Intelligent Information Management, 2023, 15, 284-305
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

Using Artificial Intelligence to Combat Money Laundering

Rashid Alhajeri[1], Abdulrahman Alhashem [2]

[1]School of Law, Case Western Reserve University, Cleveland, USA
[2]Naif Arab University for Security Sciences, Riyadh, Saudi Arabia
Email: alhashem.abdul@gmail.com

How to cite this paper: Alhajeri, R. and Alhashem, A. (2023) Using Artificial Intelligence to Combat Money Laundering. *Intelligent Information Management*, **15**, 284-305.
https://doi.org/10.4236/iim.2023.154014

Received: June 11, 2023
Accepted: July 21, 2023
Published: July 24, 2023

Abstract

Banks and other financial institutions handle sensitive records regarding people, trusts, and corporations. Money, as a sensitive and useful commodity, makes financial organizations valuable and prone to criminal elements. Common criminal activities that target the banking sector include money laundering, identity and personal records theft, and terrorism financing. These are global issues that have garnered the attention of international bodies and governments. One method proposed to deal with illicit finance and money laundering is artificial intelligence (AI). AI implements various algorithms and techniques to monitor customers, markets, and financial transactions that help identify various banking habits. Understanding clients' transactions and the nature of bank transfers enables AI to prevent and combat money laundering. This research offers an understanding of how artificial intelligence is used in the financial system to combat fraudulent activities such as money laundering. It is organized into five chapters covering various aspects of artificial intelligence and money laundering.

Keywords

Artificial Intelligence, Machine Learning, Money Laundry, Financial Institutions

1. Introduction

In a digital world, we must use technology (appropriately) to help us better identify ML and TF activity. While there is much more data to sift through, tools like machine learning and smarter screening can help both financial institutions and government authorities become more effective in their AML/CFT efforts. In relation to preventive measures, we are seeing faster and better screening tools and

pooled KYC via hashing and information sharing. [1]

Technological innovations are essential economic drivers because they improve productivity and efficiency. Artificial intelligence (AI) is an important technology made possible by the growth of interconnected devices that collect data that is transformed into automation. AI is manifested as machines that exhibit certain aspects of human intelligence, like decision-making and cognition [2]. This definition of AI includes machines that perform actions initially performed by people without intervention. AI is commonly used in the service sector, such as in health care, and in homes, restaurants, and banks. Large volumes of data make it easier for engineers to train computers to identify thinking patterns used to mimic human behaviors [3]. AI has further transformed the global financial sector. Automated teller machines are an example of the earliest form of AI in banks [4]. However, the adoption of AI in the financial sector has increased, especially in combating online fraud, terrorist financing, and money laundering.

Financial institutions adhere to certain standards designed to ensure that all sources of funds and transactions are legitimate. Illegal processes of transferring money, including finances generated from criminal activities like funding terrorism and human or drug trafficking, have specific legal implications. However, unscrupulous individuals liaise with corrupt financial organizations to channel money from illegitimate sources into the economy to appear legitimate. Criminals assisted by organizations find ways to deposit large amounts of cash to various accounts, which are later channeled into other sources to give the money credibility. This process of cleaning dirty money is known as laundering, and it is a common white-collar criminal offense.

Financial institutions have designed anti-money-laundering (AML) policies to detect and prevent this criminal activity. The AML laws focus on a limited range of transactions and behaviors, and they have substantial implications for curbing money laundering. The recent development in technology has also facilitated the detection and prevention of illegal financial transactions in businesses and financial institutions. Specifically, AI is one of the current AML techniques aimed at stopping money laundering. The AML program consists of four pillars: having a compliance officer, ongoing training-independent audits, internal policies which are (customer due diligence, transaction monitoring, and suspicious transaction reporting.)

The money laundering process typically involves three steps. The first step is placement, in which the launderer injects money obtained from illegal sources into a legitimate business [5]. Layering is the second phase in money laundering, which involves concealing dirty money through bookkeeping and transactions. Finally, the integration step consists of withdrawing the laundered funds and moving them to legitimate accounts identified by the criminals. This money laundering process uses methods of varying complexity, as discussed in this paper.

This paper will define the concept of money laundering in general, as well as

define AI and the methods of using it to protect the financial system and the flow of financial integrity to combat money laundering and terrorist financing.

2. Literature Review

Law enforcement officers have been fighting against financial crimes and money laundering for a long time. According to Jensen [6], the US Senate first established a subcommittee to investigate the use of AI technologies to detect money laundering in 1994. The investigations revealed that wire transfer technology is used to transfer money made in the US illegally to other countries. As a result, the subcommittee proposed using AI in three key areas: knowledge acquisition, data exploration, and knowledge use [6]. The knowledge acquisition approach calls for machine learning, statistical modeling, and knowledge discovery to create money launderer profiles history. In doing so, the authorities and intelligence agencies could distinguish between illicit and legitimate wire transfers. After identifying illegal profiles, the subcommittee recommended using knowledge-based systems, which would track and update new profiles because money launderers are known to adapt. Finally, data exploration facilitates visualization and link analysis, including identifying and evaluating networks of people, things to buy, and places of transferring [6]. This report forms the basis of how AI systems are used in combating money laundering. One of the challenges known in using technology to fight money laundering is high false-positive rates. This means that investigations might pick up legitimate transactions as illegal, making it difficult for crime units to investigate laundering cases. As a result, Gao and Ye [7] propose a data-mining-based framework to use in money laundering cases. In reality, gaining evidence from a single case does not help investigators apprehend many money launderers. Therefore, there is a need for a system that links powerful people, connections, or sub-groups within a money laundering scheme. Gao and Ye [7] argue that a data-mining-based approach is essential in constructing and evaluating a suspicious transaction indicator system, which could help identify and visualize a money-laundering network using unsupervised techniques. Only a few proposed money laundering systems have been tested in the real world. A study by Moustafa [8] proposes a two-phase AML system that was tested using different case studies. The suggested system is a planned-based framework for AML systems (PBAMLS), with the first phase as a monitoring phase and STRIPS Stanford Research Institute Problem Solver based planning as the second stage. The framework contains many supporting modules, such as data collection, link analysis, and risk scoring. The data collected for the system include customers' profiles, historical transactions, and sanction lists, which enables investigation. Link analysis helps identify powerful people, organizations, and perpetrators of laundering money. The PBAMLS use an association matrix algorithm and a cycle detection algorithm. Finally, the risk scoring module assigns a specific score for suspected transactions to suspected behaviors or violated rules [8]. The system utilizes KYC, rule-based monitoring,

cycling detection, and suspected link monitoring using the planning phase's automata approach. The case study reveals that PBAMLS are better because of their reduced false alarms, which boosts the decision-making process. It integrates web services that discover similar structured crimes that could occur in the future.

3. Definitions of Money Laundering and AI

Money laundering is recognized as a global issue and a cross-border crime because it is linked to organized crime, terrorism, and human and drug trafficking. Criminals involved in illicit business activities conceal their proceeds using money laundering. Several activities constitute money laundering, including transferring illicit cash/assets; possession, conversion, or use of illegal profits; failure to report laundering acts; and consulting on, facilitating, and abetting money laundering [9]. These criminal acts aim to conceal the origin of the funds/property, and make them appear legal. Money laundering has negative effects on the economy as it contributes to the growth of illegal business and affects the economy [10]. Covert activities include tax evasion, drug trafficking, corruption, human smuggling, organized crime, and unreported businesses that do not pay taxes. These criminal activities lead to the destabilization of the economy by spreading unemployment and economic inflation and its negative impact on the ligament business especially the small ones. Several stages are involved when moving illegally obtained funds through legitimate businesses or people until they make their way back to the owner as clean money.

3.1. Money Laundering and Its Stages

Money laundering "is the processing of criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source" [1]. There are three stages of money laundering. The first stage, placement, is probably the most crucial and challenging stage for money launderers and the easiest stage for law enforcement to discover because it must eliminate plausible evidence indicating the money's origin [11]. Large sums of cash are injected into the financial system through structured deposits or by combining them with legitimate business proceeds. The most commonly used legitimate enterprises are entertainment shops, liquor stores, casinos, and restaurants. Currency smuggling is another common approach to placing illegal cash into the system. It involves moving the currency illegally in or out of a country using different transportation techniques that do not leave an audit trail. Security brokers and currency exchanges also provide an outlet for money launderers to move money. An asset purchase is another common placement approach that enables criminals to change illegal bulk cash into valuable assets.

The second stage of money laundering is concerned with hiding the trail and making it difficult for auditors to follow laundering activity. This phase is known

as layering, which involves moving the funds in a financial system through a series of complex transactions [12]. The cash injected into the stream is converted into monetary instruments by involving banks and other entities. For instance, money orders and banker drafts are drawn to help complete the transactions. Additionally, the funds can be used to acquire material objects instead of holding cash. Materials bought using criminal money are then resold, making the source of the funds difficult to trace. It is also challenging to seize assets compared to unreported bulk cash.

The laundered money is eventually moved back into the economy as legal funds in the final stage, referred to as integration. This phase involves incorporating funds into the legal economy, and successful laundering is completed so that it is impossible for authorities to trace the origins of illicit funds [11]. Unlike in the layering stage, the detection and identification of funds as laundered, in the integration stage is when the money goes back to the financial system and appears as legal business proceedings. Several known integration methods include property dealings, front companies, false loans, and false import and export invoices. For instance, money launderers lend themselves money from front companies, making these seem like legitimate transactions. False invoices are also effective approaches to integrating illegal funds into the economy. Companies over-evaluate their funds, which helps them justify to authorities the source of cash deposited in banks.

3.2. Money Laundering's Impact

As noted earlier, money laundering is the process of making illegally obtained money appear legal. Dirty money is pumped into the economy through a series of transactions, many of which have negative effects. Money laundering injects large amounts of uncontrolled, illegal funds into and out of circulation, leading to the destruction of the national economy. Huge cash inflows in a country distort the demand for cash and interest rates, leading to inflation [13]. On the other hand, billions in cash outflow from an economy destabilizes and threatens the development of that country and the international financial system. Deregulated money means that capital and funds can move in and out of places within seconds. Such cash often leads to increased demand and consumption of luxury products, with a significant increase in imports, foreign payments deficits, and exports. As a result, this consumption contributes to increases in inflation and interest, leading to unemployment [13]. Those cases of instabilities caused by the demand for black money significantly negatively affect monetary policy.

Money laundering's primary source of illegal revenue in the shadow economy is informal sectors, and underground activities [13]. Because unreported income streams from the legal production of goods and services also contribute to unlawful activities, this does not necessarily mean that the entire source is illegal. However, the bigger the shadow economy, the harder it is to separate legal from illegal transactions [10]. The shadow economy involves fraud for financial gain

used to fund international criminal activities. For instance, Hetemi [14] report that in 2009, illegal funds generated from organized crime and drug trafficking contributed to 3.6% of the global GDP. A significant percent of these funds (2.7% or $1.6 trillion) was laundered and injected into the global economy.

Money laundering creates risks and vulnerabilities exploited by individuals who conduct criminal activities at the geographic and business levels. Money laundering threats include organized crime infiltration, illicit markets, tax evasion, and underground economy (Savona & Riccardi, 2017). Unreported financial transactions give rise to drug trafficking activities, sex exploitation, counterfeiting, and organized property crime, as Money laundering introduces vulnerabilities such as high use of money transfers, the presence of transit hubs, cash intensiveness, and the opacity of business ownership. [15] analysis of the impacts of money laundering in Europe reveals high levels of mafia-type infiltration, underground economy, and cash intensiveness in Italy in the Calabria provinces, the UK, and the Netherlands. Such money laundering risks are significantly linked to a high rate of suspicious transaction reports. The affected locations are exposed to serious organized crime.

Money laundering is a critical problem that significantly affects the socio-economic structure of a society. In developing countries, especially in African countries, about 80% of households do not use formal banking, which creates a problem as informal economic activities are often unregulated [16]. Therefore, unregulated sources of income significantly affect indigenous entrepreneurs. For instance, illegal funds are used to import products sold at marginally low market prices, thereby driving genuine entrepreneurs out of business. Money launderers are not interested in making profits but in cleaning dirty money. As a result, they engage in unscrupulous activities that force genuine companies that pay taxes to the government out of the system, Financial institutions' involvement in illicit money laundering activities deteriorates their reliability, making it difficult for foreign investors to invest. For instance, in the 1980s and 1990s, many Nigerian banks were involved in money laundering, which led to their disintegration and liquidation, and many people lost their savings [16]. Foreign investors could not venture into Nigerian businesses because of liabilities created by money launderers.

Money laundering affects the economic development of the country at various levels. First, it increases the shadow economy's growth and illicit flows, tax collection, and criminal activities [10]. The negative issues associated with money laundering include concealing illegal funds in the importation and distribution of luxury goods, like automobiles, and drugs. People also use illicit money to fund political insurgency, corruption, and organized crime, affecting socio-economic development.

3.3. Definition of AI and the Use of It

John McCarthy, a math professor at Dartmouth College, coined the term "artifi-

cial intelligence" in 1955 and organized the seminal conference on the subject the following year [17]. AI is a computer science sub-set that encourages robots to think or categorizes them as human beings. It works to create "intelligent" machines that can think, communicate, and conduct themselves in some of the same ways as humans [18].

Most of the studies have divided the levels of artificial intelligence into 3 levels

1) Artificial Narrow Intelligence (ANI)

These machines have a simple, narrow range of functions that they perform like Speech-recognition machines that only respond to voice commands to carry out specific tasks for example Google Assistant, Alexa, Siri in apple products.

2) Artificial General Intelligence (AGI)

Machines that have like human cognitive abilities. This type of AI is capable of working alongside humans. Currently, example of it like machine learning and robotics.

3) Artificial Super Intelligence (ASI)

Currently this type of AI does not exist yet but the idea of it that AI machines will be able to perform tasks and things that only natural person is capable of intelligence [19].

In our study we will be focusing on the second type of AI in this paper.

AI has a lot of major subfields under it one of them is machine learning the main focus in this study will be on the machine learning and the types of it

- One of the subfields of artificial intelligence is machine learning. Machines take data and learn on their own. ML enables a system to learn to recognize patterns and make predictions on its own. Machine learning systems can apply knowledge and training from large data sets quickly.
- The machine learning uses one of the AI languages which is python as there are multiple languages in the AI data base but this type is more popular and easy.

There are lots of types of machine learning algorithms we will mention the common once:

1) Supervised learning

This is a technique in which we use labeled data to teach the machine. We specify and identify the data that is fed to the device in this case. You'll get a labeled output from supervised learning. The most important aspect of supervised learning is that the model is trained using a labeled data set such as age, salary, time, locations etc. To accomplish this, we must first create a database of people with all of the necessary information and then label it to obtain the desired outcome for example it can be used to approve on credit card requests. [20]

2) Unsupervised learning

This technique based on Building a machine learning model without labeled training data or human interaction, based entirely on the data provided, requires an unsupervised learning algorithm to divide the given dataset into groups, allowing the algorithm to act on that data without being guided. The machine will

then generate an output based on the data's most prominent features, finding meaningful patterns and groupings inherent in the information. It divides it into two groups, one group that are very similar and another group that is very different [20], our focus will be on the supervised machine learning.

Technological innovations are recognized as principal economic drivers, and AI is considered a powerful technology of this era. The biggest advances of AI include perception and cognition, which help in a wide range of devices and startups to augment human labor [17]. Recently, many technology companies like Amazon, Google, and Apple have featured AI in their product launches, such as Alexa, Google Assistant, and Siri, respectively. These AI help in day-to-day operations, including searching, location identification, dictation, and problem-solving. The advancement of AI methods such as machine learning has facilitated AI's integration in multiple business activities like manufacturing, transportation, retailing, finance, education, and health care.

This section explores AI methods in the financial system, specifically looking into their use in money laundering detection and prevention. AI is transformational, especially in the financial sector, where crime detection is a priority.

The growth in technology has diversified money transfer options, including wire transfers, currency exchange, anonymous online payments, cryptocurrency, and peer-to-peer transfers. Electronic money transfers have added to traditional methods of money laundering. Therefore, AML needs to integrate technology to catch up with cybercrime as it is used by money launderers. Researchers have explored the viability of various AI and machine learning techniques in dealing with money laundering.

AI is implemented using various algorithms that monitor, collect data, and identify certain market patterns. The operating principle of AI techniques is almost the same because it includes exploring financial transactions that help to note habits, behaviors, and other features of bank transfers. The algorithms classify financial transactions as normal or fraudulent. The classification is based on training AI machines using past bank transactions that identify features that make up suspicious transactions. The algorithms' effectiveness and accuracy vary based on various factors such as training, data quality, and length of operation.

To generate alerts based on pre-defined rules, AML systems and software tools use a fuzzy logic system it is a method that doesn't use true and false to represent all logical shapes. Classical logic depends on 0 or 1 only, while there are other relationships in which the position in which it can be considered partly correct or partially false at the same time as it gives a percentage of the entered data to describe the situations in which the data are vague or not clear. Because fuzzy rules are not generated automatically, fuzzy logic captures specific statistical models created through intensive programming by a human [21] [22]. An expert-created set of conditional rules and knowledge is included in the fuzzifier. These rules are based on raw financial transaction data that are used to deter-

mine the strength of direct deposits and withdrawals. Each transaction is given a suspicious number [21]. The amounts, frequencies, and times of transactions are used to create rules.

ANFIS is crucial for tracking financial transactions and money laundering because it is used to map the relationship between input and output data. ANFIS has five layers and a number of nodes, some of which are adjustable and others of which are fixed, indicating the function of the node. This system analyzes and passes financial data from customers to the knowledge system based on the parameters provided [23]. The number of exchanges, standard exchanges, and real exchanges per week, for example, are among the parameters examined by ANFIS. The money exchange risk for each customer is calculated based on the client's typical economic transactions. Changes in customer consumption habits, such as increased online shopping and multiple deposits, would make abnormal transactions easy to spot.

In the process of cleaning illegal money and returning the clean money to the launderer, money laundering creates a path and a cycle. These trails are sometimes simple and sometimes complex, but they all form a network that can be followed with software [24]. Customers and users' transactions can be monitored by AI, which can help identify unusual or suspicious activities. Financial institutions provide operations consolidation, which keeps track of all the parties involved in a transaction. When transactions/users violate certain rules and parameters, machine learning techniques are used to generate alarms. To identify money laundering behaviors, the machine learning approach involves training a sample of raw data, which is then modeled, tested, and evaluated before being deployed. When a client meets or violates one or more conditions, an alert is generated [24]. Before it can effectively combat money laundering on a global scale, such an approach requires extensive training and evaluation.

4. The Use of AI in Financial Institutions and Performing Actions and Policy Procedures

For a long time, money laundering has been a concern for the global economy. Large sums of money are laundered every year, putting the global economy and security at risk.

This chapter aims to examine machine learning algorithms and methods for detecting suspicious transactions in depth and solutions for different types of money laundering.

Financial institutions have implemented AI to detect and prevent crimes such as insider trading, money laundering, fraud, and employee theft. These benefits are acquired by constantly experimenting with modern technologies, such as AI, in risk management to classify customers and transactions as either high or low risk. The AI algorithms implement predictive and other pre-defined binary rules to automatically analyze transactions' input and output. This enables an AI system to recognize any anomalies in the data provided, which flags and helps pre-

vent financial fraud. Additionally, scientists continually find ways to improve algorithms' accuracy and reliability, reducing false alerts as they analyze records more carefully.

AML solutions implemented in banks have a linear pipeline workflow that links with the data source. Data analysts and programmers then add certain parameters that help identify risky transactions, customers, or communications that might indicate fraudulent behavior. A typical AML system consists of four layers: a data layer, a screening and monitoring layer, an alert and event layer, and an operational layer [25]. The banking system relies on credible information provided by customers to monitor legitimate and suspicious activities. Therefore, the data layer is concerned with the collection, management, and storage of data. Financial institutions with effective AML systems do not solely rely on internal and employee data because they also obtain information from fraud watchlists and regulatory authorities. The data records are then analyzed using different AI and machine learning techniques natural language processing, that improves the capability of computers to read, understand, and derive meaning from human languages. And insights that help link relationships between clients and transactions [25].

The screening and monitoring layer analyzes clients and transactions for suspicious activities. This stage is automated, and it implements certain rule-based techniques this technique is to capture the expert skills of a specialized human and to incorporate them into a computer system. and risk analysis approaches. Rule-based systems have pre-defined parameters and thresholds used to identify launderers [25]. The AI systems need not be too strict, which could lead to multiple false alerts, or insufficiently strict, which could allow illicit transactions to occur. This layer obtains user information stored in the data layer to screen customers and transactions. Whenever suspicious activity is identified, the alert and event layer raises the alarm, indicating the occurrence of a suspected transaction. A human operator then reviews the raised issues and takes the appropriate actions, including allowing, rejecting, or blocking the transaction manually [25]. The manual operations of reviewing the transactions might overwhelm human operators, especially when a system reveals too many false positives.

The issue of many false alerts is resolved using a combination of AI and data mining techniques. One approach followed is outlier detection for fraud or laundering identification [25]. In this approach, researchers define various parameters of a peer group by analyzing its transaction habits. Hundreds of thousands of records spanning several months to years are needed to classify data into different clusters or groups. Such data are effective because they capture the similarities and differences in grouping transactions with the highest similarity index to one cluster. The accounts or transactions in one cluster are similar, and they are different from other clusters [26]. The benefit of this approach is that it helps group riskier accounts and transactions together. Additionally, because money laundering techniques evolve with time, AI can identify outliers and be-

havioral pattern changes. Therefore, AI and machine learning techniques can identify suspicious transactions or irregular networks of money transfers not defined within the outlier parameters.

Despite the glowing reviews associated with AI for dealing with financial fraud, certain limitations affect the technology's reliability. Users with malicious intent can exploit AI systems to threaten digital and physical security in financial systems [27]. AI can threaten digital security through a wide range of activities such as using machine and data analytics to social potential victims. AI can learn certain habits of bank users and profile them by stealing their credentials, which are later used in money laundering. Spear phishing attacks can be used to learn critical details about people or to steal money or personal information by approaching clients pretending to be a government trustworthy or financial department.

AI relies on the accuracy of data sets to effectively identify money laundering and illicit behaviors. Therefore, humans can alter AI-based AML systems' efficiency by conducting data poisoning attacks [27]. The data used in training AI systems can be poisoned by providing fake records, making the program learn mistakes that attackers later exploit. Since the process is automated, it would be difficult for humans to identify certain flaws, allowing launderers to operate uninterrupted.

4.1. Global Efforts Put in Place to Combat Money Laundering Using AI

There exist numerous international, regional, and local rules, directives, and regulations governing money laundering. The European Union, for instance, has anti-money laundering/countering the financing of terrorism laws that define some of the responsibilities of banks and insurers, such as KYC verification, monitoring and detecting transactions to high-risk countries, identifying politically exposed individuals, and reporting suspicious clients or transactions to authorities without giving notice to the customer [28]. There are special FIUs around the world that are designed to help with handling money laundering and financial fraud cases. FIUs handle suspicious activity reports from banks for further analysis before deciding whether to alert tax authorities, customs, prosecutors, or criminal investigators.

As noted, money laundering is a global issue, which means that different governments collaborate to resolve this problem. The Financial Action Task Force (FATF) is an independent international body tasked with developing and promoting policies that protect the global financial system against terrorist financing and money laundering [1]. This body has made several internationally recognized recommendations for global AML and counter-terrorist financing standards. Each country is required to identify risks and design policies; pursue perpetrators of money laundering, terrorist financing, and financing of proliferation; apply preventive measures for the financial sector; establish various pow-

ers and responsibilities for agencies tasked with AML; enhance transparency and availability of beneficial ownership information; and facilitate international coordination and cooperation [1]. There are 40 recommendations endorsed by 180 countries. FATF continually reviews these standards in collaboration with the International Monetary Fund, the United Nations, regional bodies, and the World Bank. Yearly reviews help FATF address emerging issues in money laundering, clarify various unclear directives, and ensure that the standards are rigorous for handling global financial fraud.

Regional principles and directives set for guiding particular areas also contain some form of universality. For instance, the Japanese Society for Artificial Intelligence Ethical Guidelines created a proposal for federal algorithmic auditing, which was later adopted by the US Senate Intelligence Committee [29]. The adoption of the report was aimed at guaranteeing unbiased decision-making. Additionally, the European Union (EU) developed the General Data Protection Regulation act to govern AI use in member states and all other entities handling data for EU citizens. International bodies governing AI, such as the Organization for Economic Co-operation and Development (OECD), work with regional organizations like the Artificial Intelligence High-Level Expert Group (AI HLEG) to create principles focusing on AI's ethics and trustworthiness. The OECD created AI regulation principles that were later adopted by the members of G20 [29]. The AI HLEG, under EU jurisdiction, created the Ethics Guidelines for Trustworthy AI. The principles from the two organizations focus on robustness and safety, transparency, privacy and data governance, human agency and oversight, accountability, and societal and environmental well-being [29].

Technologies dedicated to finance management have continued to grow. Currently, there are financial solution systems, both in practice and in development, that facilitate cashless payments, virtual currencies, and crowdfunding platforms that collect money from Fundraisers online. The main challenge is that millions of dollars are spent on AML compliance programs, making such services expensive. Therefore, financial analysts and developers are focusing on regulating the costs associated with such developments. For instance, AML significantly relies on KYC and CDD compliance, meaning banks should invest in effective data collection methods. Regulatory technology (RegTech) companies are one of the future elements aimed at enhancing the fight against money laundering [30]. RegTech focuses entirely on developing regulatory technology solutions such as KYC and data analytics in line with financial crime compliance programs. It is expected that with the increase in smuggling methods and sophisticated money laundering techniques, RegTech will help in the identification of ultimate beneficial owners and AML [30]. Therefore, RegTech will help meet financial regulators' recommendations and deal with money laundering problems effectively.

4.2. Using AI in Determining Mens Rea and Actus Reus

One of the obstacles for law enforcement officials is to define and determine

mens rea and actus reus, as doing so requires proof of the act. The following section will explore the possible ways to use AI to determine mens rea and actus reus.

The basic definition of AI indicates machines that function with limited human oversight. AI-based AML systems utilize algorithms to monitor, collect, and identify transaction patterns that are later categorized as normal or suspicious. Depending on an algorithm's accuracy, transactions flagged as laundering become more common. This increase in identified laundering activities can, in turn, give rise to apprehension of fraudulent financial activity. However, AI lacks a legal personality because it does not behave in the same way as humans, which creates a legal conundrum for criminal law professionals [31]. Nonetheless, human acts apprehended using AI techniques have a legal ground for trial and punishment.

In many countries, mens rea and actus reus must exist for someone to be held liable for criminal activities. Actus reus indicates the guilty act or the external elements of an unlawful act, whereas mens rea indicates mental elements [32]. For instance, actus reus is the action of laundering money, while mens rea is the intent to launder money. Therefore, actus reus is the prohibited action, and mens rea is the mental element that involves intention, recklessness, or knowledge of an individual committing a crime. According to Isong and Schellekens [32], actus reus is the prescribed universal feature in criminal offenses, and it has three common elements: conduct, or the defendant's physical acts or omission leading to liability; the circumstances that include facts surrounding the defendant's behavior; and results.

Under criminal law, money laundering involves transferring, conversion, possession, and use of proceeds of crime. All of these acts involve the physical element or actus reus of the money laundering crime. Participation in, attempts to commit, association to commit, aiding, abetting, facilitating, and counseling in the laundering process constitute liability for a criminal offense and smurfing which is one of the methods used in the first stage of money laundering To deposit cash with the help of a large number of people [9]. Individuals working in financial institutions who identify and fail to report money laundering activities as defined by law and, also have liability as per actus reus. The physical elements or actus reus are identifiable using AI because it tracks the sources and networks money launderers follow. [10]. As a result, the Vienna Convention dictates that knowledge, intent, or purpose, required as an element of the offense, may be inferred from objective, factual circumstances. This indicates that criminal liability is proven if it is proven that the perpetrator had the knowledge to commit this crime [9]. Consequently, an individual can be punished for money laundering if he knew or ought to have known that the funds were proceeds of illegal activity or willful blindness. Furthermore, [33] It is noted that the prosecutions related to money laundering are based on factual evidence, as it proves that the evidence obtained is criminal evidence of criminal origin ,Therefore, a person or transac-

tions identified as suspicious using AI are prosecuted based on how the defendant received or handled the property.

4.3. Using AI in Customer Due Diligence and Knowing Your Customer

Data management is critical in the banking sector because it helps facilitate the delivery of financial services. AI is identified as a potential technology essential in managing data while boosting the speed, efficiency, and accuracy of services [4]. Understanding customers' habits, such as frequency of transactions, amounts transacted, and network use, can help create effective algorithms to detect and prevent fraudulent activities. As shown, money laundering has negative social and economic effects in society, which is why banks should be vigilant in dealing with this criminal act. Technology such as AI, crucial in client management, can help curb laundering through proper identification of customers.

4.4. Using AI in Customer Due Diligence

The first line of defense in identifying and preventing money laundering involves knowing and understanding the client. CDD, as it is commonly called, indicates that banks and financial institutions should do their part in obtaining satisfactory evidence and records that ascertain the identity and legal existence of a person applying to do business [34]. The bank officials registering a client must ensure that a person's claims are substantiated by valid and reliable documents. CDD ensures that banks fully know the person on whose behalf they conduct transactions or hold funds/assets because it can help identify any potential risks they may pose. Therefore, some of the proof needed for verification includes official documentation such as passports or identity cards, birth certificates, proof of name and address, or other credentials required by the financial institution [35]. CDD also enables the financial institutions to understand a client's nature of business and sources of wealth or funds. This facilitates easier monitoring of client accounts, such as changes in transaction networks, frequency, and amounts that would help flag risky activities.

These details are mainly useful in a traditional banking setup in which clients visit financial institutions physically. However, the introduction of electronic payment services and anonymous and irreversible transaction systems creates a CDD challenge, making it difficult to detect money laundering activities. For instance, criminals use cryptocurrencies to launder money because it conceals individuals' true identities, and they can easily avoid arrest [34]. Crypto transactions do not require a person to provide proof of source income, personally identifiable information, or income declaration. As a result, criminals conducting illegal financial acts might evade law enforcement via cryptocurrency. Consequently, more comprehensive AML approaches are needed to detect money laundering activities.

FATF created new guidance that deals with virtual currencies to reduce mon-

ey laundering and financing of terrorism activities. FATF recommends that banks conduct CDD when clients establish a new business relationship or when a customer transacts more than the designated threshold [34]. Renewing CDD when a customer changes operations helps banks update clients' profiles to monitor risky habits. FATF recommends certain parameters that should be looked into when conducting any transaction. These features include the legal transaction limit, transaction frequency, numbers and amounts of transactions, customer movements and destinations, and types of currency exchanges [36]. As a result, an AI system programmed to raise red flags once such parameters are exceeded can help a bank maintain CDD. An AI program provides regular reports indicating risk rating, location, direction of transactions (in or out), and percent transaction by type [37]. Therefore, artificial intelligence methods, such as machine learning, are used to enhance CDD.

4.5. Using AI in Knowing Your Customer

Financial institutions collect data from potential clients with the intention of boosting service delivery. Banks also use provided customer data to determine loan risks, money laundering activities, and other fraudulent activities [38]. In the case of money laundering, institutions are required to work with authorities to provide information that might work as evidence in court proceedings. Therefore, customer-focused data is critical in the banking sector, especially with the growth in online banking and fraudulent activities. AI technology is implemented in banks to help with customer identification, verification, and authorization [4]. This process of verifying clients, KYC, works in the same manner as CDD by allowing the banks to learn more about the people they work with.

Money laundering is a global problem, especially in the technological era when people easily move funds from one country to another. KYC regulations are designed to help financial institutions monitor and combat money laundering. The main challenge of this approach is identifying what data are needed to help AML assess risk effectively. Banks are mandated to collect data from local and international clients, non-profit organizations, corporations, or government institutions because such details are crucial during financial audits. However, with millions of transactions every day, it becomes difficult for banks to monitor such a large volume of data and identify all false positives/red flags regarding suspicious transfers. The best approach to regularly monitor all data is through autonomous AI systems that navigate millions of data points, analyze suspicious transactions, and note the trends and patterns of such transactions that might indicate malicious behavior [4].

The growth of online banking has introduced external threats, such as hacking, identity theft, and phishing, that compromise the integrity of user accounts. Stolen client credentials can be used to log into accounts and commit crimes such as money laundering or illegal transactions without customers' knowledge. Therefore, financial corporations must comply with all KYC rules and authenti-

cation approaches to ensure users control their accounts. Providing additional internet security would also facilitate AML and easier tracking of illicit transactions. Mondal [39] propose a KYC verification approach that uses a challenge question (CQ) during user login as a way of bolstering the verification process. This method is an example of AI that utilizes historical data collected from a client to track users' login activities and compare them with new login attempts. The parameters analyzed in the (CQ) technique include failed login attempts, new users, clients with no or few identity details, or changes in the nature of transactions [39]. Risk factors are calculated using the defined parameters, and users can be logged out if they raise one or more red flags.

4.6. Using AI in Knowing the Beneficial Owners

As noted earlier, money laundering networks can be simple or complex, and they span across multiple countries. As criminals move money from one country to another, laundered funds eventually find their way back to the economy by mixing with legitimate businesses and corporations. Money launderers hide illicit money from authorities using series of structured transactions that end up in bank or offshore accounts whose beneficial owners are not clearly known [40]. For example, a legitimate business can have a network with millions of entities in multiple countries and jurisdictions. Therefore, it is challenging to trace the beneficial owner of laundered money as it is hidden beneath layers of data records. Retrieving the records can also take a lot of time because of the differences in jurisdictions and regulations. Additionally, corporations and trusts can name shareholders and boards of directors without disclosing beneficial owners [40]. It may take weeks to months to determine the ultimate beneficial owner of laundered money, which slows down legal proceedings.

Increased terrorist financing and money laundering has caused international bodies to create standards to ease AML procedures. For instance, Canada followed the EU in creating the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to make beneficial ownership more transparent [40]. A beneficial owner is a natural person who controls or owns about 25% of a corporation. An organization, including the executives found in violation of keeping verifiable documentation about beneficial owners, becomes liable for failing to comply. However, these data are often unstructured data or handwritten notes that show the beneficial owners. Therefore, there is a need for technology to improve the processes of checking through numerous data records to identify beneficial owners.

AI is used to simplify the beneficial owner search and discovery process. Money laundering agents and employees can handle multiple laundering and legitimate transactions for similar clients. Therefore, it is possible to identify the tacit link that factors in a relationship where debtors, launderers, and creditors share the same beneficial owner using AI social network metric analyses. Such a system was implemented by Colladon and Remondi [41], who identified 90

connected nodes from a sample test by using centrality measures such as in-degree and closeness. The authors analyzed the communication between different stakeholders and transaction networks, which helped determine the centrality scores between different nodes that share the same beneficial owner. It is also easier to identify the people involved in money laundering or other financial crimes by following social network analyses the goal is not to focus only on the individual attributes but focusing more on their network relationship.

People manage to commit financial crimes undetected because of corporations' secrecy and ability to hide criminals' identities. Many countries have mandated that trusts and corporations digitize their registers to help in the fight against money laundering. Beneficial owners are required to be registered, and they must be publicly accessible with the right technology [42]. However, most of these records are not digitized or exist as unstructured data sets that are difficult to read when attempting to trace a beneficial owner. Therefore, AI technology, particularly optical character recognition (OCR) and machine learning approaches, help review the unstructured data records and achieve automation [43]. OCR reads shareholder documents provided as PDF files and converts them into machine-readable texts, analyzed using a machine learning engine. This process results in digitized and searchable structured data records consisting of shareholders and beneficial owners if provided in shareholder filings.

4.7. Using AI Monitoring in Preventive Measures

The risks associated with money transfers are high, making it prudent for banks to be aggressive in identifying, analyzing, and preventing risks. Banks found in violation of certain policies receive hefty penalties, [38]. Therefore, many banks, local and international, have implemented various security and account monitoring techniques aimed at protecting against terrorist financing, financial fraud, and money laundering. Risk detection methods used by banks include CDD and KYC principles that involve obtaining customers' personal details. The quality of data received, the volume and speed of daily transactions, and varying money laundering patterns might make it difficult for conventional methods to effectively combat financial fraud.

Technology, specifically AI, is preferred because of its ability to handle large volumes of data analysis at faster speeds and with more accuracy. AI technology functions on the principle of differentiating between normal and abnormal transactions, which helps in the easy identification of risky behaviors and patterns. Complex algorithms and big data analytics are essential in classifying customers, identifying suspicious transactions, and improving the quality of risk analysis [38]. SVM support vector machine is an example of the AI and machine learning techniques used to prevent financial risks. The SVM algorithm is a type of supervised machine-learning algorithm. Unlike traditional machine learning, which seeks to reduce empirical risks, SVM seeks to reduce structural risks. It is used to solve classification problems and minimizes the risk of data errors [38].

Certain parameters are defined to help analyze consumer data that determine credit risk, transaction risks, behavioral risk, and location risk. Historical records are used to train data sets, which are then evaluated using simulation to test the viability of the SVM technique. Once fully tested, SVM is used to monitor and identify suspicious financial transactions. An effective algorithm can understand the money laundering patterns, and decision trees help with visualization. Therefore, AI prevents money laundering by halting the transactions or blocking users from violating the set parameters.

CDD and KYC, which emphasize customer recognition, are AML preventive techniques based on AI technology. The data collected by financial institutions is stored in a collective database system, which is then harnessed, cleaned, and consolidated to create searchable information [39]. AI and machine learning approaches enhance master data management that helps eliminate conflicting records. For instance, AI helps implement a probabilistic methodology that allows banks to integrate information from a single customer, thus enhancing CDD/KYC. The consolidated data can also be modeled using pattern-based and rule-based approaches to flagging transactions that signal money laundering activity.

This paper aims to look at a cutting-edge anti-money laundering (AML) solution that offers data quality assurance, high detection accuracy, scalability, and quick performance in suspicious transaction detection. According to the findings, current methods, and algorithms in this chapter, it is essential to pay attention to data quality assurance. As it, known raw data obtained from financial institutions often results in massive volumes. Financial operations can change over time. It's essential to think about the need for ongoing reinforcement learning.

5. Conclusion and Recommendations

5.1. Conclusion

This paper has explored the use of AI in financial systems, specifically in anti-money-laundering programs. This research indicates how AI is used alongside techniques such as machine learning, and data analytics strategies to monitor and identify potential market manipulation. Some of the AI techniques that deal with money laundering include fuzzy rules, fuzzy logic, and SVM. All these systems contain pre-determined parameters created by humans. The efficiency of AML relies on data quality collected through KYC and CDD approaches, which are also used in training AML programs. AML systems identify patterns such as the frequency of banking transactions, locations from which transactions occurred, and types of transactions that help determine the risk level of such transfers. AML systems mainly classify transactions as either normal or suspicious based on parameters created when training transaction data records. A suspicious transaction raises a red flag or alert that is attended to by a human who confirms, blocks, or rejects the transfer request. In various countries, bank-

ers must take an extra step and report suspicious transactions to FIUs, which help with prosecution or criminal investigations. Various regulatory bodies and rules have been created to enhance AI's use in money laundering compliance.

5.2. Recommendations

1) The need to regulate further and lay down policies that control and define the uses of technologies and create a pioneering and advanced environment for the use of AI based of the report from world Government Summit in cooperation with Deloitte The report asks the extent to which ethical or legislative norms can govern these technologies, to ensure that artificial intelligence systems serve the public good rather than certain individuals.

2) AI can be used in financial systems to develop solutions to overcome the future risks faced by clients, or institutions, or products; to track money laundering operations; and to evaluate customers in terms of creditworthiness.

3) Governments must develop and update the regulatory environment in line with the development of AI that causes rapid, radical changes, including managing the risks of AI appropriately within the government to reach a sector that promotes AI. It is further important to develop policies to organize artificial intelligence in smart way and ensure that it benefits society and the economy.

4) International governments who are interested in developing the infrastructure of their financial system should ensure that they educate a generation in matters of modern technology advancement, and focusing to prioritize and pay attention on people who requires to enhance their expertise and skills that are necessary to combat corruption in its various forms.

Acknowledgment

I would like to thank all the faculty members at Case Western Reserve University, led by Dr. Richard Gordon, the godfather of the Financial Integrity Program, for allowing us to study this unique curriculum. Without Dr. Gordon's constant help and guidance, we would not be able to succeed. Dr. Alek El-Kamhawy is the Director and leading supporter for all of us in this program, and I would also like to thank the faculty members at Naif Arab University, particularly the President of the University, His Excellency Dr. Abdul Majed Al-Banyan, who received us with a sincere welcome and continuous guidance. I would further like to thank the directors of the program, Dr. Majed Al-Otaibi and Dr. Abdullah Bouhimed. Dr. Faleh Al-Qahtani, thank you for all that you have done for us, and, of course, Miss Khadija, thank you for teaching us how to make all of this happen. I would also like to thank all of my family members for supporting me during this period, for their endurance and patience and their unlimited assistance. Last but not least, I want to thank the person who worked on guiding, advising, and teaching me. If it were not for his interest in me, I would not have reached this level. Dr. Rashid Alhajeri, thank you for all the support you have provided and the time you gave me.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Financial Action Task Force (2019) FATF-GAFI. https://www.fatf-gafi.org/publications/?hf=10&b=0&s=desc(fatf_releasedate)

[2] Huang, M.H. and Rust, R.T. (2018) Artificial Intelligence in Service. *Journal of Service Research*, **21**, 155-172. https://doi.org/10.1177/1094670517752459

[3] Allam, Z. and Dhunny, Z.A. (2019) On Big Data, Artificial Intelligence and Smart Cities. *Cities*, **89**, 80-91. https://doi.org/10.1016/j.cities.2019.01.032

[4] Kaya, O. (2019) Artificial Intelligence in Banking. Artificial Intelligence. http://dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000495172/Artificial_intelligence_in_banking%3A_A_lever_for_pr.pdf

[5] Yantis, B., Attia, M. and Lethouris, G. (2018) Money Laundering. *American Criminal Law Review*, **55**, 1469.

[6] Jensen, D. (1997) Prospective Assessment of AI Technologies for Fraud Detection: A Case Study. AAAI Workshop on AI Approaches to Fraud Detection and Risk Management, 34-38.

[7] Gao, Z. and Ye, M. (2007) A Framework for Data Mining-Based Anti-Money Laundering Research. *Journal of Money Laundering Control*, **10**, 170-179. https://doi.org/10.1108/13685200710746875

[8] Moustafa, T.H., Abd El-Megied, M.Z., Sobh, T.S. and Shafea, K.M. (2015) Anti Money Laundering Using a Two-Phase System. *Journal of Money Laundering Control*, **18**, 304-329. https://doi.org/10.1108/JMLC-05-2014-0015

[9] Hanafi, A. (2010) The Dynamic Aspects of Criminal Act and Criminal Liability in Money Laundering Practices. *Jurnal Hukum Ius Quia Iustum*, **17**, 633-650. https://doi.org/10.20885/iustum.vol17.iss4.art7

[10] Hendriyetty, N. and Grewal, B.S. (2017) Macroeconomics of Money Laundering: Effects and Measurements. *Journal of Financial Crime*, **24**, 65-81. https://doi.org/10.1108/JFC-01-2016-0004

[11] Teichmann, F.M. and Falker, M.C. (2020) Money Laundering through Consulting Companies. *Journal of Financial Regulation and Compliance*, **28**, 485-500. https://doi.org/10.1108/JFRC-07-2019-0091

[12] Karim, A.S., Mohamed, N., Ahmad, M.A.N. and Prabowo, H.Y. (2019) Money Laundering in Indonesia Bankers: Compliance, Practice, and Impact. *ICFF* 2019: *Proceedings of the* 1*st International Conference on Financial Forensics and Fraud*, Bali, 13-14 August 2019, p. 13. https://doi.org/10.4108/eai.13-8-2019.2294249

[13] Soroka, M. and Kugai, K. (2020) Money Laundering Consequences for the National Economy. Вітчизняна наука на зламі епох: Проблеми та перспективи розвитку. Університет Григорія Сковороди в Переяславі. https://er.knutd.edu.ua/bitstream/123456789/15973/1/Kugai_Soroka_Money_laundering_consequences_for_the_national_economy.pdf

[14] Hetemi, A., Merovci, S. and Gulhan, O. (2018) Consequences of Money Laundering on Economic Growth—The Case of Kosovo and Its Trade Partners. *Acta Universitatis Danubius*, **14**, 113-125. https://core.ac.uk/download/pdf/229459748.pdf

[15] Savona, E.U. and Riccardi, M. (2017) Assessing the Risk of Money Laundering in Europe. Final Report of Project IARM. https://dspace.library.uu.nl/bitstream/handle/1874/373562/ProjectIARM_FinalReport.pdf?sequence=1

[16] Oluwadayisi, A.O. and Mimiko, M.O. (2016) Effects of Money Laundering on the Economy of Nigeria. *Beijing Law Review*, **7**, 158-169. https://doi.org/10.4236/blr.2016.72017

[17] Brynjolfsson, E. and Mcafee, A. (2017) The Business of Artificial Intelligence. *Harvard Business Review*, **7**, 3-11. https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf

[18] Moor, J. (2006) The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. https://www.researchgate.net/publication/220605256_The_Dartmouth_College_Artificial_Intelligence_Conference_The_Next_Fifty_Years

[19] Strelkova, P. (2017) Three Types of Artificial Intelligence. http://eztuir.ztu.edu.ua/bitstream/handle/123456789/6479/142.pdf?sequence=1&i

[20] Joshi, P. (2017) Artificial Intelligence with Python. Packt Publishing, Birmingham.

[21] Chen, Z., Teoh, E.N., Nazir, A., Karuppiah, E.K. and Lam, K.S. (2018) Machine Learning Techniques for Anti-Money Laundering (AML) Solutions in Suspicious Transaction Detection: A Review. *Knowledge and Information Systems*, **57**, 245-285. https://doi.org/10.1007/s10115-017-1144-z

[22] Bellomarini, L., Laurenza, E. and Sallinger, E. (2020) Rule-Based Anti-Money Laundering in Financial Intelligence Units: Experience and Vision. https://ceur-ws.org/Vol-2644/paper40.pdf

[23] Jamshidi, M.B., Gorjiankhanzad, M., Lalbakhsh, A. and Roshani, S. (2019) A Novel Multiobjective Approach for Detecting Money Laundering with a Neuro-Fuzzy Technique. 2019 *IEEE* 16*th International Conference on Networking*, *Sensing and Control* (*ICNSC*), Banff, 9-11 May 2019, 454-458. https://doi.org/10.1109/ICNSC.2019.8743234

[24] Garcia-Bedoya, O., Granados, O. and Burgos, J.C. (2020) AI against Money Laundering Networks: The Colombian Case. *Journal of Money Laundering Control*, **24**, 49-62. https://doi.org/10.1108/JMLC-04-2020-0033

[25] Han, J., Huang, Y., Liu, S. and Towey, K. (2020) Artificial Intelligence for Anti-Money Laundering: A Review and Extension. *Digital Finance*, **2**, 211-239. https://doi.org/10.1007/s42521-020-00023-1

[26] Salehi, A., Ghazanfari, M. and Fathian, M. (2017) Data Mining Techniques for Anti Money Laundering. *International Journal of Applied Engineering Research*, **12**, 10084-10094. http://www.ripublication.com/ijaer17/ijaerv12n20_120.pdf

[27] Brundage, M., Avin, S. and Clark, J. (2018) The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

[28] Bertrand, A., Maxwell, W. and Vamparys, X. (2020) Are AI-Based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights? *ICML* 2020 *Law and Machine Learning Workshop*, Vienne, July 2020.

[29] Truby, J., Brown, R. and Dahdal, A. (2020) Banking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector. *Law and Financial Markets Review*, **14**, 110-120. https://doi.org/10.1080/17521440.2020.1760454

[30] Kurum, E. (2020) RegTech Solutions and AML Compliance: What Future for Financial Crime? *Journal of Financial Crime*, **30**, 776-794. https://doi.org/10.1108/JFC-04-2020-0051

[31] Claussén Karlsson, M. (2017) Artificial Intelligence and the External Element of the Crime. https://www.diva-portal.org/smash/get/diva2:1115160/FULLTEXT01.pdf

[32] Isong, R.O. and Schellekens, M. (2019) Robots and Criminal Culpability in the United Kingdom. http://arno.uvt.nl/show.cgi?fid=147344

[33] Bell, R.E. (2000) Proving the Criminal Origin of Property in Money-Laundering Prosecutions. *Journal of Money Laundering Control*, **4**, 12-25. https://doi.org/10.1108/eb027258

[34] Johari, R.J., Zul, N.B., Talib, N. and Hussin, S.A.H.S. (2020) Money Laundering: Customer Due Diligence in the Era of Cryptocurrencies. 1*st International Conference on Accounting, Management and Entrepreneurship* (*ICAMER* 2019), Cirebon, 26 September 2019, 130-135. https://doi.org/10.2991/aebmr.k.200305.033

[35] ElYacoubi, D. (2020) Challenges in Customer Due Diligence for Banks in the UAE. *Journal of Money Laundering Control*, **23**, 527-539. https://doi.org/10.1108/JMLC-08-2019-0065

[36] Suntura, J.H.C. (2019) Customer Identification in Currency Exchange Companies as Per FATF Recommendations. *Journal of Money Laundering Control*, **23**, 96-102.

[37] Zhang, Y. and Trubey, P. (2019) Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *Computational Economics*, **54**, 1043-1063. https://link.springer.com/article/10.1007/s10614-018-9864-z https://doi.org/10.1007/s10614-018-9864-z

[38] Chen, T.H. (2020) Do You Know Your Customer? Bank Risk Assessment Based on Machine Learning. *Applied Soft Computing*, **86**, Article ID: 105779. https://doi.org/10.1016/j.asoc.2019.105779

[39] Mondal, P.C., Deb, R. and Huda, M.N. (2016) Know Your Customer (KYC) Based Authentication Method for Financial Services through the Internet. 2016 19*th International Conference on Computer and Information Technology* (*ICCIT*), Dhaka, 18-20 December 2016, 535-540. https://doi.org/10.1109/ICCITECHN.2016.7860255

[40] Meunier, D. (2018) Hidden Beneficial Ownership and Control: Canada as a Pawn in the Global Game of Money Laundering. CD Howe Institute. https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Final%20for%20advance%20release%20Commentary_519_0.pdf

[41] Colladon, A.F. and Remondi, E. (2017) Using Social Network Analysis to Prevent Money Laundering. *Expert Systems with Applications*, **67**, 49-58.

[42] Knobel, A. (2017) Technology and Online Beneficial Ownership Registries: Easier to Create Companies and Better at Preventing Financial Crimes. https://www.taxjustice.net/wp-content/uploads/2017/06/Technology-and-online-beneficial-ownership-registries-June-1-1.pdf

[43] Whiting, J. (2020) Leveraging Artificial Intelligence to Revolutionise Ultimate Beneficial Ownership Discovery. The AI Journal. https://aijourn.com/leveraging-artificial-intelligence-to-revolutionise-ultimate-beneficial-ownership-discovery/