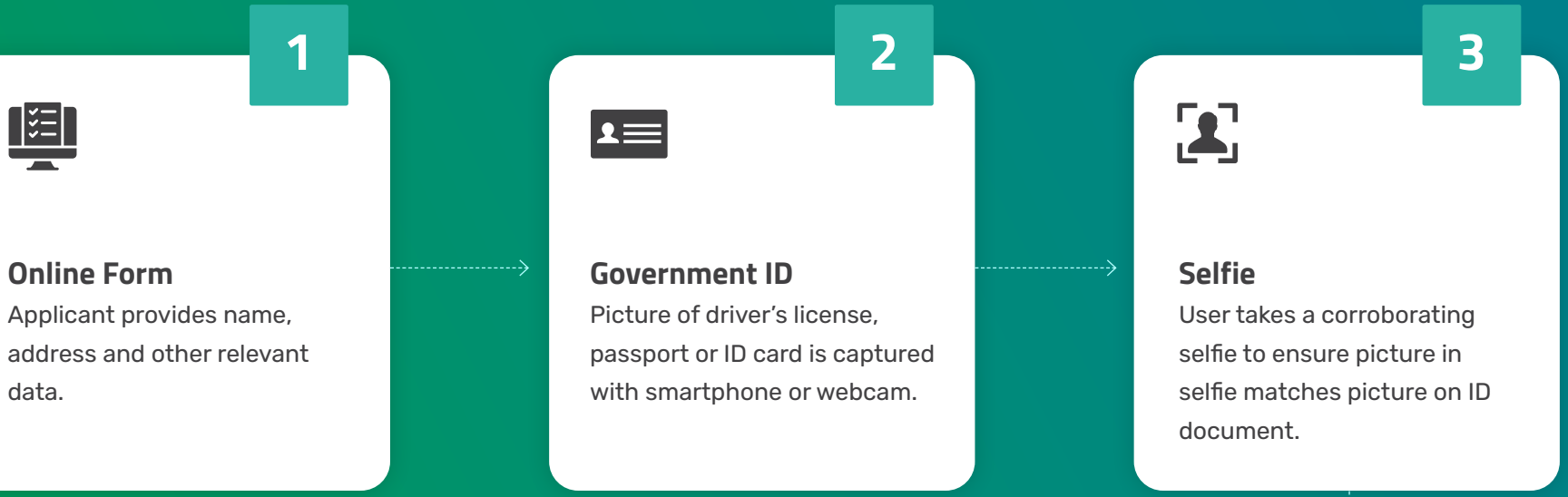
SARs can cover almost any activity that is out of the ordinary, especially if the activity gives rise to a suspicion that the account holder is attempting to hide something or make an illegal transaction.

What to Look for in an eKYC Identity Verification Solution

There are countless considerations and elements to complying with eKYC and figuring out how to orchestrate all the steps, from initial identity verification to due diligence to ongoing monitoring. It's confusing, to say the least.

The graphic below walks through nine steps an organization may go through as part of their eKYC process. While each institution needs to decide how to enforce KYC based on its unique business needs and the risk profiles of its users, this sample flowchart details the kinds of checks that can be performed to answer and address the fundamental compliance requirements:

- Is the applicant the person or business they claim to be online?
- Does the risk profile of the applicant raise any red flags?
- How can I ensure that customers are monitored on an ongoing basis?



4

Database Check

Organization pings a variety of third-party databases to ensure that the individual exists (usually based on name and date of birth checks).

5

Fraud Signals

Organization may check a variety of fraud signals, including the IP address of the phone, email address verification and even the speed at which the online forms are completed by users.

6

AML Screening

User is screened against regional government-issued watchlists and politically exposed person lists as part of anti-money laundering compliance mandates.

7

Proof of Address

Since the address is often not included on the ID document, the organization may need to capture proof of address (e.g., copy of bank statement or utility bill).

8

Risk Pools

Based on these checks, screening and fraud signals, users are assigned to risk pools and those flagged as high risk may be reviewed manually to make a final determination.

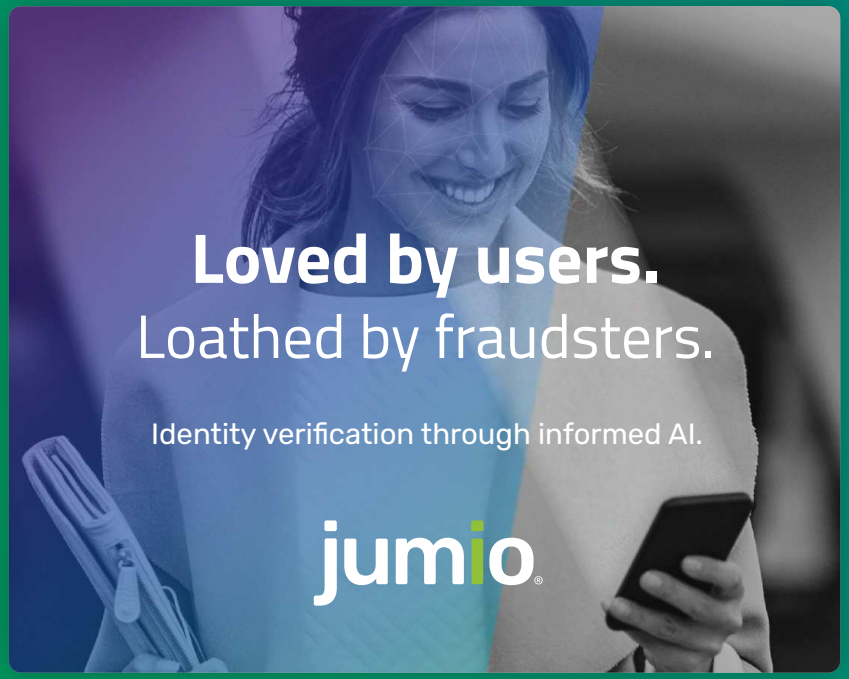
9

Ongoing Monitoring

After the customer has been onboarded, customers are monitored on an ongoing basis. This includes transaction monitoring, AML monitoring and behavioral monitoring (anomaly detection).

In addition to securely meeting the technical objectives above, the ideal eKYC solution must meet several other crucial requirements. The first is obviously effectiveness. Does the system work seamlessly, create a positive customer onboarding experience and is it cost-effective? For example, a typical European bank serving 10 million customers could save up to €10 million annually and avoid growing fines by implementing technology to improve KYC processes, according to recent research from Consult Hyperion.

The second is convenience for global scaling. A solution that is only viable in limited jurisdictions is of little use for a company with an international presence or global ambitions. No company would want to use a solution that requires multiple contracts, setups and integration for each market.



Getting a Handle on eKYC

Companies are striving to grow their customer base through faster, easier and lower-cost digital channels, yet the current regulatory and cybersecurity landscape creates a layer of complexity. Consumers want the convenience of signing up through digital channels and don't want to have transactions blocked or be constantly providing additional information. Paradoxically, institutions that comply with stringent Anti-Money Laundering and Know Your Customer regulations typically have to send new customers out of their preferred (digital) channel for identity verification.

These opposing realities have created a clear need for eKYC processes to verify customer identities. eKYC enables banks, ecommerce sites, insurance companies, home exchange platforms, credit card providers and businesses in the sharing economy to assess the risks or illegal intentions of each user, whether they're opening or attempting to log into an account, applying for a loan or making a payment.

The right eKYC strategy can transform an organization's manual KYC, AML and customer onboarding processes into a streamlined online approach. Jumio has such a solution, and hundreds of international companies already use our end-to-end identity verification and authentication solutions.

If you'd like to discuss your eKYC compliance challenges, please reach out to us at www.jumio.com.