Deep Science Publishing
https://doi.org/10.70593/978-93-49910-19-5_4

# Chapter 4: Advanced techniques in Anti-Money Laundering (AML), Know Your Customer (KYC), and real-time identity resolution

## 4.1. Introduction to AML and KYC

Money laundering has been around for as long as money. The earliest accounts date back to ancient Greece and Rome. However, money laundering as we know it today began to evolve to mask the criminal enterprise it often conceals only hundreds of years ago. In 1931, an individual became involved in the creation of casinos in Havana, Cuba, to launder operations for the then-legal income from illegal gambling in the United States. It was almost fifty years before the popularity of casino gambling in Nevada, the casinos' visibility in Las Vegas, and the newfound capability to monitor the funds flowing in and out of the casinos began to attract the attention of regulatory authorities. In 1985, the U.S. Treasury Department adopted regulations requiring casinos to file Currency Transaction Reports on cash wagers of more than $10,000. By the late 1980s, casino corporations were being cited for millions of dollars of currency transaction violations. Shortly thereafter, Congress enacted anti-money laundering legislation (Colladon & Remondi, 2017; Lin et al., 2020; Campedelli & D'Ignazio, 2021).

Developments in the casino industry set the stage for a more involved U.S. regulatory framework that expanded into industries beyond gaming because it was felt that just going after the proceeds of crime would not be enough to stem the flow of money into Florida properties and businesses. In 1991, Congress passed the Bank Secrecy Act, which required financial institutions to create effective anti-money laundering programs — including the filing of currency transaction reports for cash transactions over $10,000, as well as reports of suspicious activity inside or outside the bank, whenever a bank employee sees or knows something that doesn’t look right. The Act was expanded into a second stage in 1996 (Weber & Studer, 2016; Zhdanova & Moulin, 2020).

### 4.1.1. Overview of Anti-Money Laundering (AML) and Know Your Customer (KYC) Principles

Preventing money laundering is the most crucial aspect of a safe and secure financial industry. Money laundering by criminals and the infringement of the laws and regulations of traditional financial markets informally jeopardize the security of all nations. All countries must take preventative and curtailing measures to those activities by establishing legal and legislative frameworks to ensure strict privacy and security of customer data. The primary goal is to provide relevant banks with tools and knowledge to help identify abnormal activity in financial transactions and to permit forensic specialists the opportunity to assist during court proceedings. With the implementation

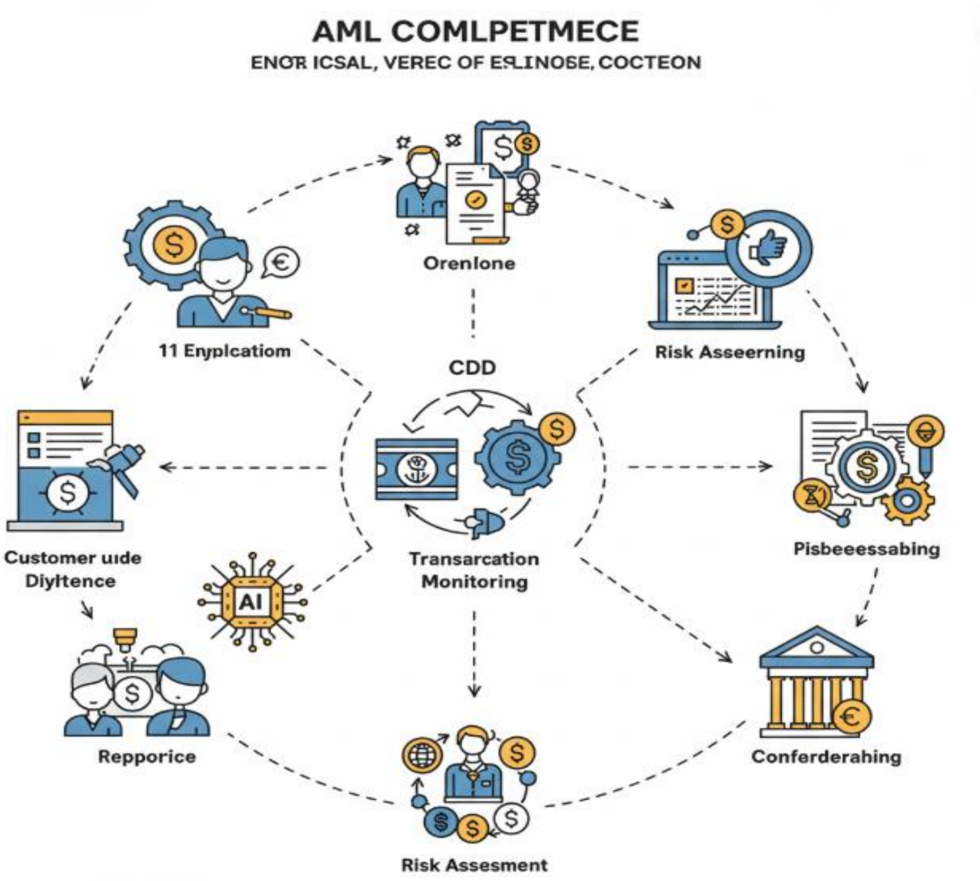

**Fig 4 . 1 :** Ecosystem of AML Implementation of an effective KYC program, financial institutions play a vital role in the fight against money laundering, enhancing the detection and reporting of potentially suspicious money laundering activities and transactions. This paper delves into essential developments and enhancements of the KYC process that can help financial institutes detect both present and future money laundering schemes. It covers traditional techniques used to validate the submitted KYC documentation and strives to enhance them through a data-driven method by using machine learning techniques. It illustrates the importance of considering Natural Language Processing when building machine learning models and the need to work with legal enforcement agencies to better understand how to build a better and more extensive database with accurate information to train machine learning models. The goal is to exempt innocent individuals from investigations or accusations of laundering money and subsequently crashing their lives and businesses. The result would be a more mature AML environment with less leakage where the priority will be risk rather than costs.

### 4.2. Regulatory Framework

Anti-Money Laundering (AML) legislation in response to recent scandals involving the International Banking System is at an all-time high and growing. The actions of the financiers and investors are now subject to scrutiny and regulation. The US, Germany, and Great Britain have historically put many laws in place as a check and balance against the actions of investors, banks, accountancy, and consulting companies and have made sure to regulate the AML area including accountant oversight and regulation. International organizations have made it a priority to write international guidelines that countries must implement into their laws, for fear of being blacklisted.

The average person does not realize that the payment system they use is seriously scrutinized each day. Money must be traced until the ending consumer product is located, and then the product must be investigated to see if any illegal action supported the initial purchase. The cost of compliance and strengthening of the back-end infrastructure of banks is exorbitant. Countries and companies have their requirements in the KYC process for which customer types must go through extra scrutiny before transacting with financial institutions. So much data capture is a huge burden and impossible to maintain without sophisticated detection algorithms, filtering technologies, and categorization methodologies. Detection is still an inordinate burden on companies and financial institutions but dictates that the source of origin for all products can be scrutinized.

There is not error-free modeling and the generation of detection scenarios is governed by risk thresholds that assume a good apprehension of the firm’s activity or the type of fraud being investigated. The said level and complexity of detection algorithm modeling selection, optimization, and tuning for supervised methods is a process that needs to be automated for mass-market deployment.

### 4.2.1. International Standards

Introduction to International Standards

There are certain measures that must be taken on an international level, which draw out rules and the details to be followed by governments for proper handling of money laundering practices. Through different conventions and agreements, the countries of the world agreed on these measures.

Financial Action Task Force

The most important organization working to prevent money laundering practices and legislation is the Financial Action Task Force. The FATF was created as a working group to put tension on tax havens, with a specific set of rules to encourage the lack of secrecy in jurisdictions that form part of the international financial system. Over the years and given the globalization of financial services and the increasing reality of an international dimension to crime and tax evasion, the FATF structure evolved into a body capable of creating, with a certain authority and degree of credibility, a set of rules and regulations that could not be ignored by the vast majority of countries.

The FATF is in charge of creating recommendations that serve as a guide for AML programs by guiding a country's internal processes to prevent criminals from entering, being in, or using the financial system in any money laundering, tax evasion, or terrorist financing crime. Since the establishment of the first recommendations in 1990, there have been two rounds of revisions and in 2003, the FATF published its current set of 40 recommendations, amended in 2004 and 2006. Governments are the main ones to be watched by the FATF to see if they are in line with the recommendations and they are the ones that are the object of mutual evaluations between the countries whether they are members of the FATF or of organizations of countries that are not in the FATF but are closely linked to it.

### 4.2.2. Local Regulations

One of the AML/KYC challenges associated with establishing a presence in foreign jurisdictions is the fact that many countries – especially those with an emerging or developing economy – can be reluctant to adopt the stringent regulation supported by various institutions. This has been particularly true in the Middle East and North Africa, but also in jurisdictions such as Japan and China. As a result, they can have much weaker

AML/KYC activities than those carried out in other regions. But the reverse is also true. In the last few years, Japanese regulators have also adopted a very strict and proactive stance concerning AML regulations applicable to crypto companies.

At one extreme, there are jurisdictions – such as the Cayman Islands, Dubai, Hong Kong, Singapore, also Switzerland – that have put a lot of effort into developing local regulations that will allow local financial institutions to attract new foreign direct investments, including investments in blockchain and crypto services. They have enacted flexible rules that are easily adoptable by such companies – building on market-leading solutions created by the main software providers operating in those areas. But also the reverse is true: Non-compliance with AML controls can quickly lead to a company being kicked out of the jurisdiction. This is something that crypto companies working with tokens considered securities must take into account. Exchanges will not work with companies in jurisdictions where no AML regulations or weak AML regulations are applied.

### 4.3. Understanding Money Laundering

The act of creating economic value in a criminal or socially unacceptable way is in itself how we describe an illicit activity. To be able to move the financial proceeds from such activity and make it appear to have come from a legitimate source or business, additional dirty work has to be performed. Money laundering is the process where an individual or group takes the illicit proceeds and cleans them to be able to move them anywhere in the economy where they appear to have come from a legitimate business so that long-term loans, lines of credit, and investments can be made. Concealing and disguising how an illicit activity created the money is the method used. Money laundering is like any other business in that the amount of profit must exceed the costs of money laundering for the money laundering to occur and continue. The difference is that while legitimate businesses already sell products and services that are in demand for which customers are willing to pay, these illicit businesses must lower the costs of their products and services. The most common illegal activities that create a need to launder money include illegal drugs, gambling, prostitution, racketeering, fraud, and even murder. While money laundering has been in use by criminals for a long time, it became noted and specific criminal charges were made for money laundering only in the past century. As more criminals began to expand their illicit activities which included using money from illegal activities to establish legitimate-looking businesses, the business of money laundering expanded. Criminal organizations began to develop money laundering businesses. Criminals began to use banks, with few questions being asked about the source of funds, and offshore tax havens to shield their activities from law enforcement. Today, the motivation to use money laundering has increased exponentially due to the mass data transfers that have made it more difficult to avoid detection and who have no way to verify the source of these transactions except through the use of transaction validation.

### 4.3.1. Stages of Money Laundering

Money laundering is often described in three stages: placement, layering, and integration – a simple, logical pattern. Placement describes the introduction of the proceeds of crime into the financial system, usually in the form of cash affecting the financial institution’s liquidity and risking detection when business is scarce but cash is plentiful. Layering describes the process of concealing the origins of the proceeds of crime after the proceeds have been placed into the financial system. It is called layering because the roots of the proceeds are "layered" further from the perpetrator, sometimes passing through several layers of financial institutions and techniques. Integration describes the stage at which the asset can be freely used without fear of detection, often because the asset has been commingled with legitimate assets.

Placement methods often exploit bank facilities, as these are vulnerable to the receipt of large quantities of deposits but are not linked in the same way to flows of cash for business activity. Hence, bank notes from drug trafficking or other criminality may be deposited into large amounts of business accounts to appear like legitimate company revenues. Financial institutions with no branch network to report unusual cash activity tend to be targeted for this purpose. That is why cash-intensive businesses, especially those with branches, are also targeted by criminals for money laundering. Criminals use the cash business to "clean" their drug trafficking money. These businesses normally include restaurants, travel agencies, retailing, and money transfer services.

### 4.3.2. Common Techniques Used

Now that we've had a brief introduction to money laundering terminology and its processes, let us dig deeper into the techniques employed by financial criminals in the concealment of money laundering activities. Money laundering is the act of disguising illegal money to make it seem legit. Criminals cover their money with phony businesses, fake tax returns, and other techniques or tools disguised as legitimate transactions. Money laundering techniques are not limited to any one criminal organization or group. Any group or organization that earns cash from criminal activity is likely practicing money laundering via several techniques. Laundering schemes vary, depending on the nature of the perpetrator's illicit activities.

Many techniques are used in laundry activities across the globe. These span cash-intensive businesses, bogus firms, and trade-based money laundering. Most money laundering methods come down to covering cash activities within financial institutions, such as banks, casinos, or credit unions, or transferring illicit cash to other countries. Virtually any business that takes in cash payments is susceptible to "smurfing" – the term used for engaging in large transactions, then depositing the smaller cash amounts into banks or ATMs, one at a time, and at various institutions across a wide area over several days. Bank branch tellers and ATM systems are programmed to block deposits that exceed a designated amount, resulting in smaller lures being utilized by money launderers. It's the use of such tiny amounts on many occasions that gives criminals the appearance of a legitimate business person.

## 4.4. KYC Processes

The primary purpose of KYC Processes is to prevent, detect, and mitigate money laundering activities through the identification of customers who open accounts or engage in financial transactions. The term KYC refers to customer identification and the due diligence that organizations must undertake to know their customers and assess money-laundering risks, including the risk of doing business with PEPs. KYC is a component of AML core processes, which also include transaction monitoring and suspicious activity reporting. Transaction monitoring analyzes financial transaction patterns to detect possible money laundering activity. Suspicious activity reporting entails reporting suspicious transaction activity to the appropriate government agencies. KYC is important because a transaction in furtherance of a money laundering plot cannot be reported unless the organization knows enough about the customer and the source of the customer's funds to recognize the transaction as suspicious. Without KYC valuable information is missing from the transaction monitoring and reporting functions, and these functions are significantly impaired. Customer Identification Procedures require organizations to obtain identifying information from customers before, or upon account opening and must be employed for customers that open bank accounts. CIPs generally specify what identifying information must be obtained, such as name, address, and date of birth for individuals, or tax identification number for businesses, and, in the case of personal customers, as well as verifying the identity of customers through the use of documentary and non-documentary means, and obtaining information concerning the source of the customer's funds, the purpose of the account, and the anticipated account activity. Other identifying information must be obtained within a reasonable period after opening the account. It is important to note that not all identifying information must be obtained before an account is opened; for example, an organization does not need to obtain information from a customer until the fifth day after account opening.

### 4.4.1. Customer Identification Procedures

Customer Identification Procedures (CIPs) are the initial step in the KYC process. Under the Bank Secrecy Act and its implementing regulations, banks and financial institutions are required to implement a written anti-money laundering (AML) program that provides a framework for the techniques, tools, resources, and unit responsibilities needed to prevent such abuses. The CIP is the first step in meeting this obligation. It establishes what customers will need to present before the opening of an account, what actions a bank must undertake to verify the customer's identity, and the timing of these actions.

In addition to guiding proactive measures designed to help mitigate the risk of the institution being used as a conduit for illicit activity, legislation introduced in 2001, and the subsequent creation of the Financial Crime Enforcement Network established CIPs as an active countermeasure against money laundering. This is achieved through proactive identification of customers and verification of personal information at account inception, as failure to do so could have disastrous consequences both for the institution's overall health and for national security. The CIP, therefore, helps to buttress the KYC process, which seeks to give the financial institution a clearer picture of what activities can be expected of every customer, be they an individual, a company, or another entity.

KYC processes strengthen the AML program by enabling financial institutions to focus on their higher-risk accounts. Determining acceptable KYC processes depends on several factors, including the institution's size, risk profile, and risk appetite. However, KYC processes are considered an “evolving continuum.” The regulatory environment is ever-changing, requiring institutions to adapt their procedures to ensure compliance. In addition, the nature of KYC processes means that they are not static; customers' behaviors and, therefore, the perceived risk levels associated with their accounts are subject to change.

### 4.4.2. Customer Due Diligence

Customer due diligence (CDD) is the process of assessing the risk posed by a customer, and then mitigating that risk with appropriate KYC controls and ongoing monitoring. Money laundering and terrorism financing risks vary by the location and activity of the customer and the nature of the transaction. A CDD process encompasses obtaining identifying and verifying the identity of the customer, understanding the purpose and expected nature of the business relationship, obtaining information on or establishing the business entity’s ownership and control structure, assessing the money laundering and terrorism financing risks associated with the customer based on transactions conducted in the course of the business relationship, and ongoing monitoring of the relationship.

In a CDD process, the financial institution assesses the risk profile of the customer. Risk profile components include the nature and purpose of the business relationship, the type of customer, the type of products or services requested, geographic location, and the customer’s expected use of the product or service. Factors used to conduct the risk assessment can include the customer’s accounts and transaction history, the transaction amounts, and the frequency or duration of transactions. Risk profiles should identify higher-risk and lower-rate customers. Enhanced due diligence procedures are required for high-risk customers, while simplified procedures can be applied to low-risk customers. The accounts and transactions of customers without an established relationship can also be high risk and should be subject to closer scrutiny, including file notes documenting the reason for the relationship and the type of activity.

### 4.4.3. Enhanced Due Diligence

The need for Enhanced Due Diligence (EDD), or Supplemental Due Diligence, is determined by risk tolerances and policies or by the choice of the client. What the organizations would typically do is perform a standard level of Customer Due Diligence (CDD) and after evaluation, determine if they should have done signaled EDD or used an example of a clear account. Research on the client’s background may be conducted if the organization’s risk assessment shows that any of the above signs are present, including examination on public databases, peer-written information, prior working experience, risk on the job performed by the client, etc. If face-to-face verification is unable to be accomplished, the organization’s policy must determine how this is treated. There are two common ways that organizations approach this: either they would flag certain documents or they would put the client on a no-plan basis. Part of the documents included in KYC documents are: Identification Records, Address Verification, Client’s Income Source, Occupation Assessment, Government Document Type, Client Contact Point History, Phonetic Name in Japanese and Roman, and Client’s Name History. KYC Trusted parties typically do not appear online. The access required is unique to account managers or the like. Being unrelated to the client being studied also helps to ensure this. It is best to research or verify everything that you can find before launching into a full-on KYC. The entire KYC effort includes not only analyzing to expand or prove links and relationships but also physically meeting the clients to obtain signed forms.

## 4.5. Technological Innovations in AML and KYC

As described in this research work, most AML/KYC technology innovations employ machine learning, data analytics, and blockchain technology, or a combination thereof.

Infogrlaphce
Anti-Money Lauidering Srvering
AR Ipowed tanopiera Nonitore flunnolgisēninin
oives ger innohtion bar timmorunolping staretur a
éresep at wadsteyıdo s tomed. loard sssem ıoors.
Gred mord
AI
1

**Fig 4 . 2 :** Technological Innovations in AML and KYC

The implementation of AI and machine learning has transformed the AML/KYC landscape tremendously during the last two years. Financial institutions are moving from intermittent reporting to daily reviews of client transactions, and machine learning has empowered them to do this at global scales, including millions or billions of transactions. Machine learning software tools have advanced and proliferated quickly. Hardware constraints of the past have been removed with the rapid growth of Computing Clouds. GPU acceleration has made parallel computing on personal computers an easy and low-cost operation. More than 95% of all transactions are now considered low risk. Responding to a fast-changing regulatory environment and increased expectations from customers, several banks are investing significantly to reinvent their KYC processes with the help of technology. Some such banks have developed KYC utilities that are powered by a shared domain infrastructure, with secure scheme stamping and a single trusted source of truth for risk-relevant data, making it possible for multiple financial institutions to manage their customer onboarding and due diligence processes jointly. As this work delineates nicely, collaboration among financial institutions in sanction screening, transaction monitoring, and real-time risk assessment along the customer lifecycle is more than just a good idea. It is a best practice that is increasingly required by the regulators. Technology has the potential to make information sharing simple and cost-effective, allowing banks and their partners to fulfill regulatory expectations while providing better service to their customers.

### 4.5.1. Machine Learning Applications

In 1993, some neural networks for data mining were introduced but later became a little outdated due to their complexity. A data mining technique was developed in 2008, and it was proved in 2010 that neural networks have greater success. Afterward, the novel approach used a combination of dynamic neural networks to prevent money laundering. A study on money laundering prevention using dynamic neural networks is worth mentioning. Data mining methods put together with hot sets faced some problems but later in 2011, the feasibility of this issue was proved. A dynamic computational technique was suggested in 2014, with further implementation in the future. In 2017, there was a thought of enhancing the AML perspective and a potential data pooling scheme was discussed. Ordinal regression and transaction monitoring were merged.

In 2019, a machine learning framework for anti-money laundering compliance was proposed, called AMLX. AMLX walks through the general steps needed to complete a machine learning experiment and discusses ways to make a machine learning model to help facilitate a company's compliance with learning-based policies and secure that AML compliance is validated. AMLX offers a simplified view of the critical steps needed to build a machine learning model and is aimed to help anti-money laundering experts with little machine learning experience. AMLX draws from several libraries, including support for time series, automatic hyperparameter optimization, optimized for telephone dataset combined with transformation of the dataset, support for optimized hyperparameter selection for each target set dataset, automatic variable scaling, optimization for imbalanced datasets, and pipeline completion with various machine learning algorithms chosen and trained for the considered datasets.

### 4.5.2. Blockchain Technology

Attention has recently surrounded Blockchain technology, especially as regards virtual currencies. A blockchain is a decentralized approach to data storage that captures transaction records across large networks of users. Each block in the chain contains a set of transaction records. The hash of the previous block is stored, along with a timestamp and a set of transactions, inside a block in the Blockchain. Blockchains are accessible, in real-time, to all relevant parties, and hence are decentralized, providing transparency.

Each block in the chain is linked cryptographically to the previous block using a cryptographic hash. To achieve consistency along multiple copies of the chain, a consensus protocol is used, whereby a subset of participants in the network – the miners – work on solving a hard computational problem, the solution of which is unique and verifiable. The miners are incentivized to compete to consume resources to solve the problem by receiving a reward for publishing a new block, as well as transaction fees.

The consensus protocol does not allow any single miner to dominate the system, ensuring that block publication occurs regularly. A unique and verifiable solution to the problem is based on a cryptographic hash function with specific characteristics. If such characteristics make the hash highly random and difficult to pre-calculate, the effect of miners competing is that blocks are only published on average once every second, although they arrive randomly at that average rate. Following the publication of a new block, other miners will also complete the solution for the recently published block – but with non-trivial probability, delayed by a certain time duration.

### 4.5.3. Data Analytics

A key step for the proper execution of any of the mentioned AML activities is the collection and validation of the data needed. AML actors need to understand and quickly evaluate both the formal and informal economic behavior of customers to make fast and accurate risk assessments. In such a context, data analytics, combined with an in-depth analysis of source data, is crucial for relaying quality data, both enriching existing data and identifying relevant data that is missing or must be obtained.

Supervised or unsupervised learning can provide homes and businesses with a level of credit risk assessment and credit scoring that goes way beyond anything that is currently in use. Even without taking advantage of machine learning techniques, many historical patterns and changes could be detected, which could help identify high-risk profiles. These purely statistical analyses use methods such as linear regression or advanced clustering algorithms, and combination models built by hierarchically, sequentially, or even iteratively aggregating results from several decision trees or neural networks, which help segment taxpayers by levels of compliance or risk or to characterize events.

After identifying these risk profiles, it is also crucial that AML activities be sustained by an engine for statistically modeling more sophisticated taxpayers' behavioral forecasting, detecting trends or anomalies in taxpayers' behavior, or event-sequence clustering. Consequently, whenever deviation from expected or historical behavior is detected, real-time alerts are generated, so that instant review can be made by compliance officers or that some preventive or mitigation measures can be taken. These capabilities depend on many factors, among which availability and quality of data play a crucial role.

## 4.6. Real-Time Identity Resolution

1. Definition and Importance Real-Time Identity Resolution (RTIR) refers to the technology that allows businesses and organizations to validate and verify user identity in real-time against official trusted sources either internally or externally. For most of today's businesses, customers want instant response about whether their mobile number or email address is valid before verification to do business, not after payment as has been the norm. The ability to identify legitimate customers through real-time validation is crucial to eliminating lost revenue due to fraud, helping businesses meet trust and safety mandates, especially for payment cards and online transactions, increasing customer satisfaction, increasing revenue, and reducing chargebacks. However, failing to validate email addresses, mobile numbers, IP addresses, and other identifiers in real time could have serious consequences for a business. Every time a payment transaction fails, customers are frustrated with no reason why, chargeback fees are incurred, and banks become liable. Additionally, many firms ineffectively enabled KYC and AML processes due to the difficulty of deploying expensive RTIR False Positive verification processes. Virtually every industry housing sensitive or critical record needs the ability to validate the identity and demographic information of potential customers in real time. However, organizations often only automate name/account/ID validation processes for customer onboarding.

2. Techniques for Real-Time Verification There are several ways to ensure Real-Time Identity Resolution during each stage of the process. The first step is either pre-customer onboarding, or more ideally, KYC and AML Identity Theft Prevention, and checks the customer's mobile phone number associated with the account or email address submitted. These checks consist of direct requests quality assurance checks, and trusted information provider vendors. Missions that require commercial transactions cannot afford to deploy and rely on outdated testing. During the second phase, RTIR links are confirmed correct by testing provided via unique invitation links to sensitive information leveraging stable and trusted sources to verify the identity. The links then go to files uploaded encrypted to those trusted sources, which are additional services that ensure both the accuracy of data and the security of critical personal information.

### 4.6.1. Definition and Importance

Real-time Identity Resolution (RIR) is the capacity to accurately identify a known individual by comparing a source identity, such as a phone number or credit card number, with an identity profile stored in an identity resolution system. For an RIR system to have market value, it must deliver this capability in a manner that is permissive, instantaneous, highly available, and scalable. If the system only works on a small number of individuals or only for a specific and brief period it has no market value.

It must also be extremely accurate – a consequence of the need for rapid KYC clearances of legitimate customers. RIR must be compared to the alternative of batch identity resolution or identity verification, which has existed in universes for a long time. In this scenario, an identity resolution service provider is engaged by a financial institution to perform KYC or AML on several identities in a batch process. If there are tens of thousands of potential customers, that might not seem to be a very demanding requirement. But in fact, it is a very demanding and expensive service because it is often in a universe with tens of millions of people. Consequently, the service provider will often take up to 10 days to provide the cleared list and many users will have to resort to alternative financial service providers to still make timely decisions.

In comparison, RIR must be "perfect," essentially instantaneous, and extremely inexpensive, because the decision must be made within seconds. If the lists of transactions being screened and the individuals on those lists are not current, if the identities are in a foreign database, or if the process involves some of the complex algorithms often used for identity resolution, the service provider will often be able to return an answer only after an hour or more. And that clearly cannot be allowed to happen if RIR is to serve these critical operations.

### 4.6.2. Techniques for Real-Time Verification

A given individual is usually a member of many different databases. For example, a bank may store one's name for a bank account, a merchant may have a name on a credit card, and an insurance company besides the bank may have the same name on an insurance policy. Unless maintained in synchronization, the information in different institutions may differ in some format aspects like: Name spelling, Name transposition, the presence or absence of one middle name, the presence of a family name suffix, etc. Furthermore, also different verification policies and questions exist. Nevertheless, we use a generic scoring function, which summarizes the confidence that two names refer to the same individual. It receives input strings from two different databases that it is supposed to compare and outputs a score. Determining the score for two different names is done by comparing their tokens after normalizing both names with some techniques. Normalization consists of removing punctuation, accents, and mixed cases from the two original names to generate their tokens.

Even after normalization, two tokens from two different names may still be very similar, if not look the same. Their similarity can be calculated by a given similarity metric. The output score of the function for the two names is a combination of two sub-scores that correspond to comparing the family names and given names (i.e. first and possibly middle names). These two sub-scores are on a normalized basis; hence their values are in the range [0, 1). Scores may depend on the tokens and the similarity metric used. The identifier construction process is modular. The two key operations are tokenization and transformation, whose decisions affect the identifier calculation. There are many existing transformation algorithms. Tokenization and scoring are implemented for family names and given names. Security and other enterprise goals make it possible to reduce the number of compared pairs. For example, consider the reduction based on the comparison of face images attached to the records.

## 4.7. Risk Assessment in AML and KYC

Risk assessment is the foundation of know-your-customer (KYC) and anti-money laundering (AML) successful measures. It determines which customers need what levels of due diligence and analysis, and what appropriate transaction monitoring and reporting should be provided. Priority in resources, not only in the KYC and AML but in many other domains, should be based on the relative riskiness. Risk departments in many financial institutions are largely supportive and secondary to the main lines of management and operations. The result is that assessments are compromised by a lack of weight and authority.

Despite the development of advanced deep learning, graphical models, simulation forecasting, and other AI and machine learning technologies for assessments, actual risk assessments are often limited and do not accurately measure or project money laundering potential by customer or transaction types or amounts. Basic data on ethnicity, nationality, source of funds, types of business and dynamics, arrangement complexity, physical locations of high-risk jurisdictions, family and business associations, and similar foundational data could easily be converted into dynamic scoring models.

All businesses have risks. In banking, insurance, investments, remittances, and monetary exchanges, the core risk is the financial loss that would be incurred if the money laundering that is intentionally concealed behind the financial transaction is detected. A combination of substantial penalties in the form of monetary fines, company and individual loss of reputation, career, and retribution, as well as personal sanctions, is the motivation for the KYC/AML compliance process. Financial transaction fraud and theft have a potentially damaging impact on all businesses, monetary relationship or not. KYC/AML should also be in the risk forecast and pricing equations for all other businesses.

### 4.7.1. Risk-Based Approach

Risk-based approaches to Anti-Money Laundering (AML) and Know Your Customer (KYC) measures emerged in the late 1990s. Financial resolve understands that criminals seek to utilize the financial system to move their illegal funds to create illegal accomplices. Thus, any customer request for moving funds into or out of the financial system exposes it to AML and KYC risk. Financial institutions understand that all customers cannot be treated as criminals, and attach a level of risk to every customer request recorded on its books. Maintaining a risk-based attitude towards criminals and other associated clients interacting with the financial industry is essential. Over the decades, other financial institutions have further developed their position on the subject. External pressures come from increasing expectations of law enforcement, negative media exposure, court cases, and fines related to AML failures.

Every financial interaction with the customer could be considered for carrying reduced or higher risk. Financial institutions measure the customer-attributed risk for the duration of moments, pre-transaction, transaction initiated, transaction completion, and post-transaction analysis. Financial institutions therefore maintain an attitude of customer risk by reference to three parts of the risk equation, pre-screen and monitor all high-risk international transactions, instantaneously perform AML Transaction Monitoring reviews, accelerated profile updates, perform enhanced due diligence for authorities, comply with State and Federal Privacy Laws, protect customers and identity verification data from internal and external threat actors. Funneling participation-micro-businesses-interactions into direct events should resolve the problem of AML and KYC overweight with flow-through activities. The goal is to allow every world citizen to leverage the advantages of transferring funds into or unto the two largest banks.

### 4.7.2. Quantitative and Qualitative Assessments

There are two primary approaches employed when assessing risk: qualitative assessment and quantitative assessment. A qualitative assessment relies on subjective judgment, pre-defined rules, best practices, personal experience, and analysis of past negative outcomes. Assessments can be prepared by an individual or a group. This process should be documented and operated by its policy and procedures with well-defined minimum competencies for the qualified staff who draft such assessments. A qualitative assessment can be completed for any potential risk in any type of jurisdiction. Limiting a qualitative risk assessment to a small number of jurisdictions does introduce a level of risk because there are criminals that may target them. At a minimum, it should be more detailed for the larger jurisdictions and only built to higher levels of regulation that apply broadly to the country or sector. Some issues may be related and not warrant a separate assessment.

On the plus side, qualitative assessments can be completed by personnel who may not be trained in advanced statistical analysis. A qualitative assessment is also flexible and can be quickly modified to cover newly identified risks. However, qualitative assessments rely heavily on assumptions made by an individual or small group of individuals. They are also highly sensitive to these assumptions. They are generally less expensive to obtain. Most importantly, qualitative assessments should be easier to explain to concerned citizenry as they are perhaps more intuitive than quantitative assessments. The drawbacks can include subjectivity and the assessment can be quickly out-of-date. Because many of these issues are not strongly correlated, if one country begins to notice a significant increase in some illicit activity, it would be advisable to have controls in place to prevent an increase in that particular type of illicit activity.

## 4.8. Challenges in AML and KYC Implementation

The implementation of Anti-Money Laundering (AML) and Know Your Customer (KYC) protocols for transaction monitoring can pose several significant challenges for financial institutions. These challenges not only present barriers that must be overcome but also usually require the acquisition of complex technology that must then be implemented correctly to mitigate financial risk while also remaining compliant with legislative rules and laws. However, for whatever level of difficulty there is in their implementation, these protocols are necessary.

Data privacy is of paramount importance to banks and other financial institutions. Customers need to be assured that the information they provide will not be handled in ways that may breach other important facets of banking. Collection and analysis of customer commercial data patterns encompass sensitive information related to transaction activities for all financial institutions. It can be concerning for customers to know that their activity is being monitored, and negative press can inform them of rights involving data privacy concerns. There are laws related to data monitoring activities that must be followed. Compliance with these laws regarding data sharing must be carefully planned before the implementation of an AML/KYC program, and there could be issues related to data set acquisition if learning models from third-party vendors are used.

Integrating AML and KYC protocols into existing systems may pose some operational difficulties for some banks and financial institutions. Depending on the size and capabilities of current systems, it may involve hiring someone to evaluate what technologies currently in place that support transactional activity monitoring may not interface properly with new AML/KYC capabilities. Banks have legacy systems that run on older technology. Operational risk can threaten bank business functions, and systems should be reviewed to confirm that there will be no interruptions to day-to-day banking operations. Finally, regulatory compliance can vary from country to country, and the correct government and non-government entities must be consulted before any implementation of AML and KYC protocols is executed.

### 4.8.1. Data Privacy Concerns

The world of money is amid a major evolutionary leap, brought on by the mounting demand for Speed, Ubiquity, Traceability, Inclusivity, and Trust. The migration from traditional cash to digital alternatives has been accelerated by the pandemic, and spurred by the advent of digital assets in the form of Cryptocurrency, Central Bank Digital Currency, Stablecoin, and Digital Wallet. Enacting the anti-money laundering regulation that drives digital assets to setback toward traditional finance is a misplaced panic. These amendments in the AML regime serve to plant the money in all modifiable and traceable electronic formats. Appropriate application of AML Know Your Customer on behalf of users of Digital Finance demands the same 5 essential principles of Money – Speed, Ubiquity, Traceability, Trust, Inclusive – but in a 180-degree reversed implementation. So, we land squarely within the realm of Biometrics and AI. User enrollment and identity resolution are required to be biometrically authenticated in real time on each user transaction. Digitized KYC of unrepeatable identity for users of Dig-Fi must pass privacy issues mandated by privacy regulations. The principles laid down five categories of data subject rights including privacy by design, data minimization, storage limitation, and accuracy in KYC. Within the context of privacy laws, biometric data is sensitive data. Data Protection Impact Assessment must be sequentially carried out for each stage before, during, and after the Dig-Fi adoption implementation.

### 4.8.2. Integration with Existing Systems

The integration of new AML and KYC systems with existing business and financial infrastructures, including activity monitoring, transaction cycle management processes, sign-on control systems, and even legacy database systems is a concern. Certainly, if there is a potential delay in the timeliness, efficiency, and accuracy of the identification of sanctioned parties or the monitoring of the transactions conducted by customers that could conceal or facilitate money laundering operations, this would be of great concern to any organization.

However, the need for centralized real-time identity verification, address verification, identity resolution, and activity monitoring functions are key to the detection and reporting of significantly dangerous money laundering activities and accomplices to terrorists or their benefactors. Processes that are neither real-time nor digital, such as credit entries, goods/services sold, shipping details, vendor codes, and air travel, are indications of a potentially illicit transaction connected to a sinister purpose. If the linking of highlighted behaviors that could indicate terrorism financing operations is not centralized in real-time, there is the possibility of decision logic not being considered. Additionally, if the linking of terrorist behavior direction centrally could not be discovered, then significant money laundering and AML efforts would not be connected.

Without centralized analysis, it is impossible to compare historic behaviors across accounts and organizations, thus inhibiting the accurate detection of illicit activity conducted across systems and institutions.

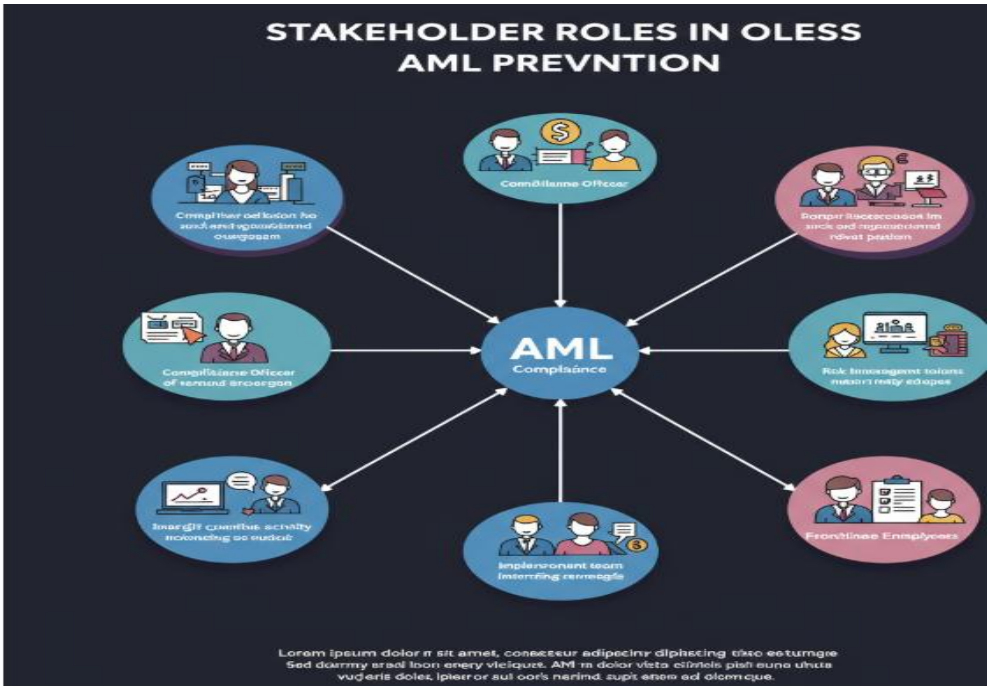

**Fig 4 . 3 :** Stakeholder Roles in AML Prevention

If existing processes become so cumbersome, slow, and error-laden because of the bottleneck effect of legacy KYC, AML, and transaction processing systems that legitimate transactions are rejected or flagged much too often, then existing corporate activities and most importantly, corporate profitability, are endangered. Outdated and time-consuming KYC and AML processes and bureaucratic controls that add cost and delays associated with the operations of no-fault organizations will lead organizations not to behave as wanted and are uneconomic.

### 4.8.3. Regulatory Compliance Issues

Regulatory bodies have opined that for data privacy and protection laws to apply, there must be ‘processing’ or intent to ‘process’ data without exception. Several laws also recommend a risk-based approach to KYC implementation and AML compliance. This risk-based approach is essential when addressing applicable data privacy, protection, and security laws. Such laws are aimed at businesses that typically face stricter KYC validation, AML compliance, and privacy compliance requirements. For any KYC validation or AML compliance solution, consider the following steps to assess it against data privacy, protection, and security requirements:

- What kind of data is being used, and what are the KYC checks or AML compliance checks being performed? Is there scrubbing done with a PIP definition that addresses KYC and AML compliance screening?

- For what purpose is the data being used? Consider “expected purpose” contained in applicable laws or contracts with customers, as well as the terms and conditions from the third parties providing the data that allow for commercial or non-commercial use. For what purpose is the KYC or AML screening being used?

- Is the data processed by a provider located in a jurisdiction with less strength of data privacy protections than the relevant business? If so, then the risk of allowing for data processing is greater, especially if the personal data may be disclosed to a third person outside the jurisdiction of the provider.

- Check if the KYC or AML screening is happening in real-time or bulk processing, or if risk-based processing is being used.

## 4.9. Conclusion

Summary and Future Directions in AML and KYC Practices

The challenges of modern anti-money laundering (AML) detection and response systems cannot be understated. Financial threats caused by terrorists and criminals and their usage of sophisticated schemes to cover their tracks and avoid detection by AML systems are a continuing challenge for the financial industry. Technologies that can improve current AML procedures by automating customer due diligence (CDD) are in extreme demand. Financial institutions must also consider that many of these new technologies will require regulatory approval or re-interpretation for adoption, especially for the porous border between CDD and transaction monitoring.

The KYC automation process takes what used to take weeks or months to perform and automates it to the point where it can be done in a few hours and potentially at a lower cost with improved quality. While the concept around KYC may be as simple as obtaining information from potential customers during the account opening phase, applying the correct data attributes to make risk-based decisions around which customers need to be reviewed, what data should be pulled, how to pull it, and how often it should be reviewed requires technology that can pull together the best sources of internal and external customer information all in one simple package. There are still many questions to be addressed along the way, as well as exciting challenges such as regulatory re-interpretation, the standardization of data-sharing partnerships, and the development of KYC utility models that will benefit all stakeholders in the future direction of the AML KYC industry.

### 4.9.1. Summary and Future Directions in AML and KYC Practices

The development of anti-money laundering (AML) and know-your-customer (KYC) regulations has moved from the original basis of preventing terrorism and crime financing through safeguarding trust in the banking system to compliance-based regulations that sometimes fail to achieve results. This has resulted in strain on small banks and credit unions in the United States. New tools for real-time KYC enable banks and nonbank financial institutions to ensure strict compliance with KYC regulations and help speed up regulatory approval while lowering costs for regulators and compliant banks. Regulatory technology also decreases regulatory burden and expectations in banks in smaller states that have low traffic in high-risk areas. Furthermore, the AML and KYC processes have been unduly manual when the actual risk of transactional money smuggling is very small. Automated AML processes, sensitive to money laundering attempts while adjusting to normal customer transactions, both lower costs of alerting banks to only risk transactions as well as the overreporting of nonadvantageous false positives to regulators. These trade-offs require the development of intelligent tools for real-time business and individual identification and risk profiles that ensure AML and KYC business efficiency for banks and regulatory relations and safety. The use of AI and blockchain technologies proves vital in achieving efficiency gains and security in the AML and KYC processes. Dynamic actor KYC identification and risk profiling are cornerstone technologies that enable banks and other financial institutions to perform KYC operations at the same level of sophistication, speed, and level of accuracy as they perform AML functions. The use of real-time actor identification and risk profiling in enforcement before onboarding bank customers opens the door to real-time capability.

## References

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Financial Sector: Legal, Regulatory, and Technological Aspects. Computer Law & Security Review, 32(1), 4–14.
https://doi.org/10.1016/j.clsr.2015.12.010

Colladon, A. F., & Remondi, E. (2017). Using Social Network Analysis to Prevent Money Laundering. Expert Systems with Applications, 67, 49–58.
https://doi.org/10.1016/j.eswa.2016.09.029

Campedelli, G. M., & D'Ignazio, A. (2021). Money Laundering and Financial Intelligence: A Literature Review Across Disciplines. Journal of Financial Crime, 28(2), 556–573.

https://doi.org/10.1108/JFC-06-2020-0107

Lin, J., Wang, Y., & Zhou, Y. (2020). AML and KYC in the Era of Big Data: A New Paradigm for Financial Crime Prevention. Journal of Risk and Financial Management, 13(12), 306. https://doi.org/10.3390/jrfm13120306

Zhdanova, M., & Moulin, B. (2020). Real-Time Identity Resolution for Financial Fraud Prevention. Procedia Computer Science, 176, 2728–2737. https://doi.org/10.1016/j.procs.2020.09.316