ANTI-MONEY LAUNDERING PRACTICES IN THE SCOPE OF RISK MITIGATION AND COMPARISON WITH ANTI-MONEY LAUNDERING REGULATIONS

Atty. Nejat Utku Inaltong LL.M. & MBL

DEDICATION

I would be honoured to dedicate this paper to my parents, Semra and Ceyhan Inaltong. Their immense support gave me the values and education necessary to conduct and finalise this paper.

Thank you for passing me the torch of knowledge and the sense of justice

TABLE OF CONTENTS

1. INTRODUCTION…….

2. ANTI-MONEY LAUNDERING PRACTICES AND RED FLAGS ……...

3. CUSTOMER DUE DILIGENCE AND EFFECTIVE ANTI-MONEY LAUNDERING PRACTICES

4. INTERNATIONAL AND EUROPEAN AML REGULATIONS……

5. FUTURE CHALLENGES IN AML DUE TO NEW TECHNOLOGICAL DEVELOPMENTS AND TRENDS

6. CONCLUDING REMARKS…….

ABBREVIATION	MEANING
AML	Anti Money Laundering
AMLD	Anti-Money Laundering Directive
CDD	Customer Due Diligence
CID	Customer Identification
CIP	Customer Identification Program
Directive	Anti-Money Laundering Directive
EBA	European Bank Authority
ECB	European Central Bank
EU	European Union
FATF	The Financial Action Task Force (FATF)
FI	Financial Institution
FinCEN	The Financial Crimes Enforcement Network
FCC	Financial Crime Compliance
Member State	Member state of the European Union
NFT	Non-Fungible Tokens
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
SAS	Suspicious Activities
SAR	Suspicious Activity Report

1. INTRODUCTION

In the age of digitalisation, online financial services have become a vital part of overall transactions in the world, facilitating a better, faster and more efficient way to transfer money securely and substantially. Nevertheless, it has also brought various difficulties regarding monitoring and screening online transaction assets and establishing risk management practices. Therefore, promoting the gravity of instituting anti-money laundering practices in European and Global contexts could be answered best in the scope of cyber & information security, data privacy, digital banking and especially compliance law. Although most of the measures are limited in the jurisdiction of the respective countries, it is vital to understand the possible effects of money laundering and terrorist financing that might disturb the integrity and transparency of financial markets globally. It is challenging to assess the scale of money laundering around the globe. However, according to UNODC's database[1], the money laundering scheme can be roughly estimated at $2 trillion, representing 2-5% of the world's total GDP. Therefore, understanding the measures for combating money laundering from the two most influential judicatures(the EU and International law) is essential to raising awareness to detect and prevent transactions with a criminal background. This paper will focus on AML practices in the scope of compliance law. After covering the essence of AML regulations and practices, it will be followed by reviewing landmark judicial precedents and accepted doctrines around the globe to establish a more profound understanding of how to prevent these illegal activities. Subsequently, this paper will argue about specific case laws to extend the knowledge of the legal existence of fair use to avoid misinterpretation. This paper will be finalised with the author's concluding remarks.

2. ANTI-MONEY LAUNDERING PRACTICES AND RED FLAGS

Before dwelling on the details of the AML in EU law, understanding the essence of the term "Money Laundering" is inevitable. Substantially, money laundering is executing transactions to convert illegally obtained money into legal money that can appear as transfers, deposits, withdrawals and so on[2]. Money laundering has three stages:

[1] UNDOC, *Money Laundering*, https://www.unodc.org/unodc/en/money-laundering/overview.html, last access 13.04.2025

[2] ICAS, *AML Awareness: Three stages of money laundering,*[January 2019], available at: https://www.icas.com/professional-resources/anti-money-laundering-resources/latest-developments/aml-awareness-three-stages-of-money-laundering, last access 13.04.2025

1. **Placement**: Introducing illegally obtained money into the financial system through cash businesses, false invoicing, smurfing, trusts & offshore companies, foreign bank accounts, and aborted transactions.
2. **Layering**: The continuous use of placement and extraction to move around the illicit funds to disguise their origins.
3. **Integration/Extractions**: The aforementioned "clean" investments or methods allow illegal funds to be withdrawn and reused in a standard economy without attracting attention from the tax authorities or law enforcement.

In brief, money laundering aims to introduce illicit funds to the global financial markets and integrate them to make them look legitimate without suspicion.

At first glance, money laundering might seem like a variation of the deception to secure unfair or unlawful gain, simply a type of “fraud”; however, it is just the tip of the iceberg. The crime organisations use their illicit funds to invest in arms sales, narcotics, human trafficking, contraband smuggling, embezzlement, insider trading, bribery, and fraud schemes that truly disturb not only the financial institutions but also world peace in a drastic way[3]. Therefore, detecting possible money laundering practices and taking measures is diligence work since the new technologies and the rise of e-money and property on a global scale can be exploited by criminal organisations to cover their schemes. Therefore, it is not always feasible to prevent money laundering activities but mitigate money laundering risks through Efficient AML Solutions. The success of efficient AML practices can be simply summarised by not getting fined by AML/CFT authorities or managing to prevent illegal funds from entering the legitimate financial system, but having only the threshold requirements would not be competent in today’s tech-driven world, especially since AML compliance is a fundamental requirement[4]. Indeed, the bigger picture is that through numerous crimes such as tax evasion, theft, dampening corruption, and fraud, money laundering practices cause collective and societal harm when these funds could have been spent on more productive things, such as public welfare. Therefore, AML is not just a

[3]Comply Advantage, *What are the 3 Stages of Money Laundering?*, https://complyadvantage.com/insights/3-stages-money-laundering/, last access: 13.04.2025
[4] Trulioo, *AML compliance checklist: best practices for Anti-Money Laundering,* https://www.trulioo.com/blog/aml-compliance , last access: 13.04.2025

procedure to avoid fines or a common regulation to implement in financial institutions; it is also a critical component of a functioning and fair society.

Primarily, we have to understand that each jurisdiction can have its sui generis AML requirements, which can be divided into two significant jurisprudence: EU and international law. However, their intersection points can be concisely explained with protective practices through written policies to understand their intersection points. Since the implementation of the AML regulations cannot be monocentric, it is fundamental to have guidelines and written (internal) policies to inform all employees, from executives to regulators, making it easier to detect AML red flags. At its core, money laundering activities fundamentally legitimise illegal funds, indicating that the source of funds might not come from legal means. One of the most common unusual activities and AML reflags are:

1. In large cash transactions, their source of funds is not traceable
2. Numerous transactions could be a sign of transaction stacking; one specific example would be the division of deposits to make them fall below reporting requirements.
3. Spikes in activity or amounts in balance
4. Transactions involving cash-intensive industries, like gaming, or with nations with a track record of money laundering, such as high-risk nations
5. Transactions involving people or companies that could launder money, including PEPs or current legal sanctions

After detecting the red flags, a SAR(Suspicious Activity Report) should be filed if the criminal activity has reasonable grounds for suspicion by conducting event-triggered due diligence checks and then filing with the local Financial Intelligence Unit. SARs are highly confidential — the individual who discovered the activity isn't required to disclose their name or contact information, and the filer is prohibited from disclosing information that could reveal the report's existence.

3. CUSTOMER DUE DILIGENCE AND EFFECTIVE ANTI-MONEY LAUNDERING PRACTICES

Crime organisations change their methods for placement, layering, and integration activities to emerge smelling roses. Therefore, it is fundamental for financial institutions or compliance service providers to keep their guidelines and methods up to date through four main pillars: ID verification, AML screening, AML monitoring, and periodic risk assessment with the help of AI and machine learning.

Red flags related to money laundering might be found during the first due diligence phase or through continuing monitoring protocols. During these onboarding processes, a benchmark for normal activities should become apparent (*the steps a business must take to verify a customer's true identity and risk level*). Therefore, mitigating the risk of detecting and managing problematic accounts or transactions before they become a risk is fundamental to combating money laundering.

3.1 ID Verification and CIP

ID verification processes are one of the first stepping stones for CDD. Financial institutions have invested in the latest technology to create effective KYC policies and internal guidelines to alleviate risk assessment. Traditional methods to verify CID exist, such as Knowledge-Based Authentication (KBA) or two-factor authentication. However, cybercriminals find ways to breach the systems and commit identity fraud crimes, which makes the aforementioned methods that were once effective in providing the necessary security measures remain insufficient in authenticating or verifying whether the user logging in is the actual owner of the account[5]. In this vulnerable financial ecosystem, pinpointing fraudulent activities through effective and accurate digital ID verification methods becomes even more pivotal. Consequently, groundbreaking and innovative technological development is submerged to combat identity fraud with cutting-edge AI-based digital ID verification, a more straightforward, secure, and cost-effective process than more conventional ones, such as machine learning technologies. These technologies include facial and voice liveness detection, behavioural analysis(*Analyzing behavioural data, such as*

[5] Fineksus, *Customer Due Diligence Checklist — 4 Steps to Improve Your CDD*, https://fineksus.com/customer-due-diligence-checklist-4-steps-to-improve-your-cdd/, last access 13.04.2025

website visits, newsletter subscriptions, and cart additions), and age and gender analysis, among the most effective digital ID verification methods powered by AI and machine learning technologies. It notably facilitates the digital onboarding processes since this pioneering technology alleviates the need for manual intervention to the minimum, which decreases operational workload and time spent on them tremendously[6]. Therefore, digital ID verification methods, especially in the customer onboarding process, mitigate any fraudulent concerns of digital customers regarding pace, safety, flexibility, and smoothness. Henceforth, to be able to have a secure and comforting digital environment and find different methods to verify their customers' identities would also affect efficiency and customer satisfaction benefits that will conduct an accurate and adequate digital ID verification in the meantime, ensuring the regulatory compliance with AML and KYC for transition monitoring activities.

3.2 AML Screening

One of the main goals of the AML regulations and obligations is to detect and manage problematic accounts or transactions before they become a risk, which serves two purposes; on the one hand, it is to protect the client's confidentiality while providing a secure environment for their assets by having a great digital customer experience and on the other hand, fighting against threads on business continuity and complying with the regulatory needs for the financial institutions[7]. One of the four pillars of practical AML guidelines is scanning their current and potential customers on sanctions, PEPs, banned/wanted lists, and adverse media data through AML Screening software[8]. AML screening must be carried out delicately with an exhaustive program that is required to gather data from assorted government sources, international regulators and law enforcement agencies. Additional elements that are crucial for AML screening include the global sanctions list check, which automates watchlist compliance checks and scans for known or suspected entities and individuals connected to money laundering, terrorism, financial fraud, arms proliferation, drug trafficking, or PEPs. [9]

---

[6] Ibid.
[7] Lutkevich Ben, *What is risk mitigation?*, https://www.techtarget.com/searchdisasterrecovery/definition/risk-mitigation, last access 13.04.2025
[8] Sanction Scanner, *What is AML Name Screening?*, https://sanctionscanner.com/knowledge-base/aml-name-screening-189, last access 13.04.2025
[9] Trulioo, *AML compliance checklist: best practices for Anti-Money Laundering*

Since screening searches all available information on a client or a prospective client that is feasible through diligently collected data, the KYC screening process continues throughout the customer's lifecycle. AML practices bound each other in that conducting the screening process without monitoring the status of the individual, business, the ultimate beneficial owner (UBO), the transactions they made, and even the press coverage and public reputation of the customer is impossible. In addition, over-screening would be dangerous since one of the key components of screening is knowing how to process the collected data competently when the AML process uncovers it. Therefore, an effective AML program should require a cohesive, collective, integrated and holistic approach to research clients during the KYC process with different screenings[10].

3.3 Name Screening

AML name screening is one of the main pillars or methods conducted for risk assessment of current or potential customers of organisations under the AML obligations in the operated country, namely, a KYC strategy to scan the collected data from the customers from sanctions, PEPs, banned/wanted lists, and adverse media. Identifying and verifying exactly whom the institution works with through AML software by taking a name and searching it on a name-screening database effectuates the AML procedure[11].

AML Name screening, alias sanctions and PEP screening also include the Adverse Media Screening process, which facilitates two key components that make this procedure inevitable for a successful AML program: building the risk assessment and assisting institutions in detecting and reporting suspicious activities. On the one hand, risk assessment detects high-risk customers and takes the necessary steps to monitor their financial activities through CDD & KYC. On the other hand, institutions will comply with the compliance law in the operated country to protect themselves from regulatory penalties. Executing the program requires goals, including identifying risk sources and analysing risk reduction strategies through effective AML / OFAC compliance processes. Additionally, a reliable way to evaluate AML risk is to use the primary

[10] Lucinity,*6 Best Practices for Streamlining Your KYC Compliance Process* https://lucinity.com/blog/6-best-practices-for-streamlining-your-kyc-compliance-process, last access 13.04.2025

[11] Sanction Scanner, *What is AML Name Screening?*, https://sanctionscanner.com/knowledge-base/aml-name-screening-189, last access 13.04.2025

money laundering indicators, which include the type and size of a business, the types of consumers, the products and services offered to customers, the tactics used to attract new clients and interact with current ones, and geographic risks[12]. Using reliable filtering software, which includes a variety of private lists from reputable risk and compliance data technology companies like World-Check and Dow Jones Risk and Compliance, it is possible to consistently screen public and private PEP & sanction lists, as the AML name screening process involves verifying a customer's name in a name-screening database[13].

3.4 Sanction Screening

Sanctions are restrictive measures enforced on entities or individuals by curtailing their activities and exerting pressure and influence on them. This stage of the screening process is now possible thanks to established sanctions lists, which flag individuals, companies, and nations that have committed or are suspected of committing crimes to reduce financial crime. As a result, it lowers the risk for financial institutions to do business with sanctioned entities[14]. These lists embody various regulatory and enhanced due diligence lists from major sanctioning bodies worldwide, such as the OFAC, EU, UN sanctions, and many other regulatory and law enforcement organisations like the International Criminal Court. An effective Financial Crime Compliance (FCC) program should incorporate sanction screening by integrating deep regulatory expertise, applied technology, and sophisticated analytics. This program will use screening procedures to promote two primary goals or areas: transaction and screening of customers.

Transaction screening refers to identifying transactions involving targeted individuals or entities. On the other hand, customer or name screening is designed to identify targeted individuals or entities during onboarding or the lifecycle of the customer relationship with the financial institution. Thus, transaction and customer screening are intended to execute a sturdy set of controls for identifying sanctions targets, and it should be recognised that there are various limitations in the way in which these controls are managed and should always be employed as part of a broader FCC programme to implement in the internal playbook of compliance

[12] Fineksus, *What is AML Name Screening?*, https://fineksus.com/what-is-aml-name-screening/, last access 13.04.2025
[13] Ibid
[14] Trulioo, *Sanctions and PEP screening: a critical step in the KYC process,* https://www.trulioo.com/blog/sanctions-pep-screening, last access: 13.04.2025

departments[15]. On the other hand, financial institutions should also take into consideration other financial risks to enforce their sanctions screening programme commensurate in line with its complexity, size and nature; hence, the FIs should take into consideration the following:

1. The jurisdictions where the financial institution is located and its juxtaposition geographically, culturally and historically to sanctioned countries
2. The type of customers the financial institution has, such as international or domestic, where those customers are located and what kind of business they undertake
3. The volume of transactions and distribution channels
4. What type of services and products does the financial institution propose? Do those products represent an elevated sanctions risk, such as cross-border transactions, foreign correspondent accounts, trade-related products or payable-through accounts[16]?

Principally, this phase of risk management compares data sourced from an FI's operations, such as customer and transactional records, against lists of names and other indicators of sanctioned parties or locations by matching one string of text against another to detect similarities to suggest a possible match with sanctions screening programme[17]. This program can be run effectively by integrating prevention, detection, and investigation of risk management but also in conjunction with other financial crime risk prevention and control processes as follows:

Policies and Procedures

Determining the framework for what needs to be screened in what frequency and context to set how alerts should be arbitrated and conducting a coherent process of resolving alerts, especially when the key information is unreliable or fruitless.

[15] The Wolfsberg Group, *Wolfsberg Guidance on Sanctions Screening*, https://db.wolfsberg-group.org/assets/4b6c2db6-696d-492e-bdd5-c51552708597/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf , last access 13.04.2025
[16] Ibid.
[17] Wolfsberg Guidance on Sanctions Screening, page 2

Responsible Person

Ensuring the proper abilities and expertise in understanding the nuances of sanctions requirements and determining the possible influence of screening outcomes and decisions while having the necessary technical aptitudes of screening software.

Risk Assessment

Implementing risk-based decisions to solve peculiar questions such as what type of data attributes to the screening process, when to screen, what kinds of lists to use and most importantly, how precise or "fuzzy" to set the screening filter. Moreover, the decision-making and governance structure must be as straightforward as possible to be enunciated, documented and sustained by analysis and testing[18].

Internal Controls

Various methodologies and technologies are available for implementing screening control processes; nevertheless, although these variations might differ, no unequivocally defined module, technology, or configuration is better or worse. Each has unique strengths and limitations, vital to understanding its capabilities. FIs would document how their screening systems are applied to demonstrate that the application is expected to be detected and manage the specific sanctions risks to which the FI is exposed.

Testing

The final stage of the screening process is to test the procedure to validate that the screening system is performing as initially planned and evaluate its effectiveness in managing the specific risks expressed in the FI's Risk Assessment, which metrics, analysis, and reporting should support.

[18] Ibid. p.3

3.5 PEP Screening

Under the globalisation of the law and practices, the FIs can use this harmony to their advantage by adding sanctions lists as one of their checkups when onboarding or even with their current customers throughout CDD procedures. PEP screening cannot be considered adequate without the sanctions lists, which can be enforced on the countries, regimes, groups, and individuals by many regulatory and enhanced due diligence lists published by major sanctioning bodies and international law organisations such as the US Consolidated Sanctions (US Sanction Lists), OFAC—Specially Designated Nationals (SDN), Office of the Superintendent of Financial Institutions (Canada), Bureau of Industry and Security (US).

Although there are various sanctions lists, and it might give the impression that they are focused more on a domestic law level, with the given technology and malicious acts of the criminal organisations, to establish a robust AML to detect these sanctioned entities, FIs have to look from a broader perspective by applying following practices:

1. FIs must comply with international law by regularly keeping up-to-date with sanctioned individuals, organisations, and government lists.
2. To achieve a more profound risk mitigation process, the sanctions software used to detect blocked people should be updated for the operated country and contain the countries with which the FI is affiliated or has business partnerships.
3. Observing international political sanctions to stay current on the most recent trends on the kind of people who can be sanctioned.

A PEP is defined by the FATF Guidance: Politically Exposed Persons (Rec 12 and 22) as a person who has been given a significant public position or political role that could be abused to launder illegal funds or, in addition, any other predicate offences, such as bribery or corruption[19]. In addition to imposing a higher risk profile for ML since the positions that these individuals hold can be abused to launder illicit funds, sometimes the FIs want to over-comply with their

[19] FATF, *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html, last access 13.04.2025

regulatory needs to the extent that the PEP status of an individual might never expire,e and even some countries extending the regulatory scope of PEPs to their close associates and immediate family members. Once a PEP is identified, EDD measures need to be applied:

1. Identifying PEPs(For documentation and regulatory reasons)
2. Securing senior management's approval is necessary to start or maintain these business & commercial collaborations.
3. Establish a source of funds/wealth
4. Apply ongoing EDD

The importance of having detailed and regulated EDD for PEP screening would significantly mitigate the risk of getting fined, but even more so that if the organisation fails to identify sanctions evasion, bad actors or a PEP involved in unorganised crime, it would also lead to potential reputational damage that deters potential investors from affiliating with the FI[20].

3.6 AML Monitoring

AML monitoring systems focus mainly on four factors, but these are not numerus clausus:

1. *Background checks*
2. *Criminal charges*
3. *Global Sanctions lists, AML watch lists*
4. *PEP Status*

This system is usually also made part of the ongoing CDD in which the engine(aka AML software) is set to continuously screen the entire customer base so that the organisation can be aware of any potential changes by getting triggered an alert that a possible change has occurred for one of their customers to the operator.

[20] Trulioo, *Sanctions and PEP screening: a critical step in the KYC process,* https://www.trulioo.com/blog/sanctions-pep-screening, last access 13.04.2025

AML or transaction monitoring allows FIs to monitor CU transactions daily or in real-time to compute the risk, and by combining this information with analysis of customers' historical information and account profiles, the software can provide FI with a holistic picture analysis of a customer's entire profile, risk levels, and predicted future activity. The transactions monitored can include cash deposits and withdrawals, wire transfers, and other activities; hence, the objective of AML activity and transaction monitoring is to identify suspicious customer transactions, including substantial transactions, complex transactions, and unexpected patterns of transactions that don't seem to have a legitimate purpose. For instance, a customer is suddenly elected into a high political position, involved in a financial crime, or has other adverse media reports, giving a reason for suspicion. This alarm can be a false positive, meaning the system has made an error. But if the alarm is genuinely positive and the suspicion has some legitimate grounds, an event-driven review is triggered, a means of due diligence outside the regular cycle.

If a customer is in the form of a legal entity and based on the AML risk-scoring methodology, this customer has a moderate AML risk. Subsequently, a regular CDD will be applied, and the customer's information will be reviewed for the next time in three years. However, the AML screening engine now generates an alert where an adverse media report shows that the customer has been involved in an enormous ML scandal. However, the organisation's name is not used, and the media reporting says that the CU has abused products and services for ML that are similar to those the organisation offers. This also triggers an event-driven review; therefore, it must be done immediately instead of reviewing the CU for the next time in three years. Henceforth, ML activity and transaction monitoring programs should include:

1. The transaction monitoring program should be able to recognise different forms of ML and types of transactions customers might use to conceal it; for instance, the program should alert the FI when the CU makes significant cash deposits.
2. The program should be able to monitor customers who act suspiciously during transactions or whose transactions raise suspicions of suspicious activity or specific transaction thresholds.

3. The program should be able to track a customer's transaction history, making it easier to spot and flag any unusual activity and compare customers' ongoing transaction activities to particular risky forms or patterns of transactions.
4. Ensure that the monitoring system alerts the FI representatives about unusual, large, or complex transactions or patterns of transactions.

Suppose the monitoring program identifies suspicious customer transactions or behaviour. In that case, it is essential first to apply the even-driven CDD and eventually consider making a suspicious activity or suspicious transaction report.

3.7 CDD and Checklist for Financial Institutions

In essence, CDD is a pivotal step of a strong AML program that FI, businesses or other organisations use to collect related data/information from their customer to identify and mitigate risks such as money laundering, financing terrorism, and other illicit activities[21]. Henceforth, it is one of the core components of the organisation's risk management strategy, which is regulated in most of the respected countries' jurisdiction, for instance, in the US, pursuant to the 31 CFR Chapter X of the Bank Secrecy Act(BSA), the potential fines for a pattern of negligent activity that violates the BSA differentiates from $50,000 to $1 million involving international money laundering[22].

CDD also consists of ongoing monitoring of the customer's activities to identify transactions that are above a threshold or red flags that indicate the pattern of illicit activity traces; nevertheless, since the criminals find various ways to launder the money through committing crimes that involve disguising the proceeds of illegal activities as legitimate funds, in substance, finding the correlation between CDD and Money Laundering is the key component to combat. Thereafter, CDD can be efficient for FIs to identify and report suspicious activity with a cohesive approach by detecting typical financial crimes involving financing terrorism, tax evasion, and corruption. Since CDD is an ongoing risk assessment and management process, it is essential to consider

[21] Signicat, *Customer Due Diligence (CDD) and its importance in risk management and compliance,* https://www.signicat.com/blog/customer-due-diligence-cdd-and-its-role-in-banking , last access 13.04.2025
[22] OFACS Sanctions Lawyer, *Bank Secrecy Act Compliance Lawyer*, https://ofaclawyer.net/bank-secrecy-act-compliance-lawyer/ , last access 13.04.2025

customers' circumstances and changes in their activities that can lead to their risk profile transformation; therefore, continuously monitoring and updating their CDD processes can reflect these modifications. There are three main CDD measures that FIs can use:

1. **Standard Customer or Client(Ongoing) Due Diligence**

   It refers to a more basic standard level of information collected by the customer by checking provided data through databases or solutions such as documents and biometric checks from the FIs' side. This type of CDD is common for account opening, which can be accomplished by obtaining information about the customer's business and financial history, reviewing identification documents, and reviewing public records and other sources of information. Therefore, creating a robust and gripping anti-money laundering CDD program requires the following:

- Contriving an adequate risk assessment strategy
- Empowering compliance and legal teams
- Developing powerful AML automation technologies with AI and machine learning systems
- Keeping regulatory requirements up to date in the operated country
- Performing continual reviews and audits with a potent CDD playbook and guidelines.

2. **Enhanced Customer Due Diligence**

   EDD refers to a more thorough review of a customer's activities and risk profile since these types of CUs may be required for higher-risk profiles or transactions involving large sums of money that illicit funds could have derived. In the words of one syllable, EDD is the second CDD layer, which must be regulated in every respected country's domestic AML/CFT legislation under Recommendation 10 of the FATF's 40 Recommendations. Moreover, according to Recommendation 19 of the FATF, EDD measures would be carried out on persons or situations that present a greater risk, including persons, situations that present a greater risk, including[23]:

[23] Comply Advantage, *What is Enhanced Due Diligence (EDD)?*, https://complyadvantage.com/insights/enhanced-due-diligence/ , last access 13.04.2025

1. Unusual situations, such as an inexplicable geographic distance between the company and its client—such as offshore or shell companies—lead to forming a business connection.
2. Overseas customers or the ones that are subject to economic sanctions
3. Legal arrangements or persons that are personal asset-holding vehicles that can facilitate ML scheme activities.
4. Companies that have an operational structure that has nominee shareholders or shares in bearer form
5. Cash-intensive businesses such as casinos
6. When determining the source of wealth, the company's beneficial ownership structure seems overly complicated or convoluted.
7. Countries without adequate AML/CFT systems impose a higher risk
8. Countries subject to sanctions, embargoes, or even significant corruption or criminal activity in their respective jurisdiction are under increased monitoring in FATF's list.
9. Countries that sponsor or encourage terrorism or have officially recognised terrorist groups active there.
10. Private banking activities could lead to higher-risk customer profiles since they can provide personalised services to higher net-worth customers.
11. Transactions or commercial partnerships that are anonymous or conducted virtually
12. Payments made to unidentified or unaffiliated third parties
13. Geographical risk factors: countries without sufficient AML and combating the finance of CFT regulation, non-FATF member countries or countries facing sanctions and embargoes with a reputation for extensive levels of corruption, or even countries blacklisted for financing or supporting terrorist activities

In different jurisdictions, EDD is seriously considered for risk mitigation activities as in EU law, under Article 18 of 4AMLD, businesses located in a country on the high-risk countries list require EDD. In contrast, FATF also recommends best EDD practices as follows:

1. Getting more identifying information from other sources rather than relying on a predetermined list of documents
2. Carrying out additional searches for the customer profile
3. Substantiating the source of funds involved to ensure they are not proceeds from any criminal activities or derived from illicit funding
4. Procuring additional information from the customer about the purpose and nature of business relationships with its affiliates
5. Delegating an intelligence report on the customer or beneficial owner to have stronger monitoring practices

Moreover, since this whole procedure of CDD or EDD is a living organism that keeps a constantly evolving entity, in all jurisdictions, AML trends, sanctions, and screening databases should be updated to ensure customers are not on the watchlist or any PEPs[24].

4. INTERNATIONAL AND EUROPEAN AML REGULATIONS

Enforcing Global AML and CFT compliance is a complex challenge since it can vary notably by jurisdiction, risk environment assessment, and fintech innovations development daily [25]. Henceforth, to comply with these regulatory necessities, businesses should adopt a holistic understanding as their regulatory instruments to mitigate the risk, which means imposing both at a national and international level[26].

4.1 The Financial Action Task Force (FATF)

FATF is an intergovernmental organisation with 39 member states that set international standards to prevent international money laundering and terrorism financing and to ameliorate global compliance standards. Furthermore, the FATF has created and advanced a set of AML/CFT recommendations to accomplish those objectives, which its member-states must implement with

[24] Comply Advantage, *What is Enhanced Due Diligence (EDD)?,* https://complyadvantage.com/insights/enhanced-due-diligence/ last access 13.04.2025
[25] Ripjar, *Anti-Money Laundering Regulations Around the World*, https://ripjar.com/blog/aml-anti-money-laundering-regulations/, last access 13.04.2025
[26] Comply Advantage, *Global AML Regulations: What You Need To Know*, https://complyadvantage.com/insights/aml-regulations/, last access 13.04.2025

their domestic legislation. Its primary function is to set globally integrated standards for AML compliance and monitor their effective implementation. In today's fast-paced, tech-driven world, criminal trends, regulations, and fintech innovations emerge rapidly; the FATF adjusts its AML/CFT recommendations to reflect the global risk environment and pursues its objectives by keeping its guidelines updated with the upcoming trends.

The FATF Compliance Policy-making Body established 40 FATF Recommendations to guarantee a coordinated global response to prevent terrorism, corruption, and organised crime. The body aims to generate the political will necessary for member states to implement the following basic AML measures and controls and national legislative and regulatory reforms to implement the fundamental AML measures and controls.:

- Every government must treat money laundering as a criminal offence, and a national financial intelligence unit must handle money laundering reports.
- Domestic businesses should take a risk-based approach to money laundering. They should perform holistic risk assessments on their customers and deploy proportionate compliance responses to mitigate the risk.
- Businesses should use Know-Your-Customer (KYC) procedures, such as customer due diligence (CDD), to create accurate customer risk profiles.
- Businesses should implement ongoing screening and monitoring activities for their customers to detect suspicious activity and capture changes in risk profiles.
- Relevant risk indicators, such as sanctions lists, politically exposed person (PEP) lists, and adverse news reports, must be checked against high-risk clients.
- Financial entities/authorities should assist international counterparts in cross-border criminal investigations to receive more effective solutions.
- Implement Know Your Customer (KYC) ID verification measures.
- Maintain suitable records of high-risk clients and apply due diligence measures regularly.
- Keeping KYC monitoring the accounts for suspicious financial activity regularly and reporting suspicious activity to the relevant national authority.
- Enforcing robust sanctions against PEP and obliging entities that fail to comply with FATF regulations.

4.2 EU Law

Member States often issue their own AML laws based closely on FATF guidance or apply changes pursuant to the recommendations. Moreover, due to the unique mechanism of the EU directives, they require "harmonisation" of the EU law, which essentially stands as the standardisation or approximation to the determination of EU-wide legally binding standards/protocols/codes to be met in all Member States. Therefore, in EU law, AML rules are determined and issued by the EU Parliament as the AML, and each Member State has to implement the latest directive in its legal system.

The EU issued its first AML directive in 1991. Since then, the directives have been published periodically, including updates that follow changes in money laundering practices and techniques internationally and are often made in line with updated FATF guidelines. These updates are reflected in newly issued directives, which usually contribute to or update previous directives as the EU parliament publishes these new directives with implementation deadlines for Member States to harmonise their national law in line with EU law[27].

With the implementation of the most recent sixth directive, also called 6AMLD, in June 2021, there have been five more directive difficulties to date. Institutions should implement the following requirements to adhere to the most recent 5-6 AMLD rules:

- **5AMLD:** The Fifth Anti-Money Laundering Directive emphasises the importance of cryptocurrency regulation, radically introducing a legal definition of cryptocurrency, reporting obligations, and rules for crypto wallets. 5MLD also introduces new legal requirements for prepaid cards, transactions involving high-value goods, beneficial ownership, customers from high-risk third countries, and Politically Exposed Persons (PEP) lists.
- **6AMLD:** The Sixth Anti-Money Laundering Directive includes provisions for a harmonised definition of money laundering offences, an extension of the scope of money laundering and the criminal liability of persons associated with it, and stricter punishments for those convicted of money laundering. The Sixth Anti-Money

[27] Comply Advantage, *Global AML Regulations: What You Need To Know*, https://complyadvantage.com/insights/aml-regulations/, last access 13.04.2025

Laundering Directive enacted provisions for a more integrated and harmonised definition of money laundering offences, in line with an extension of the scope of money laundering and the criminal liability of persons associated with it, and more severe punishments for those convicted of money laundering[28]. The new directive focused on removing loopholes in the domestic legislation of member states by harmonising the definition of money laundering across the EU. On the one hand, previously, the criminal framework combating money laundering according to the EU law can fittingly be described as a mosaic of regimes and regulations rather than as a complete body, which has led to a lack of legal clarity in certain individual cases and the lack of recognition of some crimes and security breaches by companies. However, on the other hand, the 6AMLD points out these problems by hardening and clarifying the definitions of offences and penalties, thus providing solutions to these niche cases via strengthening case law practices and including the evolution of corporate responsibility.

Moreover, the 6th AMLD integrated three main points to be considered as aggression: criminal activity, the acquisition of any property through the criminal act and the laundering, which is essential for what RegTech companies are working on, corporate responsibility and identification under article 7. The aforementioned article determines that a legal person should be held accountable in conditions where the "*lack of supervision or control*" by this legal person with a *"leadership/major governance position*" has made the criminal act possible. For instance, articles 5 and 8 focus on the application of sanctions for both companies and individuals to reduce legal disputes and confusion:

- One of the groundbreaking regulations was the denial of the right to governmental benefits or support and provisional or permanent prohibitions to access public funds, including grants and concessions.
- Another one is the temporary or permanent disability for commercial activities.
- Imposition of judicial surveillance.
- Judicial closure orders and temporary or permanent closure of establishments to settle a code of fair competition

[28] MOODY'S, *Understanding the 6th Anti-Money Laundering Directive (6AMLD)*, https://www.moodys.com/web/en/us/kyc/resources/insights/understanding-the-6th-anti-money-laundering-directive-6amld-key-changes-and-compliance.html, last access 13.04.2025

- Criminal punishment that could result in the imprisonment of responsible professionals if the causal connection is established

4.3 The UK

The Financial Conduct Authority (FCA), an independent public organisation in the UK, oversees the behaviour of almost 50,000 businesses to guarantee that the country's financial markets are truthful, competitive, and equitable. In addition to its independent, non-governmental body, which regulates the UK's financial services industry, specialising in combating money laundering and other financial criminal activities, firms and individuals must be authorised or registered by the FCA to carry out certain economic activities.

Beyond preventing financial crimes, the FCA's broad objectives also include protecting consumers from unethical behaviour, maintaining the stability of the economic system in the United Kingdom and encouraging market stability and integrity while promoting competition through rule enforcement and investigations. In summary, FCA's executive authority consists of:

1. **Regulation**: Establishing the minimum legal requirements for financial products in the UK and enforcing FCA-mandated regulatory prohibitions on non-compliant products.
2. **Supervision:** This involves ensuring that UK FIs operate securely and adhere to niche AML regulations, conducting risk assessments, monitoring suspicious activity(SA), and reporting to appropriate authorities.
3. **Authorisation:** One of the most critical pieces of legislation is imposing registration and requirements on financial institutions before issuing authorisation to operate in the UK.

The main pillars of UK AML/CFT rules are the Proceeds of Crime Act of 2002, the Money Laundering, Terrorist Financing, and Transfer of Funds Act of 2017, and the Terrorism Act of 2000. According to FATF principles, these laws define the crime of money laundering and set strict compliance requirements. Furthermore, the UK remains committed to implementing elements of 6AMLD even after exiting the EU.

4.4 The US

The central anti-money laundering regulation in the US is the Bank Secrecy Act (BSA), which FinCEN administers; with FINCEN, the US Office of Foreign Assets Control (OFAC) is responsible for enforcing US sanctions laws. Although the BSA's primary focus is to combat money laundering activities, its scope has expanded to include other financial crimes; for instance, it was amended by the Patriot Act to implement countering terrorist financing (CFT) measures in 2001. Under the BSA, financial institutions must fulfil a bundle of requirements as follows:

1. **The BSA Compliance Program:** US financial institutions must develop and implement an internal anti-money laundering program or create a playbook to suit their risk profile to incorporate manual guidance on identifying and controlling risks. AML programs should consist of written policies and procedures, employee training, audit schedules and the appointment of a compliance officer.
2. **Reporting to the BSA:** The BSA includes standards for AML reporting and filing, including SAR, Currency Transaction Reports (CTR), and Form 8300 for high-value transactions, which is the report of cash payments over $10,000 in a trade or business.
3. **Record Keeping:** FIs must maintain thorough documentation of the above-described suspicious activity, including purchasers' identities and the value of their transactions, to report clarity measurements and comply with current amendments and codes. Furthermore, the US criminal code stipulates that employees of financial institutions who deliberately violate the BSA or its implementing regulations face criminal penalties of up to $250,000, five years in jail, or both.

In the more recent developments, in 202,1, the US passed the Anti-Money Laundering Act 2020 (AMLA), the utmost quintessential amendment to the BSA since the Patriot Act, which instituted and introduced the following AML/CFT measures:

- The new regulations will compel beneficial ownership disclosure.
- More severe financial penalties for ML offences and any compliance violations according to the BSA or relevant legislative regulation

- New protections have been introduced for corporate AML/CFT whistleblowers, who report money-laundering violations and sanctions evasion through a government program that offers rewards.
- Expanding administrative powers of US authorities to look into foreign banks suspected of money laundering in more detail.
- A pilot project to expand the exchange of SARs and associated data with US bank affiliates, subsidiaries, and branches abroad.

4.5 Hong Kong Monetary Authority (HKMA)

HKMA is the main one responsible for the integrity and stability of Hong Kong's banking system and monetary policy under the authority of the AML and CTF Ordinance. The HKMA is the regulatory body liable for combating ML and financing terrorism. HKMA operates to ensure that FIs in Hong Kong are meeting diverse legal requirements, the most important being the development and implementation of an effective AML/CFT, which must feature the following programs:

1. **Risk Assessment:** Financial institutions must develop their AML program using a risk-based approach to niche AML/CFT risks/threats.
2. **Procedures and Controls:** AML/CFT programs must include various methods and controls, including an independent holistic audit schedule, employee training and screening, and compliance management.
3. **Compliance Officers:** Each financial institution must appoint an MLRO officer with sufficient authority to take initiative for its AML/CFT program and submit SAR to the authorities
4. **Due Diligence:** FIs must perform due diligence procedures on their customers – and enhance due diligence procedures when there is a suspicion of money laundering or terrorism financing activities.
5. **Know Your Customer:** Customer identities must be verified through independent auditing, and FIs must keep records of those background checks.

5. FUTURE CHALLENGES IN AML DUE TO NEW TECHNOLOGICAL DEVELOPMENTS AND TRENDS

In 2023, identifying and mitigating money laundering risks through various trends will be more complex than ever, while ever-strengthening legislation around the globe will increase the cost of an AML failure**.** This section of the paper summarises the main trends concerning money laundering risk through key legislative developments for FIs to be aware of. It also elaborates on technological developments to transform financial crime risk management. Due to the mass advancements of the global payment infrastructure, the threat and complexity of financial crime continue to grow; hence, to be prepared for future challenges, having the right processes, programs and policies in place are the key components for complying with legislative regulations. The widespread use of contactless digital payment methods following COVID has given criminals a chance to exploit flaws in the recently modified digital systems, which changes the rules for financial crimes involving cyber security because cyber terrorists are combining technology and social engineering to create increasingly intricate and difficult-to-detect plans[29]. To avoid possible AML violations, companies and financial institutions should smoothly enhance their AML processes by considering a few essential lessons from recent and upcoming developments:

5.1 The Gig Economy's Emergence

The phrase "gig" economy describes the labour market in which workers accept temporary assignments, or "gigs," in place of full-time jobs, explicitly choosing to work independently for different companies on a task-by-task basis rather than the usual 9 to 5 schedule. The work arrangements may vary from short-term, freelance to project-based. Technological developments and the emergence of digital talent platforms such as Upwork, Fiverr, and PeoplePerHour are linking workers and employers and becoming the driving force behind the increasing prominence of the gig economy since it offers workers greater control over their work-life balance, the ability to explore different roles and industries, notedly, being more advantageous to have another source of incomes[30]. The gig economy has ballooned into an ample sector, contributing an

[29] Guide House, *2023 Anti Money Laundering | In-Depth Feature*, https://guidehouse.com/insights/financial-crimes/2023/anti-money-laundering-financier-worldwide-feature , last access 13.04.2025

[30] AI Group Workforce Development, *The Emergence of the Gig Economy*, https://cdn.aigroup.com.au/Reports/2016/Gig_Economy_August_2016.pdf , last access 13.04.2025

estimated $792 billion to the US economy solely in a year that attracts the bad actors to fabricate new methods to launder the illicit funds due to the abundance of small-scale transactions and peer-to-peer interactions that could lead to opportunities cannot be easily traceable by the FIs[31]. The following methods are rising and becoming a trend of money laundering practice:

5.1.2 Fractionated Transactions

Since gig workers usually conduct several tiny transactions for the sweat of their brows, it is challenging to spot suspicious trends. If money launderers used this fragmentation to mix their illicit funds with lawful income, authorities would have difficulty identifying the source of the money.

5.1.3 Omission of Systematic Oversight

Gig workers are not constantly subject to the same level of financial reporting and scrutiny as those with regular employment, such as payroll; money launderers can influence transactions without raising suspicions.

5.1.4 Cross-Border Transactions

Since the technological developments facilitated the creation of business and bank accounts such as offshore companies and the lack of cooperation between jurisdictions to prevent money laundering from being audited as it should be, the emergence of global gig economy platforms enables cross-border transactions easier, primarily through shell companies. Therefore, bad actors use this worldwide reach to shift money between jurisdictions, expediting it more arduous to monitor and control money laundering operations.

5.1.5 The Taxi Aggregator “Ghost-rides”

Uber, one of the largest taxi aggregators in the world, came under media scrutiny after the allegation that bad actors were using its operations to launder money. The modus operandi of the fraudsters can be briefly explained as follows: bad actors from a random corner of the world would book rides with complicit drivers thousands of kilometres away by typically recruiting complicit Uber drivers. In this method, “ghost rides” would never actually take place; firstly,

[31] Emmanuel Agwu, *Emerging Trends in AML: What Businesses Need to Know in 2023 and Beyond*, [August 2023]

complicit drivers would accept ride requests from money laundering clients at pre-established rates and then Uber takes its cut from these rides where the complicit drivers distribute their earnings to the contractor of the laundering scheme where they would take the cut, and passes along the remaining, clean money to the complicit driver. Fraudsters also implement their purchase of Uber rides with stolen credit cards and then cancel them on short notice after the ride begins, which gives a refund from Uber's end and then sends it to the fraudsters' bank account. The fraudsters would take a cut of the refund and return the rest to the complicit driver who provided the stolen credit card, which facilitates launderers' stolen funds into legitimate money. Uber has turned into a platform for cybercriminals because it is difficult to effectively monitor all of the transactions on its platform because of its vast volume, and the technologies available are insufficient to stop transaction laundering. In addition, the "Acupuncture" method defines overseas transactions, especially the money laundering transactions on Uber that occur in China. In the acupuncture method, the complicit drivers collect the money from the stolen credit card through the ghost ride and then transfer the sum to the overseas criminals to launder the funds, addressed as "nurses."

5.1.6 Airbnb Scam

Money launderers developed a method of using stolen credit cards to launder illicit funds through Airbnb hosts. They would cooperate and meet with them on underground forums. In the Airbnb scheme, the complicit hosts would split the payment with the money launderers and leave fake reviews to efficiently complete the transaction by the vast scope of Airbnb's operations since it is not easily traceable to detect illegal activity. Like the Uber scheme, complicit guests usually collaborate through "job offers" posted on the dark web, which can be dissimulated as having non-existent guests in their Airbnb accommodation and transferring legitimate funds to their bank accounts. When the bookings are processed through the platform, the two parties, aka abettors, share the payment and create false end-of-stay reviews to finalise the transactional loop. Moreover, since Airbnb operates thousands of locations with abundant governing jurisdictions, no standard regulation can effectively screen and monitor its services; therefore, cybercriminals seized this opportunity of the legal gap in AML practices. Subsequently, when these assets acquired correspondingly from this financial crime are transferred to the Airbnb accounts, they are already integrated into the financial system "legally". Suppose it is necessary to launder large

sums of money. In that case, bad actors might make annual deals with money mules who retain several accommodations to provide a service in Airbnb that appears to be given to a customer who is not there.

It raises the question of whether Airbnb's platform is flimsy against bad actors or whether a more significant issue is at play. The answer would be transaction laundering, a polished method that is a merchant-based fraud scheme whereby an incognito entity conveys e-commerce transactions through a legitimate merchant account. Regulators tend to focus on traditional transactions that occur in the physical world, such as shell companies, and transactions that exceed regulatory thresholds and devote massive resources for AML screening and monitoring, which contradicts the modern payment activities online that do not always fall under the radar for both regulators and law enforcement officials. Therefore, without the extension of the measurements fully integrated into the digital world through utilising new technological remedies to detect and prevent Transaction Laundering, the blind spot within the law will be abused by the bad actors[32].

The rapid advancement of online marketplaces has pros and cons, but it also brings an additional risk: Transaction laundering has become prevalent amongst frequently visited marketplaces. In sum, bad actors use dumpy businesses to pay the credentials of a legitimate merchant to process through various payment methods, particularly credit card payments for products and services which are illicit or illegal. In essence, forestalling money laundering activities in the gig economy could be achieved by three steps: first, adapting an effective KYC and AML protocol, thriving reporting mechanisms such as suspicious activities and transactions, compliance regulatory reporting, currency transaction reporting, foreign account tax compliance act management, common reporting standard and management analytics and ultimately concerted regulatory efforts which stands for a collaborative exertion between governments, financial institutions, and platforms to set up efficient methods for identifying and combating money laundering.

[32] Finextra, Cooking the Bookings? How Airbnb Became Entangled in a Transaction Laundering Scandal, [February 2018],https://www.finextra.com/blogposting/15086/cooking-the-bookings-how-airbnb-became-entangled-in-a-transaction-laundering-scandal last access 13.04.2025

5.1.7 Freelancer platforms and micro-laundering

Micro laundering is an ML method that transfers large amounts of money by distributing it over hundreds of e-transactions, as in scattering it below the AML threshold; hence, the transactions won't trigger monitoring systems. On the other hand, freelancer platforms that can be expanded to online job marketplaces are a primary target for bad actors. The launderer's scheme fundamentally remains the same: finding a complicit individual who feigns to be a freelancer, setting up a protection or job on the platform and choosing the complicit individual from a host of other legitimate applicants who apply for the job. After the bad actors hire the complicit, the platform receives the money and gets its cut. Then, the money is successfully paid to the complicit for completing the "alleged" project; the complicit, in this scheme, the "freelancer" takes their cut and sends the rest back to the fraudulent job coordinator. In effect, the freelancer platforms are vulnerable to these types of money laundering activities due to the reason that payments on these platforms are held in escrow and are disbursed to the freelancer upon completing the assignment, which successfully helps to cover up the launderer's tracks since they manage to stay under the radar or regulative sanctions through micro-laundering by setting up the task in smaller amounts from $2 to $20. Not only are freelancer platforms threatened by micro-laundering activities, but online payment services and mobile micro-payments interconnected with traditional payment services such as PayPal are in peril since funds can be moved to or from various payment methods. Subsequently, another trending method is using prepaid cards to transfer funds between scammed bank accounts with instant transactions or executing card cracking or card testing: fraudsters would use stolen or fake card data to charge money onto the prepaid cards, then rapidly withdraw the funds not to trigger the financial institutions' monitoring systems.

The rapid advancement of online marketplaces has pros and cons, but it also brings an additional risk: Transaction laundering has become prevalent amongst frequently visited marketplaces. Therefore, bad actors use dumpy businesses to pay the credentials of a legitimate merchant to process through various payment methods, particularly credit card payments for products and services which are illicit or illegal. In essence, forestalling money laundering activities in the gig economy could be achieved by three steps: first, adapting an effective KYC and AML protocol, thriving reporting mechanisms such as suspicious activities and transactions, compliance

regulatory reporting, currency transaction reporting, foreign account tax compliance act management, common reporting standard and management analytics and ultimately concerted regulatory efforts which stands for a collaborative exertion between governments, financial institutions, and platforms to set up efficient methods for identifying and combating money laundering.

5.2 The Growing AI Trend

AI has been developing quickly in recent years and has the potential to significantly change AML procedures by improving the precision and effectiveness of identifying and stopping suspicious activity. Nonetheless, testing AI could lead to legal problems since automated systems would monitor customer data to identify any odd behaviour that might violate fundamental rights, such as the right to privacy, data protection, and data retention. The AML systems should abide by the proportionality test under EU fundamental rights law, which is very similar to the German administrative law; at the EU level, the test comprises three steps: appropriateness, necessity and proportionality stricto (justifying a limitation on a constitutional right).

Data retention is very nontrivial at the EU law level, as argued by ECJ in the joined cases of Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Watson. According to the ECJ's preliminary ruling/ prior review, national legislation setting up mass surveillance of electronic communications to combat crime violated the right to privacy and data protection. This ruling was based on the appeal of Swedish and UK courts after ECJ's former ruling in Digital Rights Ireland overriding EU's Directive 2006/24/EC on data retention under the general obligation to retain specific communications data contextured a significant interference with the fundamental rights lawfully to establish the protection for private life, data minimisation and purpose limitation for personal data.

The Court cogitated that Directive 2002/58 on privacy and electronic communications shall be construed in light of Articles 7 and 8 of the CFREU, videlicet, the rights to privacy and data protection. Even though the rule's primary goal is to prevent crime, it also gives national laws the power to interpret the law more broadly and encourage "liberal construction," which violates human rights laws by indiscriminately keeping track of all subscribers and registered users'

location and traffic information for all electronic communication channels. In particular, national legislation established this equitable person construction of a collection of all the traffic and location ground on crime prevention to such an extent that it has compromised all the people using electronic communications services, even those not going under any criminal proceedings. Hence, it was apparent that such restrictions on human rights were not limited to what was necessary, violating one of the essential principles of EU law: data minimisation.

Subsequently, the ECJ emphasised that even though the situation for restraints may change depending on the measures implemented, such as the prevention, investigation, detection, and prosecution of serious crimes, data retention must continue to meet objective standards that establish a link between the data to be retained and the goal being pursued. Lastly, the ECJ's ruling can be concluded in paragraphs 114 and 125 of the decision ECLI:EU: C:2016:970:
"*Directive 2002/58 shall be elucidated as precluding national legislation that permits national authorities access to the retained data, unless the objective proceeded by that access, in the context of combating crime, was restricted exclusively to fighting serious crime(such as organised crime and terrorism) was, subject to prior review by a court or an autonomous administrative authority, and requisites the data to be retained within the EU.*"

This ruling can be a pivotal guide for data retention with AI technology; since the automated systems store massive personal data, it might be challenging for AI to demarcate how much data can be processed,d and since its scope is vast, it would bring AI challenges whether overruling compliance regulations would violate aforementiıned human rights. To get a better grasp on AI's impact on AML activities, knowing the three most common levels of AI would be a pathfinder:

5.2.1 Artificial Narrow Intelligence (ANI)

This level of AI is the most recognised and embedded in our daily lives. It has a more straightforward, narrow range of functions, such as customer service chatbots; recommendation engines like Google, Netflix, and Spotify; and voice assistants like Apple's Siri and Amazon's Alexa.

5.2.2 Artificial General Intelligence (AGI)

At this level of AI, machines have human cognitive abilities that can work alongside humans, such as machine learning and robotics. The most remarkable asset of this type of AI is that it can behave human-likely across all tasks carried out by comprehending cause and effect and following common sense in making decisions.

5.2.3 Artificial Super Intelligence (ASI)

At the given moment, this type of AI does not exist yet. However, if this type of AI machine existed, it would have the capability to carry out and perform tasks and things that only a natural person is capable of. Oxford philosopher Nick Bostrom describes ASI as "*any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interes*t."

The current AML software is powered through AGI technology by using machine learning to detect any possible transaction over the legal threshold according to the governing law or examine transaction, account, customer relationship, company, and other data to identify patterns, instances, groups, anomalies, and networks for financial institutions. Machine learning can be summarised as using and ameliorating machines by using the inputted data and being able to adapt and learn independently without following explicit instructions through utilising algorithms and statistical models to analyse and draw conjecturing from schema & structure in data. Therefore, machine learning enables a system to learn to recognise patterns and make predictions on its own quickly through the application of knowledge and training from large data sets. Henceforth, implementing AI in AML practices is a double-edged sword: on the one side, the advantages of AI in Anti-Money Laundering are imperative, and on the other side, it can be arduous to implement AI in Anti-Money Laundering[33].

Furthermore, there are two types of machine learning, **supervised** and **unsupervised**, and three primary techniques, which can be categorised as **natural language processing**, **network analysis,** and **predictive analytics**.

[33] R.Alhajeri and A. Alhashem, *Using Artificial Intelligence to Combat Money Laundering,*Intelligent Information Management [Vol.15 No.4] [July 2023]

-) Supervised Learning

This type of machine learning uses labelled datasets to teach algorithms to predict outcomes and perceive patterns by specifying and identifying the data fed to the device. A primary example is filtering in email services. In these systems, financial organisations can train databases to recognise patterns or anomalies in new data and organise any suspicious activities through transactions correspondingly and effectively.

-) Unsupervised Learning

The unsupervised technique is based on building a machine learning model without labelled training data or even human interaction, founded entirely on the raw data presented, which requires an unsupervised learning algorithm to separate the given dataset into different groups, leading to allow the algorithm to act on that data without being steered by human intervention. One core importance of this learning is that the machine generates an output based on the data's most notable traits and finds logical patterns and groupings subsistent in the information. Unsupervised learning technologies and their assistance have facilitated AI's integration into various business activities in the financial area, including searching, location identification, dictation, and problem-solving, and auditors are using it to analyse multiple data points, including personal information, biometrics, behavioural patterns, and especially detecting anomalies in financial transactions[34].

-) Natural Language Processing

This language-based AI technique exercises AI and data to predict the next word in a sentence sequence. By utilising coding language sets or tools such as ChatGPT, this language is programmed to learn to complete sophisticated written requests, which can vary from legal contracts to advanced cognitive tasks, such as computer coding and programming, all based exclusively on text prompts.

This method has the potency to streamline standard AML tasks, as well as the screening of client names and related parties from various lists for sanctions, negative news, risk indicators, and political exposure. The financial institutions will even be able to cluster groups of names with entities for a specific jurisdiction, fostering and reducing false positives. In one example, a CFO

[34] Persona,*AML and AI: How machine learning can help prevent money laundering* ,https://withpersona.com/blog/aml-ai, last access 13.04.2025

named “Mehmet Can” can be searched, in conjunction with any or all of their identifying data, to reduce the number of results for other individuals with any part of the same name accordingly[35].

-) Network Analysis

The chronicler of AI's brain is network analytics. An account, a name, or a location are examples of a single factor, data, or input that machine learning and analytics may quickly analyse. They cannot, however, undoubtedly link these variables across a whole network of people in a financial institution's enormous database. For example, a beneficial client owner's sister who goes by her maiden name but is married to a PEP in another nation improves her comprehension of social behaviour, communication optimisation, and complicated systems[36].

-) Analysis of Predictive Data

This technology uses machine learning and historical data to forecast future events, trends, and paradigms. Predictive analytics can be utilised to study expected in contrast to actual activity, one of the principles used to assess ongoing risk assessment and fraud detection throughout transaction monitoring. Here are some cases of AI Improving AML Procedures:

-) Enhanced Customer Due Diligence (CDD)

A traditional CDD process is more prone to human errors because it requires more manual identity verification assessments. It is also more time-consuming to conclude the risk assessment and comply with the prerequisites in the respective country. AI-powered tools can facilitate and automate the CDD process using advanced data analytics to verify customer identity and adhere to risk mitigation necessities. Many examples of these automated technologies exist, such as facial recognition technology, which is used to corroborate customer identities, and remarkably natural language processing, which makes it possible to analyse unstructured data sources such as social media profiles to evaluate customer risk and reduce false positive alerts to save considerable time.

[35] Ibid
[36] Ibid

-) Efficient Transaction Monitoring

In a classical transaction monitoring activity, the monitoring systems depend on pre-defined rules, patterns and thresholds to flag conceivably suspicious transactions, which might cause the system to have many false positives. Therefore, AI technology streamlines automating manual tasks in a significant proportion, which assists in freeing up resources for other critical tasks and reduces the time consumed for compliance reviews, which leads financial institutions to take action against potential threats rapidly. Consequently, as a result of the fast adaptation abilities of AI, it can adjust to changes in criminal behaviour and regulatory requirements, generating fewer false positives through machine learning algorithms that learn from historical data and identify patterns of illicit money laundry activities. Some of these activities can be listed as:

- Multiple deposits or withdrawals in a transient period.
- Transactions involving high-risk countries or individuals or PEPs.

-) Ameliorated Suspicious Activity Reporting and Automated Risk Assessment

SARs support reporting potential ML activities to the relevant authorities and comprehensively sustain ongoing monitoring; nonetheless, they take valuable employee time that could be used more efficiently. Henceforth, implementing AI-powered SAR tools using NLP would assist in analysing and categorising SAR reports by identifying patterns of suspicious behaviour, which could trigger alerts for compliance teams to investigate more thoroughly.

-) Cost Effective

Since AI streamlines many AML processes and solutions to be more automated, it can reduce costs associated with compliance reviews and investigations while improving the efficiency of compliance programs. On the other hand, AI implementation brings challenges to FIs through compliance with their AML programs:

-) Data quality

AI's machine learning is dependent on constant "high-quality" data input and reconciliation to execute as many error-free predictions as possible due to poor data quality, for instance, incomplete or inaccurate input that can steer to false positives or false negatives, which would eventually end up disrupting the effectiveness of AML programs.

-) Interpretability

Since data processing and AI-based technologies are still rapidly advancing, it is challenging for FIs to explain to regulators or auditors how decisions are made using complex and arduous AI algorithms.

-) Regulatory compliance

Due to its nature, complying with knotting and changing dynamics of AML regulations and implementing AI in AML programs are becoming more challenging every day for FIs since it takes significant time, labour and resources to implement while maintaining compliance.

-) Human expertise

No matter how automated and facilitated the AML process can get with AI advancements, authentic and human expertise is still indispensable to making accurate decisions based on AI-generated insights.

-) Bias

One downside of the transferred data to the algorithms is that if the AI is trained on biased data or isn't appropriately structured to address biases, it can lead to discrimination and inaccurate predictions.

There are many similarities between AI and AML since both frequently rely on patterns in highly layered data sets. Deposit frequency, quantity, location, and jurisdictions of businesses, controllers, owners, and politically exposed persons (PEPs) can all be significant trends related to AML. Machine learning can execute the task of practically discovering the hidden connections between the variables, making it a cost-efficient focal point for FIs.

In summary, AML solutions implemented in FIs have a linear pipeline workflow that links with the data source powered by AI. It is imperative to add specific parameters to assist in identifying risky transactions, customers, or communications that might indicate fraudulent behaviour by data analysts and programmers. Secondly, an ordinary AML system supported with AI consists of 4 plies: a data layer, a screening and monitoring layer, an alert and event layer, and an operational layer. Furthermore, the banking system relies on credible information submitted by

customers to monitor legitimate and suspicious activities. As a result, the data layer concerns data collection, management, and storage.

5.3 Rapid Crypto-currency Changes

Cryptocurrencies are intangible properties that are freewheeling and fungible financial instruments that are not bound to any country's borders or specific agencies within the government. Cryptocurrency-based transactions bring a lot of different challenges for FIs since these transactions are based on blockchain technology, which notably presents a "pseudo-anonymity" between a unique identifier address (provides a location where funds can be received, stored, and sent) and a bank. Moreover, in traditional customer onboarding, there is compulsory proof of identity and KYC/CDD standards that FIs must follow to possibly match or link any possible fraudulent financial transactions in the future; on the other hand, this kind of requirement is not applicable to create/have a cryptocurrency address, which causes for this address to be used as a pseudonym for hiding the owner’s identification. Henceforth, not being able to match the beneficial owners' addresses to real-world identities would bring a massive challenge to the trustworthiness of any cryptocurrency transactions since they won't be linked to the identity of the parties involved and use wallet addresses as a substitute, which would stay anonymous. Although crypto-currencies fortify the anonymity between aforementioned transactions, the latest technology and strengthened techniques for cryptocurrency transaction monitoring facilitate the detection of illicit activities.

a) Deep Analysis of Blockchain

On the one hand, deep analysis of Blockchain helps FIs detect patterns of suspicious activities, such as the movement of colossal amounts of money, numerous transactions to and from the same address, transactions with known illicit entities, and, most notably, hidden wallets and transaction mixing services that are used to disguise the source of the funds. Nonetheless, this technology requires substantial technical dexterity and specialised software to analyse blockchain data; therefore, FIs must invest in the imperative tools and resources to execute practical blockchain analysis to discern and prevent fraudulent activities.

b) Monitoring Based on Behaviour Patterns

Behaviour-based monitoring is another technique used to analyse the behaviour of cryptocurrency users and identify any unusual patterns of activity, which allows FIs to be notably more effective in determining new and nascent threats in the cryptocurrency market. As a consequence of continuously monitoring user behaviour and identifying patterns of activity, not only FIs but also regulators can swiftly distinguish new threats and formulate effective risk mitigation and management strategies. For instance, when a user unexpectedly starts carrying out a high volume of transactions or sending cryptocurrencies to peculiar locations, it could be a sign of suspicious activity. Despite the advantages of behaviour-based monitoring, one of the biggest challenges is that legitimate users may conduct uncommon behaviour that doesn't indicate any illegal activity. Hence, it is vital to establish a balance between detecting suspicious activity and reducing false positives.

c) Analysis Conducted Between Peers

This technique analysis concerns peer-to-peer exchanges, or decentralised exchanges that let users trade cryptocurrencies without intermediaries. Peer-to-peer exchanges have gained popularity among cybercriminals because they make it simple to exchange cryptocurrencies for fiat money to obfuscate their illicit activities.

d) Monitoring Based on Risk Assessment

This type of risk assessment plays a vital role in determining travel rule crypto necessities. The travel rule stands for crypto assets, which states that the customer's personal information must supplement any crypto transaction that exceeds a particular threshold. Therefore, to comply with the regulations, Virtual asset service providers(VASP) must sanction and screen the counterparty customer and perform DD on the counterparty VASP. This method entails any risk associated with each transaction and allocating a risk score based on several factors such as customer behaviour and, transaction amount, location in which the higher the score gets, it is more likely to be subjected to additional inspection and perusal that can reduce false positives and augments the effectiveness of transaction monitoring[37].

[37] Sanction Scanner, *Challenges and Techniques in Cryptocurrency Transaction Monitoring*, https://sanctionscanner.com/blog/challenges-and-techniques-in-cryptocurrency-transaction-monitoring-735 , last access 10.01.2025

5.4 The Occurrence of Metaverse

Metaverse's money laundering practices involve unconventiınal layering, placement, and integration methods. The detectability of fraudulent activities challenges legislation worldwide due to three additional risks posed by the Metaverse platform: **anonymity, jurisdiction,** and **NFTs**.

A) Anonymity

Conventional and non-virtual ML activity risks being exposed due to identification processes that FIs imply under their AML policies. For instance, when the placement stage of ML occurs through a bank account, it is more likely to be linked to a real person who deposited or transactioned the money, which will presumably end up being reported and decrease the chances of staying anonymous. On the other hand, anonymity within the Metaverse can be more plausible since the current legislation does not force users to identify themselves; thus, these fraudsters can stay anonymous through Metaverse's interoperability that permits the use of different avatars(*Metaverse User*) and payment providers(*Credit Cards, Central Bank Digital Currencies*). Therefore, an avatar doesn't need to be provided by the same company as the payment system, which facilitates peer-to-peer payments to stay on an anonymous basis[38].

b) Jurisdiction

The anonymity of the Metaverse, the large-scale access to the platform, and peer-to-peer payments without the need for the arduously regulated financial sectors create two significant problems in jurisdiction and applied law: the effortless accessibility of parties internationally and the legality of current regulations. Consequently, the providers of the virtual world and its payment system can reside in advantageous countries. In this context, "favourable" refers to reduced tax, legal, or enforcement requirements, and providers are drawn to these jurisdictions because they are cost-effective. Peer-to-peer payment systems allow businesses to circumvent highly regulated banking institutions, and peer-to-peer payments that happen without the involvement of regulated parties entail higher risks. The financial institution in the EU records the transaction when a payment is made through a bank or money transfer agency from the EU to

[38] M. Annelieke, *Money Laundering and Financing of Terrorism via the Metaverse*, Regulating the Metaverse Economy, SpringerBriefs in Law [November 2023]

a state with fewer regulations. This institution should notify the relevant authorities if the transaction amount appears suspicious.

Organisations can relocate to areas with lax regulations or move entirely away from a particular jurisdiction. It is possible to establish virtual environments in the Metaverse without regard to jurisdiction. Although a virtual environment provider may choose to create the climate anonymously, it is challenging to determine in the absence of a recognised host provider. It might be possible to track down and utilise the server that hosts the environment as jurisdiction. Nonetheless, this would be an expensive and challenging process. Providing financial services in this setting was difficult since the financial institution needed customers' trust.

c) NFTs

Non-fungible tokens (NFTs) are a type of token that is linked to non-fungible items and built on blockchain technology. These must be one-of-a-kind items, such as a work of art, a collectable, or a musical composition. To establish ownership, the item's owner can make NFTs depending on the item and in a virtual setting; the NFT then functions as a type of originality and ownership certificate. The (virtual) object does not need to be transferred; however, this certificate can be purchased and transferred. NFTs are regarded as the digital equivalent of property rights; therefore, it follows that NFTs are a technology that will be present for the foreseeable future. Furthermore, Metaverse will create an additional venue for the virtual walls showcasing digital art.

Information sharing via NFTs carries considerable risk, which needs to be processed as seamlessly as possible, and a party must make sure the funds go to the proper party in the end if it intends to fund terrorism. Any kind of funds can pass via "ordinary MLFT"; thus, they don't need to be precisely the same cryptocurrency coin or euro note that ends up in the other wallet, and it would be more beneficial if several currencies arrive at the destination since financial regulations are more tightened in some jurisdictions. The initiator is pleased as long as a specific value is received after the chain, and the same NFT that is sent must arrive at the intended recipient when employing NFT for information transfer.

In consequence, with NFTs, it is possible to create unique global, artificial, and immaterial items and sell them on the Metaverse marketplace without enrolling in Metaverse platforms to turn a

profit. This increases the risk of aggressive market manipulation, rug pulls, honeypots, and crypto scams. Most notably, it can be utilised for ML due to unpredictable pricing since the value can be determined in a highly subjective aspect.

5.5 Video Games

People of all ages are enjoying playing video games online. However, the gaming industry's growth has led to an unprecedented increase in vulnerability to financial crimes. Microtransactions and loot boxes in video games have become more attractive to criminals as a means of money laundering due to the growth of virtual economies and the rising value of in-game currency and products. Money launderers find the Internet appealing since it offers anonymity and worldwide accessibility, making it comparatively simple to transact money across borders and via various banking systems. Furthermore, the absence of regulation and monitoring regarding virtual currency and in-game commodities in video games may facilitate the activities of money launderers in these settings through the following practices:

a) In-game currencies

The in-game currency used in video games is a virtual currency obtained by conquering obstacles and winning challenges. One type of money in a virtual environment is in-game currency, which may be acquired in several ways. Every massively multiplayer online role-playing game (MMORPG) has its in-game economy and currency. MMORPGs such as Final Fantasy XIV, Runescape, and World of Warcraft are well-known. Convertible and nonconvertible in-game currencies are the two categories of in-game money. [39]:

Convertible In-game Currency

A player can trade convertible in-game cash for actual fiat money or money approved by a fiat or government edict. The convertible game currency has a specific exchange mechanism and a dynamic exchange rate. Players can purchase, sell, or trade virtual properties using this cash.

[39] European Commission, *The Consumer Protection Cooperation Network's Key Principles on In-game Virtual Currencies* [March 2025]

Nonconvertible In-Game Currency

Players can convert actual fiat money into the game's currency through nonconvertible in-game currency. It is not possible to trade this currency with other players, and it can be used to purchase video game accessories like weapons, talents, and other things to personalise or enhance a character's skill set. Nowadays, many well-known games worldwide employ this kind of money and make money by selling in-game currencies that aren't convertible.

b) Microtransactions

Microtransactions enable users to buy digital items, virtual currencies, and gaming material. Microtransactions refer to the players' use of real money to purchase in-game goods. Microtransactions are seen in free-to-play games and mobile apps, and they are frequently inexpensive. "Games that require players to first buy a base game, typically in the form of loot boxes, also have microtransactions. While some purchases may be modest ($0.99–$4.99), others can cost up to $80-$99 to unlock a specific character in a game, so "microtransactions" are somewhat deceptive. Criminals purchase expensive characters, props, or gaming features through microtransactions, then resell the characters or in-game virtual currency on secondary market websites for a profit. After being invested in the game, the funds are changed into the game's currency. Since microtransactions enable the purchase of goods for small sums of money, criminals can avoid detection, making tracing money laundering through microtransactions challenging.

Criminals also use microtransactions to launder money by selling video gaming platform accounts. A criminal could set up an account, use illicit funds to purchase goods through microtransactions, and then make "real," "clean" money by selling the account online, and $5 to $3,500 can be sold from these accounts. In such situations, the money laundered typically takes the form of credit card theft. The money obtained by the offender is "clean" money, and the account has already been sold by the time the crime is reported.

c) Loot Boxes.

Loot boxes are described by the National Society for the Prevention of Cruelty to Children (NSPCC) as "*mystery boxes containing a random selection of items that can be purchased with*

real money or credits built up within a game." Typically, loot boxes are accessible throughout gameplay, where the game being played determines what is in a loot box. For instance, a player can purchase a key to open a loot box containing various in-game items that improve the player experience. Loot boxes may contain cosmetic goods for personalising the game (such as new skins for a player's avatar) or objects that impact gameplay (such as new weapons, tools, levels, maps, and in-game money).

5.6 Technological Challenges in AML Compliance

The AML scene has changed substantially over time. AML laws used to be relatively straightforward, but as technology and international trade have grown, money laundering has advanced, and restrictions have become more intricate. Nowadays, companies have various difficulties adhering to AML rules.

5.6.1 The Challenges of AML in the Globalization of Financial Services

With the globalisation of financial services, effective AML policies are more critical than ever. Complex ownership arrangements, varying legal restrictions, and cross-border transactions provide significant challenges for anti-money-laundering specialists.

5.6.2 Transactions Across Borders

As businesses grow worldwide, tracking payments between nations becomes increasingly challenging. This makes it more difficult to identify and investigate potential money laundering scenarios.

5.6.3 Ultimate Beneficial Ownership (UBO)

When assets are preserved in intricate ownership structures, such as shell corporations and offshore bank accounts, it can be challenging to determine their real owners. Even though UBO identification is crucial for AML compliance, it can be difficult because there isn't a consistent regulatory framework or an extensive global database.

5.6.4 Regulatory Organizations

Since there are so many regulatory bodies, each with its own set of AML regulations, navigating the global regulatory environment has historically been a hurdle for businesses implementing AML. Harmonizing laws and improving international cooperation are essential for effectively managing AML issues.

6. CONCLUDING REMARKS

A wide range of technical developments in 2025 will assist compliance leaders in radically changing their AML strategies, cutting expenses, and lowering regulatory risks. Businesses will use intelligent, integrated solutions that provide real-time risk assessment, sophisticated verification, and flexible compliance processes as financial crime grows more complex in the following years. AML's future lies in complying with regulations and developing dynamic, tech-driven ecosystems that can quickly and accurately anticipate, identify, and address new financial dangers**.** Effective KYC compliance is an essential technique that safeguards FIs from risks and fosters client trust, and it goes beyond merely meeting regulatory requirements. FIs can save operating expenses and streamline KYC procedures by implementing the best practices discussed in this article. The main conclusions to be drawn from this article:

- Concentrate on high-risk clients and transactions to effectively manage compliance activities and lower financial crime risk.
- AI and machine learning can increase precision by automating data collection, validation, and risk assessment. And reduce manual labour.
- Utilise a centralised data management system to keep records current, expedite compliance procedures, and guarantee a thorough understanding of every client.
- To stay compliant and ready for new challenges, institutions regularly update their compliance policies to reflect changing requirements.

FIs must ultimately follow stringent AML protocols to fulfil their responsibilities to protect the financial system and its participants from the adverse effects of money laundering. By working together and staying innovative, the financial sector can continue to lead the fight against financial crime and achieve a better and safer financial future for all.

BIBLIOGRAPHY

-) AI Group Workforce Development, *The Emergence of the Gig Economy*, https://cdn.aigroup.com.au/Reports/2016/Gig_Economy_August_2016.pdf (last access 13.04.2025)

-) Comply Advantage, *What are the 3 Stages of Money Laundering?*, https://complyadvantage.com/insights/3-stages-money-laundering/ (last access 13.04.2025)

-) Comply Advantage, *What is Enhanced Due Diligence (EDD)?*, https://complyadvantage.com/insights/enhanced-due-diligence/ (last access 13.04.2025)

-) Comply Advantage, *Global AML Regulations: What You Need To Know*, https://complyadvantage.com/insights/aml-regulations/, (last access 13.04.2025)

-) MOODY'S, *Understanding the 6th Anti-Money Laundering Directive (6AMLD)*, https://www.moodys.com/web/en/us/kyc/resources/insights/understanding-the-6th-anti-money-laundering-directive-6amld-key-changes-and-compliance.html (last access 13.04.2025)

-) Customer Due Diligence (CDD) and its importance in risk management and compliance, https://www.signicat.com/blog/customer-due-diligence-cdd-and-its-role-in-banking (last access 13.04.2025)

-) Emmanuel Agwu, *Emerging Trends in AML: What Businesses Need to Know in 2023 and Beyond*, August 2023, available at: https://www.youverify.co/blog/emerging-trends-in-aml-what-businesses-need-to-know, (last access 13.04.2025)

-) European Commission, *The Consumer Protection Cooperation Network's Key Principles on In-game Virtual Currencies* [March 2025],

https://commission.europa.eu/document/download/8af13e88-6540-436c-b137-9853e7fe866a_en?filename=Key%20principles%20on%20in-game%20virtual%20currencies.pdf (last access 13.04.2025)

-) Lucinity, *6 Best Practices for Streamlining Your KYC Compliance Process*, https://lucinity.com/blog/6-best-practices-for-streamlining-your-kyc-compliance-process (last access 13.04.2025)

-) FATF, *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html (last access 13.04.2025)

-) Fineksus, *Customer Due Diligence Checklist — 4 Steps to Improve Your CDD*, https://fineksus.com/customer-due-diligence-checklist-4-steps-to-improve-your-cdd/ (last access 13.04.2025)

-) Fineksus, *What is AML Name Screening?*, https://fineksus.com/what-is-aml-name-screening/ (last access 13.04.2025)

-) Finextra, *Cooking the Bookings? How Airbnb Became Entangled in a Transaction Laundering Scandal*, https://www.finextra.com/blogposting/15086/cooking-the-bookings-how-airbnb-became-entangled-in-a-transaction-laundering-scandal (last access 13.04.2025)

-) Guide House, *2023 Anti Money Laundering | In-Depth Feature*,https://guidehouse.com/insights/financial-crimes/2023/anti-money-laundering-financier-worldwide-feature (last access 13.04.2025)

-) ICAS, *AML Awareness: Three stages of money laundering*, available at: https://www.icas.com/professional-resources/anti-money-laundering-resources/latest-developments/aml-awareness-three-stages-of-money-laundering (last access 13.04.2025)

-) Lutkevich Ben, *What is risk mitigation?*,

https://www.techtarget.com/searchdisasterrecovery/definition/risk-mitigation (last access 13.04.2025)

-) M. Annelieke, *Money Laundering and Financing of Terrorism via the Metaverse*, Regulating the Metaverse Economy, SpringerBriefs in Law [November 2023], https://link.springer.com/chapter/10.1007/978-3-031-46417-1_4 (last access 13.04.2025)

-) OFACS Sanctions Lawyer, *Bank Secrecy Act Compliance Lawyer*,

https://ofaclawyer.net/bank-secrecy-act-compliance-lawyer/ (last access 13.04.2025)

-) Persona, *AML and AI: How machine learning can help prevent money laundering,*

https://withpersona.com/blog/aml-ai (last access 13.04.2025)

-) R.Alhajeri and A. Alhashem, *Using Artificial Intelligence to Combat Money Laundering*, Intelligent Information Management [Vol.15 No.4], [July 2023]

https://www.scirp.org/journal/paperinformation?paperid=126482 (last access 13.04.2025)

-) Ripjar, *Anti-Money Laundering Regulations Around the World*,

https://ripjar.com/blog/aml-anti-money-laundering-regulations/ (last access 13.04.2025)

-) Sanction Scanner, *Challenges and Techniques in Cryptocurrency Transaction Monitoring*, https://sanctionscanner.com/blog/challenges-and-techniques-in-cryptocurrency-transaction-monitoring-735 (last access 13.04.2025)

-) Sanction Scanner, *What is AML Name Screening?*,

https://sanctionscanner.com/knowledge-base/aml-name-screening-189 (last access 13.04.2025)

-) Trulioo, *AML compliance checklist: best practices for Anti-Money Laundering,*

https://www.trulioo.com/blog/aml-compliance (last access: 13.04.2025)

-) Trulioo, *Sanctions and PEP screening: a critical step in the KYC process,*

https://www.trulioo.com/blog/sanctions-pep-screening (last access:13.04.2025)

-) The Wolfsberg Group, *Wolfsberg Guidance on Sanctions Screening*, https://db.wolfsberg-group.org/assets/4b6c2db6-696d-492e-bdd5-c51552708597/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf (last access 13.04.2025)

-) United Nations, *Money Laundering,* https://www.unodc.org/unodc/en/money-laundering/overview.html (last access 13.04.2025)