Next

Céline Carucci

Generation

Anti-money laundering in the age of crypto-currencies

Nr. 10

EIZ Publishing

Author: Céline Carucci
Publisher: EIZ Publishing (https://eizpublishing.ch)
Layout & Production: buch & netz (https://buchundnetz.com)
ISBN:
978-3-03805-743-7 (Print – Softcover)
978-3-03805-744-4 (PDF)
978-3-03805-745-1 (ePub)
DOI: https://doi.org/10.36862/eiz-ng010
Version: 1.00-20250626

This publication was supported by funding from the "Stiftung für wissenschaftliche Forschung an der Universität Zürich".

This work is available in print and various digital formats in **OpenAccess**. Additional information is available at: https://eizpublishing.ch/next-generation/.

Next Generation

The “Next Generation” series offers a platform for young academics in all areas of law. The aim is to promote the visibility of special talents at an early stage. The volumes in this series are published in Open Access and can therefore be shared and distributed via social media and other channels. Each contribution undergoes a peer review process before it is published.

Anti-money laundering in the age of cryptocurrencies

Céline Carucci*

This thesis explores the growing challenges of combating money laundering in the face of emerging technologies like cryptocurrencies, artificial intelligence, and blockchain. It examines how traditional anti-money laundering (AML) frameworks in the U.S. and the EU struggle to address these challenges, particularly the anonymous and decentralized nature of digital currencies. By analyzing recent regulatory developments in both regions, the thesis aims to assess how effectively new measures target digitalized money laundering and whether they address the gaps in existing AML approaches.

Table of Contents

* Celine Carucci has completed her Bachelor of Law at the University of Luxembourg and has pursued an L.L.M. in International Law at the University of Maastricht with a focus on International Trade Law and International corporate and Commercial law, as well as an L.L.M. in. international and comparative Law at the University of Zürich as part of the University of Zürich's double degree program. She is currently working in the commercial litigation department at a renowned Luxembourgish legal firm in Luxembourg while undertaking the bar exam course in Luxembourg. Her areas of interest are Corporate Law, Investment funds, commercial law and banking and finance law.

List of abbreviations

AI	Artificial Intelligence
AML	Anti Money Laundering
AMLA	Anti-Money Laundering Act
AMLA	Anti-Money Laundering Authority
BSA	Bank Secrecy Act
CDD	Customer Due Diligence
CFT	Counter Terrorist Financing
CFTC	Commodities Future Trading Commission
CIP	Customer Identification Procedures
CRT	Currency Transaction Report
EU	European Union
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FRB	Federal Reserve Board
KYC	Know Your Customer
MiCA	Markets In Crypto-Assets Regulation
MS	Member States
MSB	Money Service Businesses
NCUA	National Credit Union Administration
OCC	Office Of The Comptroller Of The Currency
OFAC	Office Of Foreign Assets Control
RFIA	Responsible Financial Innovation Act
SAR	Suspicious Activity Report
SEC	Securities And Exchange Commission
TFR	Traceability Of Transfer Of Funds Regulation
UN	United Nations
US	United State

I. Introduction

A. Explanation of the general background

Every year, around 2 trillion dollars are laundered.[1] This represents roughly 2.7% of the global GDP.[2] Given the staggering amount of money getting laundered every year, money laundering represents one of the biggest challenges for regulators and law enforcement entities. Money laundering depicts the process of making money obtained through illegal means, or otherwise "dirty", appear clean to hide it.[3] Generally speaking, the fight against money laundering seeks to tackle terrorism and criminal organizations by obstructing their funding. Several methods have been devised to combat such a persistent problem both nationally and internationally, such as the know-your-customer principle or the monitoring of suspicious activities. However, this fight against money laundering has been effectively hampered by technological innovations. With the advancement of communication, technology and technological financial services, money can be moved around the world in a quick and mostly anonymous way, making the fight against money laundering incredibly harder.

B. Statement of the problem

In the past few years, we have seen the emergence of new technologies such as Artificial Intelligence (AI) and blockchain. Additionally, the development of new tech devices and the financial services they offer have facilitated the movement of money. This facilitated movement has created both positive and negative externalities. On the one hand, it is now easier than ever to access its own money anywhere in the world. On the other hand, it is also now easier for criminal organizations to move around money without encountering any issues through cryptocurrencies, for example, which are anonymous and decentralized. This makes the identification of the ultimate beneficiary extremely difficult. Given the emergence of such new challenges, traditional anti-money laundering (AML) methods have proven to be quite unsuccessful, leading to regulators adopting new measures to fight against digitalized money laundering.

---

1 Europol. Money laundering. [Online] Available at: https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering.

2 United Nations (2020) Tax abuse, money laundering and corruption plague global finance [Online] Available at: https://www.un.org/development/desa/en/news/financing/facti-interim-report.html.

3 United Nations Office on Drugs and Crime [Online] Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html.

C. Research question

Given that the U.S. and the EU are the two leading actors in the fight against money laundering, it will be relevant to analyze their regulatory developments regarding the fight against digitalized money laundering. As a result, throughout this paper, the answer to the following question will be sought: *To what extent do the US and European AML frameworks address emerging challenges in the financial sector, such as virtual currencies and digital assets?*

D. Methodology and Literary Framework

The research will be mainly doctrinal and will involve analyzing several doctrinal and legal documents dealing primarily with money laundering and cryptocurrencies. As a prerequisite to write this thesis it was essential to conduct a thorough literary review to get familiarized with money laundering and digital technologies. As a starting point to understanding money laundering, reviewing the book "Anti-money Laundering in a N*utshell*" by Sullivan was of great help. In this book, Sullivan explains in great detail all possible aspects relating to money laundering and the measures undertaken by the U.S. Government to fight it. Jason Sharma's book "*Cryptocurrency Compliance and Operations*" was a great start to understanding the different types of cryptocurrencies and how they operate and can be regulated. Given the topic's novelty, it was necessary to focus on journal articles and reports by professionals specializing in anti-money laundering and cryptocurrencies. Getting familiarized with all the different legislation on the topic was also essential to identify how they are inadequate to deal with the challenges brought on by the use of cryptocurrencies in the ongoing fight against money laundering.

E. Thesis structure

The paper will be divided into three distinct parts. The three main parts will be laid out after the introduction and definition of the topic. In the first part, the different aspects of money laundering will be explained such as its usual way of working, its cycles, and the current traditional approaches to anti-money laundering. In this part, the current/traditional U.S. and EU framework will be presented and analyzed.

In the second part, digital technologies will be presented and explained. First, digital assets and cryptocurrencies will be defined and analyzed to highlight the shortcomings of the traditional anti-money laundering frameworks. Next,

existing digital technologies and their subsets, such as AI, machine learning, and blockchain, will be presented to analyze how these can contribute to the fight against digital money laundering.

The paper's last chapter will focus on the latest regulatory developments in the U.S. and EU, where new efforts to fight anti-money laundering have been undertaken in the last few years. Several bills have been proposed in the U.S. to tackle the new challenges related to digital anti-money laundering. Its analysis will reveal whether these challenges have been effectively taken into account and how effective they might prove to be. Respectively, the analysis of the new EU anti-money laundering framework will reveal how far digital money laundering techniques have been taken into account and whether the new approaches can be useful in the fight against anti-money laundering. Following the presentation of the latest regulatory developments, it will be relevant to see how they help resolve the issues identified under Part 3 and how they fill the gaps identified under Part 2. This part will be followed by a conclusion and some general thoughts.

II. Anti-money laundering

A. Introduction

Money laundering became a known concept during the 20th Century and, more specifically, during the Roaring 20s, which was characterized by economic prosperity but also by the prohibition of the sale of alcoholic beverages. The illicit sale of alcohol, coupled with gambling and prostitution, generated a lot of cash, which needed to be introduced into the licit banking system. As people could not simply introduce these illegally obtained funds into a bank, creative methods had to be devised to disguise the source of such funds. If people deposited this cash into the bank without first concealing its origin, the bank and the government would undoubtedly raise questions regarding its origin, which gangsters could not answer without giving away their unlawful activities. Furthermore, gangsters could not simply spend the money on luxury items as it would again raise questions they could not answer. Additionally, these funds were often constituted of small dollar bills and low-value coins, which made transporting and concealing these funds incredibly difficult.[4]

To resolve their storage problem and to actually be able to use their ill-gotten gains, gangsters started opening legitimate businesses, like laundromats, with the objective of making their funds appear legitimate. Given that small coins were necessary to use laundromats, it was the perfect way to hide the true origins of their funds. The amount of money used to "wash clothes" was considerably higher on paper than the money needed to operate a laundromat, which is how the term "money laundering" was born.[5] The objective was to mix legitimately gotten gains with the illegitimate ones, thereby making the illegitimate ones appear legitimate on paper.

Money laundering refers nowadays to the "process by which criminals clean the benefits of their activities to hide their illegal origin."[6] Or, in the UN's General Assembly, slightly more complicated terms: "*The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the crime to evade the legal conse-*

4 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.
5 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.
6 European Commission, Money laundering [Online] Available at: https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/money-laundering_en.

quences of his actions."[7] The main message being conveyed through these two definitions is that people are trying to make illegally obtained money appear legal on paper so they can use it however they want.

There are a few reasons for people to launder money. On the one hand, the financial system is the safest place for people to actually hide their money. On the other hand, it is a way for people to move money around the globe quickly and efficiently and to start spending the illegally obtained money without raising any regulatory bells. For these reasons, money laundering is a key activity for criminal organizations such as drug dealers or terrorists, which is why it has now become illegal, given that it is used to finance a wide array of crimes. To thwart the expansion of these criminal activities, anti-money laundering frameworks have been adopted globally.

AML regulation will generally serve three distinct purposes. The first purpose is to disrupt the occurrence of crimes in the first place. Secondly, and obviously, AML regulation will aim to disrupt and identify money launderers and the people who enable them. Finally, AML aims to regulate obliged entities by requiring them to constantly maintain adequate compliance procedures that would allow them to identify money laundering and address it accordingly.[8]

B. Money laundering cycle and methods

1. Cycle

Although money laundering can be achieved through multiple methods with the end goal of disguising the origin of the funds, money laundering will always be done in the same circular pattern.[9] The laundering cycle will always go through three phases: placement, layering, and integration. The cycle in cases not involving terrorism financing will always be circular as it will start from the placement by the criminal and will end through the integration phase, where the money goes back to the criminal as it is ready to be used in the licit financial system.

---

7 United Nations General Assembly (UNGA) United Nations Convention against Transnational Organized Crime (2001) UN Doc A/RES/55/25.

8 Hock, B., Button, M., Sheperd, D. and Gilmour, P.M.(2024). What works in policing money laundering?. Journal of Money Laundering Control, 27(1), 5-13 . [Online] Available at: https://www.emerald.com/insight/1368-5201.htm.

9 United Nations Office on Drugs and Crime [Online] Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html.

Placement:

Placement is the first step a criminal will go through when trying to launder money, and it usually takes place soon after the funds have been illegally obtained. In this stage, criminals will have to physically transfer the money to a financial institution to begin the laundering process. This step is usually the hardest one as it will be the one that will be under the most surveillance by financial institutions. The introduction of cash in the financial system can be done in several ways, as criminals can deposit cash (also through "smurfing"), convert the cash in any form of financial instruments, gamble the cash, or even set up a fake business to make it appear like the money to be laundered is a proceed coming from the legitimate business.[10] To avoid any attention criminals will usually structure the proceedings, meaning, they will try to break the cash bills into smaller ones to deposit them in different location and over an extended period of time. For reference, to deposit 1 million dollars, much physical effort would be needed as, if broken into $20 bills, the whole sum would weigh up to 100 pounds.[11]

Layering:

Once the funds have been successfully introduced into the financial system during the placement phase, the layering begins. The goal of this phase is mainly to distance the illegal proceeds from their original source to make it more difficult to retrace the origin of the funds as well as their current location. Criminals can, in fact, simply buy paintings or any other good privately and will justify the possession of such good through an inheritance, a lost and found item, or as a present. Another way to layer the money would be to buy big-ticket items such as cars and register them under the name of a family member, friend, or student. These people usually agree to such an action after receiving a fee from the launderer.[12]

The most complicated but also effective way to layer the money is by moving around the funds to many different accounts, and sometimes to accounts with different names and corporate identities, and transferring the funds to states where bank secrecy is still applied. This will usually "muddle the trail" and break any connection between the money and the crime that was originally committed and make any investigation harder as, while the authorities are

---

10 United Nations Toolkit on synthetic drugs. Money Laundering Methods. [Online] United Nations. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/methods.html.

11 Reyonlds, J. A. (2002). The New US Anti-Money Laundering Offensive: Will It Prove Successful?. Cross Cultural Management, 9(3), 3-31.

12 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.

getting permission to access the account, the funds will be moved to escape being caught. This leads to a constant chase around the globe, which can be won by the launderer by constantly moving the funds to make it impossible for the authorities to access them. When such "layering" is being done by a professional money launderer, the money will be moved up to ten times before proceeding to the last step of the laundering cycle.[13]

Integration

Once the two first stages have been conducted successfully, the money launderer proceeds to the last step of the laundering cycle, the integration phase. During this last stage, the funds originating from criminal activity will be reintegrated into the financial system and are consequently returned to the hands of the money launderer, who can now freely dispose of them. The purpose is for the funds to now look like they originated from a legitimate and lawful source, and for that reason, they will be mixed with legitimate funds, so the distinction between the two will be almost invisible after inspection. This mix between the two types of funds will be done most seamlessly so as not to draw any attention or suspicion from the authorities and financial institutions.[14]

This step, like the others, can take various forms to make it more challenging for prying eyes to detect the illegal origin of the funds. An easy way to do that is to transfer the funds from a shell company to a legitimate bank account. Another relatively simple way would be to purchase big-ticket items such as real estate and big-ticket luxury items.[15]

2. Methods

The issue with money laundering is that it can be done through as many methods as one can think of. These methods can employ several outlets, which can be financial in nature or more business-like. One of the most used methods is cash smuggling, which implies physically moving cash in person, by car, or in luggage without raising any suspicion. Another widely used method is structuring, whereby funds are divided into smaller amounts of money, which can then be safely introduced into the financial institutions without triggering the

13 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.
14 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.
15 United Nations Toolkit on synthetic drugs. Money Laundering Methods. [Online] United Nations. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/methods.html.

filing of any suspicious transaction report.[16] Lastly, another popular method and one of the oldest methods is the purchase of real estate, which can either be rented, sold, or even renovated.[17]

C. Anti-money laundering framework in the U.S.

1. Overview

After the events in the 1970s and especially after the 9/11 tragedy, the AML/CFT have become the pillars of national and economic security strategy in the U.S. The objective of the AML/CFT policy has, however, changed from the 1970s to today. Before, the main goal was to prevent people from evading their tax obligations, which is why the BSA was created.[18] However, after the Twin Towers tragedy, the main goal of the AML and national policy became the disruption of terrorism. This led to the adoption of the 2001 U.S. PATRIOT ACT, whose primary objective was the disruption of terrorism financing.

The U.S. AML policy can be broken into two different areas. The first one is criminal AML, whereby a specified unlawful act is needed to intervene. The second one concerns the BSA and its implementation regulation. Despite the new advancements in the financial system, cash is still primarily being used to launder money given that, despite the difficulty of moving it around, it still remains the least detectable way to move around criminal proceeds in order to get through the integration and placement step of the money laundering cycle.[19]

The U.S. focuses particularly on a risk-based approach when implementing its AML policy, which, according to a FATF publication in 2015, "should be the cornerstone of an effective AML/CFT system and is essential to properly managing risks."[20] This risk-based approach, however, creates considerable

16 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.

17 Remeur, C. (2019). Understanding money laundering through real estate transactions [Online] European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/633154/EPRS_BRI(2019)633154_EN.pdf.

18 Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml.

19 Europol, (2015). Why is cash still king?. [Online] Available at: https://www.europol.europa.eu/sites/default/files/documents/europolcik (1).pdf.

20 FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities And Challenges Of New Technologies For Aml/Cft&ie=UTF-8&oe=UTF-8.

compliance costs to banks and financial institutions, which exacerbates the compliance paradox introduced by the U.S. Patriot Act.[21] In fact, the U.S. Patriot ACT intrudes considerably into the modes of revenue generation of banks and financial institutions which, coupled with the high compliance costs, makes the firms less profitable and more prone to bankruptcy.

2. Evolution of AML framework

The U.S. AML framework has most definitely been a work in progress since the 1970s, with new requirements and rules being introduced gradually at each step. This evolution started with the introduction of the ***Bank Secrecy Act*** (BSA) in the 1970s, whose main objective was the creation of a paper trail that would make investigations by the authorities easier.[22] Accordingly, the BSA created a requirement of recordkeeping and reporting for banks and financial institutions, which involved filing the currency transaction report (CRT) for every transaction reaching the statutory threshold of $10.000. The aim was to identify the person making such a transaction and to maintain a paper trail regarding the funds, making any inquiry by the authorities easier in case of necessity.[23]

The BSA was followed by the ***Money Laundering Control Act, which*** was passed in 1976. This act made money laundering a crime subject to criminal sanctions and focused on the placement of money into the legitimate financial system by prohibiting the structuring of money as well as smurfing.[24] The ***Anti-Drug Abuse Act*** of 1988 further expanded the definition of financial institutions, which were submitted to the recordkeeping and reporting requirements to include businesses such as car dealers and real estate brokers, who were then required to file a CRT for any transaction worth more than $10.000.[25] This aimed to make the layering and integration stages of the money laundering cycle more difficult, given that many were buying big-ticket items such as cars and real estate in cash to avoid any inquiry into the origin of their funds.

---

21 Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml.

22 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

23 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.

24 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

25 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

Next came the ***Annunzio Wylie Act*** of 1992, which introduced quite a few changes and additional requirements in the AML framework. This act considerably expanded the jurisdiction of the U.S. Treasury, which now required any suspicious transactions to be reported. This new reporting requirement effectively shifted the burden of enforcement from the federal agencies to the financial institutions. The act introduced new requirements for financial institutions, such as the creation of AML programs at the Secretary of Treasury's behest, as well as the review of the charter of any federally charged institute already convicted of AML violations and the introduction of special record-keeping rules to be applied in cases of transfers of funds. Importantly, it obliged financial institutions and bank employees not to inform any account holder of any suspicious transaction report being filed in its name.[26] This clearly created an ethical dilemma for the employees. However, a safeguard was introduced to protect them from any civil liability claim in case of an erroneous report being filed.

Later on, in 1994, the ***Money Laundering Suppression Act*** expanded the role of the BSA by merging the Treasury Department Office of Financial Enforcement with the FinCEN to place the administration of the BSA under one single entity, thereby rendering its management more efficient and less prone to conflicting requirements and jurisdictions.[27] This act also introduced quite a few rules concerning Money Service Businesses (MSBs) as they were now obliged to be registered under the name of their owner or person exercising control over them.[28]

The ***Money Laundering and Financial Crimes Strategy Act*** of 1998 created the High-intensity Money Laundering And Related Financial Crimes Area task force to create a single law-enforcing entity at the federal level. The objective was to concentrate the enforcement at the federal, state, and local levels by creating geographical and industry-specific risk zones on which authorities could focus to facilitate monitoring.[29]

One of the most important acts introduced is the **U.S. PATRIOT ACT** of 2001, which aimed at disrupting any financing of terrorism that could be done through money laundering. This Act comprises over 150 sections, but Title III deals exclu-

---

26 Huang, J.H. (2015). Effectiveness of US anti-money laundering regulations and HSBC case study. Journal of Money Laundering Control, 18(4), 525-532.

27 Reyonlds, J. A. (2002). The New US Anti-Money Laundering Offensive: Will It Prove Successful?. Cross Cultural Management, 9(3), 3-31.

28 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

29 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

sively with anti-money laundering requirements. This act authorized information sharing between the U.S. government and financial institutions and set up a requirement for banks to share the information with a maximum deadline of 120 hours.[30] Furthermore, it imposed an obligation to identify a correspondent bank account, prohibited the use of some bank accounts, added penalties for no compliance, required financial institutions to establish comprehensive AML programs, and encouraged them to file a report on any suspicious account to inform the government.[31] The act also prohibited U.S. banks from engaging and conducting business with foreign shell banks and required them to set extensive due diligence procedures for account holders.[32]

The ***Intelligence Reform and Terrorism Prevention Act*** of 2004 amended the BSA to allow the Secretary of Treasury to require some financial institutions to report any cross-border electronic transmittal of funds to prevent the transfer of any funds to countries where a greater risk of terrorism is present.[33]

Finally, enacted in 2020, the **AMLA** created the beneficial ownership database. Before its enactment, there was no obligation for firms and financial institutions to report the identity of the beneficial owner of a company. That created a loophole in the regulatory system, which criminals could exploit by creating opaque firm structures to evade any reporting requirement. Beneficial owners were defined as people who directly or indirectly own and control 25% of an entity and who exercise control over it. Financial institutions are now required to provide the full legal name, the date of birth, the current residential or business address, and the unique identifying number of the beneficial owner.[34] The AMLA also broadened the powers of law enforcement entities by allowing them to subpoena any information on foreign banks with a banking relationship in the U.S.[35]

---

30 Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws.

31 Huang, J.H. (2015). Effectiveness of US anti-money laundering regulations and HSBC case study. Journal of Money Laundering Control, 18(4), 525-532.

32 Tomas, J. P. and Roppolo, W.P. (2019). Chapter 41 United States of America. In Srivastava, A. and Simpson, M. Richard Powell.; (Eds.), International Guide to Money Laundering Law and Practice (5th Ed. Pp. 1143-1496). Bloomsbury Publishing.

33 Lauman, A. (2019). The History of Anti-Money Laundering – Events, Regulations, and Adaptations in the United States [Online] Kroll. Available at: https://www.kroll.com/en/insights/publications/compliance-risk/history-anti-money-laundering-united-states.

34 Comply Advantage. A Guide to the US Anti-Money Laundering Act (AMLA). [Online] Available at: https://complyadvantage.com/insights/a-guide-to-the-us-anti-money-laundering-act-amla/#:~:text=The AMLA contains provisions prohibiting,fines, imprisonment, or forfeiture.

35 Comply Advantage. A Guide to the US Anti-Money Laundering Act (AMLA). [Online] Available at: https://complyadvantage.com/insights/a-guide-to-the-us-anti-money-launder-

As shown in this section, the enactment of compliance rules has been gradual and generally reflects a response to any new challenge that the U.S. government and financial institutions identified in the application of prior legislation. This has created a comprehensive body of law that aims to address all situations that may create a money laundering risk.

3. Supervision of AML compliance

Given the impressive body of law and the complexity of the U.S. system, several institutions are responsible for supervising the banking and financial sector and, more generally, for AML compliance. As a result, the U.S. supervisory structure is quite fragmented, given that several federal institutions are responsible for AML compliance and exist in parallel with state bodies that are also charged with AML supervision.[36]

The main regulator remains FinCEN, which is tasked with issuing, coordinating, and enforcing AML/CFT rules. FinCEN was created in 1990 to detect financial crimes and provide oversight and information to law enforcement. It effectively links law enforcement and the financial and regulatory communities.[37] Given the magnitude of its tasks, it has delegated some to other agencies and institutions.

There are four banking agencies that will primarily supervise the banking sector. These are the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC), the FDIC, and the National Credit Union Administration (NCUA). The objective of these four institutions is mainly to supervise the depository institutions' compliance with the BSA and OFAC obligations.[38] There are also two capital market agencies that were tasked by FinCEN to supervise the capital markets, and especially the securities and derivatives intermediaries. The two agencies tasked with such work are the Securities and Exchange Commission (SEC) and the Commodities Future Trading Commission (CFTC).

---

ing-act-amla/#:~:text=The AMLA contains provisions prohibiting,fines, imprisonment, or forfeiture.

36 Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml.

37 Reyonlds, J. A. (2002). The New US Anti-Money Laundering Offensive: Will It Prove Successful?. Cross Cultural Management, 9(3), 3-31.

38 Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml.

Finally, FinCEN delegated the supervision of small businesses and covered financial institutions not already supervised by the other agencies, such as MSBs, credit card companies, casinos, and precious metals and stones dealers, to the IRS.[39]

4. Assessment of AML compliance

The U.S. AML frameworks focus on applying the know-your-customer (KYC) and customer due diligence (CDD) principles. These principles are at the core of financial institutions' AML requirements, which seek to establish as much information as possible about an account and its holder to facilitate any future reporting and investigation in case of suspicion of money laundering.

Customer due diligence rests on four core requirements, which oblige banks and financial institutions to identify and verify the customer's information, to identify and verify the identity of the beneficial owner owning a stake of 25% or more in a given company, to monitor and suspicious transaction and to update regularly customer information and to understand the nature and purpose of compiling risks profiles for their customers.[40]

The U.S. Patriot Act sets forth the five pillars of any AML program to be set up in U.S. banks and financial institutions. This includes formulating adequate policies and procedures, the designation of a compliance officer, the presence of an independent audit, proper training for already employed staff, and customer due diligence.[41] These pillars address the internal corporate governance of a bank or financial institution and aim to establish a proper supervision system at the bank level.

Other requirements are set up in the BSA and directly apply to employees in the exercise of their functions. These take the form of suspicious activity reports and currency transaction reports, which allow institutions to identify potential money issues and create an obligation to inform the authorities of such risks. In the exercise of their functions, employees may be brought to file a Suspicious Activity Report (SAR) or a Currency Transaction Report (CTR)

---

39 Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml.

40 Kenton, W. (2024), Anti-Money Laundering (AML): What It Is, Its History, and How It Works. [Online] Investopedia. Available at: https://www.investopedia.com/terms/a/aml.asp#:~:text=Anti Money Laundering in the U.S.&text=Financial institutions were required to,and maintain records of transactions.

41 Public Law 107 – 56 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Section 352.

whenever a given situation requires it after meeting some requirements. A SAR must be filed whenever a suspicious activity has been identified. The term suspicious has not exactly been defined as what constitutes a suspicious action may vary from one geographical zone to another or from an industry sector to another, for example. Usually, a SAR will be filed whenever an alert is generated by a financial institution's computerized transaction monitoring system.[42] An SAR can be filed when a suspicious transaction reaches the $5.000 threshold. The SAR must be filed no later than 30 days after the alert rung.[43]

A currency transaction report (CRT) is a report which is to be filled by financial institutions for any transaction made which amounts to more than $10.000. In that regard, if the same person makes many smaller value transactions consecutively, they will be treated as one whole transaction for reporting purposes. Employees of financial institutions will generally have 15 days from the day of the transaction to fill out the report, and after filing, the report is to be kept for a minimum of 5 years after the account in question is closed.[44] Generally speaking, the filing of a CRT will not prevent a financial institution from filing a suspicious activity report.

D. Anti-money laundering in frameworks in the EU

1. Overview

In the EU as well, the AML regulation race was spurred by drug trafficking, which was discovered in the late 1970s and 80s.[45] However, contrary to the U.S., it did not give rise to the formulation of an AML regulation with a definite set of rules from the very beginning. When the first AML Directive became effective in 1991, the EU was not what it is today. In fact, at the time, it was still the European Community, with a much more limited harmonization than it has today and which has developed over the last 20 years. Accordingly, the AML framework was at the time more state-regulated than EU-regulated, which meant that each Member State (MS) had its own regulation, which would be

---

42 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress. p. 170.

43 Office of the comptroller of the Currency. Suspicious Activity Report (SAR) Program [Online] Available at: https://www.occ.treas.gov/publications-and-resources/forms/sar-program/index-sar-program.html.

44 Sullivan, K., (2015). Anti–Money Laundering in a Nutshell. Apress.

45 Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. computer law & security review, 33. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302060.

applied to the banks and financial institutions present on its territory. The 1st AMLD was greatly influenced by the 40 recommendations issued by the FATF in 1990.[46]

2. Evolution of AML frameworks

Just like in the U.S., the development of a comprehensive and, in this case, also harmonized AML approach was gradual, and each evolution built upon the previous one. The harmonization of the EU AML framework started in 1991 with the advent of the **1st *Anti-Money Laundering Directiv***e (AMLD). This directive was not purely regulatory in nature but served as a stepping stone for MS to start taking money laundering seriously. Notably, the AMLD recognized that an international approach was vital for the fight against drug trafficking.[47] The directive also criminalized money laundering in compliance with the FATF 40 Recommendations published in 1990. The scope of the Directive remained fairly narrow as it only concerned banks and required MS to simply make sure that they would apply proper KYC and CDD standards. The 1st AMLD was also influenced by the BSA given that it required banks to monitor the activity of its clients to make sure the transactions made were compliant and established an obligation to identify any suspicious transaction to report them to their corresponding national authorities.[48]

The **2nd AMLD**, which came into effect in 2001, amended the first directive to broaden the scope of the term "obligated entities" to include a larger range of activities.[49] Although this directive came out in 2001, it was however not a direct response to the 9/11 terror attack as it had been already formulated before. It was the **3rd AMLD**, which became effective as of 2005 and directly tackled terror financing. This directive introduced the risk-based approach, just like in the U.S. Accordingly, financial institutions could adapt their CDD

---

46 Comply Advantage. (2020). History of Anti Money Laundering Directive: A Summary – Part One. [Online]. Available at: https://complyadvantage.com/insights/brief-history-amlds-part-one/.

47 Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.

48 Comply Advantage. (2020). History of Anti Money Laundering Directive: A Summary – Part One. [Online]. Available at: https://complyadvantage.com/insights/brief-history-amlds-part-one/.

49 Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering. Art. 1(1)(B).

standards based on the risks created by the person or entity in question.[50] Depending on the degree of risk, the financial institution would apply regular due diligence obligations or enhanced CDD obligations. A novelty that this directive introduced was the penalty, which had to be now applied after an AML breach had been noticed. Although applying the penalty became mandatory, the amount was to be decided at the MS's discretion.[51]

In 2013, a new directive was proposed, which became the **4th AMLD** in 2015. This directive was a response to the new FATF recommendation, which required the revision of CDD requirements, the establishment of a central beneficial ownership register, and the application of enhanced due diligence on politically exposed people. As a result, the 4th AMLD required the identification of any ultimate beneficiary holding 25% or more of a given entity.[52] The AMLD also required improved monitoring and reporting standards for risky transactions and investment decisions. In fact, the reporting standard was lowered to include more entities and businesses to be covered by the CDD requirements. Moreover, the 4th AMLD introduced a heavy penalty for financial institutions in case of AML violations, such as the withdrawal of the operating license and a fine that may go up to €5 Million.[53] Despite its efforts, the 4th AMLD was difficult for countries to transpose and especially costly for some financial institutions.[54]

In 2018, or only one year after the transposition deadline for the 4th AMLD, the **5th AMLD** came into force. This directive was a direct response to the terror attacks that had taken place in the prior years and introduced, for example, a

---

50 Directive 2005/60/Ec Of The European Parliament And Of The COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Recital 10.

51 Directive 2005/60/Ec Of The European Parliament And Of The COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing .Arts. 13 and 39.

52 Directive (EU) 2015/849 Of The European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Art. 30.

53 Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. computer law & security review, 33. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302060.

54 Premti, A. and Jafarinejad, M. and Balani, H. (2021). The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks. Research in International Business and Finance, 57. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531921000180#:~:text=After examining the effect of,the beta of EU banks.

reduction in prepaid card limits, which was used in the case of the Bataclan attack. This directive also introduced cryptocurrencies to the regulated field.[55]

3. Supervision of AML compliance

Unlike the U.S., the organization of the European supervisory authorities is less chaotic and avoids the creation of any overlap in jurisdiction and regulation. In fact, as mentioned previously, the EU regulatory framework is based in the case of AML regulation on a harmonization-predominant path. This means that all countries will be applying the same minimum standards. However, the specific implementation is left to individual MS. Each MS has a supervision authority charged with correctly implementing and supervising money laundering regulations. Accordingly, each MS will have its own transposition of the Directive and create different rules based on the needs observed in their respective financial sector. Despite this lack of maximum harmonization, which in the case of AML would be sorely needed, MSs still apply rather similar rules and strive jointly for a better implementation of AML measures.

4. Assessment of AML compliance

Only in the EU 60% of bank fines in recent years were levied for violating AML standards.[56] The 4th and the 5th AMLD introduced new requirements for banks and financial institutions to abide by. They are now required to improve the monitoring and reporting standards for risky decisions and must identify and provide information on the ultimate beneficial owner of a financial transaction to a central register that is readily accessible.[57] Many financial institutions were struggling with implementing the requirements set up by the EU, which could explain the high number of fines being levied in recent years. Many of the requirements set up by the 4th AMLD were, moreover, already being implemented by financial institutions before it was enforced, which made it slightly redundant. The requirements also introduced inequalities in compliance given that very big banks and financial institutions had the means to comply with the

---

55 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), Recitals 8, 10 and 14.

56 Premti, A. and Jafarinejad, M. and Balani, H. (2021). The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks. Research in International Business and Finance, 57. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531921000180#:~:text=After examining the effect of,the beta of EU banks.

57 Ramalho, D. S. and ·Matos, I.N. (2021). What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. ERA Forum, 22, 487–506.

new requirements, which generated considerable costs, while smaller banks were not able to come into compliance at the same speed and at the same degree due to a lack of funds. The requirement to identify the beneficial owner was a response to the growing trend of setting up highly opaque corporate structures, which allowed criminals to benefit from their criminal proceeds without encountering any issue.

The 4th AMLD does not address cryptocurrencies or digital assets. However, the 5th AMLD did introduce some requirements upon firms operating centralized crypto exchanges or custodial wallets. Accordingly, Member States will now have to apply the same obligations imposed on banks and financial institutions to these firms. This means the CIP, beneficial ownership identification, KYC, transaction monitoring, and suspicious activity report requirements will now also be applicable.[58]

[58] Holman, D, and Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency [Online] A&O Shearman Available at: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.allenovery.com/global/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenovery.pdf?la=en-gb&hash=6D8F26DB73634846A427983AD2F217A7&ved=2ahUKEwjD8czemtSGAxWtm_0HHTQBAjoQFnoECBMQAQ&usg=AOvVaw2LvA9mynMG6eJGFcjHKuTP.

III. Virtual currencies and digital assets

A. Digital assets and cryptocurrencies

1. Definition and classification

Digital assets designate all assets that can be stored digitally and used to designate images, music, or documents that were stored digitally. Nowadays, the term digital asset refers to anything that is created and stored digitally and that can be traded based on its value, whether tangible or intangible.[59] The FATF defined virtual assets as: "any digital representation of value that can be digitally traded, transferred or used for payment. It does not include digital representation of fiat currencies."[60]

Cryptocurrencies and crypto assets are a subset of digital assets that distinguish themselves from regular digital assets by using cryptography to secure transactions. This means that the currency in question will be enciphered in a secret code, ensuring the privacy and anonymity of the transactions. Cryptocurrencies are decentralized in nature, which distinguishes them from traditional fiat currencies issued by governments. As a result, all cryptocurrencies have no central entity governing them; instead, they are peer-to-peer systems.

There are three types of virtual currencies. The first type is a closed-system virtual currency, which cannot be obtained or exchanged through legal tender. The second type of virtual currency is unidirectional, meaning it can be purchased through legal tender, but it cannot be exchanged back. An example of this type of currency would be Amazon coins. Finally, bi-directional virtual currency may be obtained through legal tender and exchanged back into legal tender. A perfect example in this case would be a cryptocurrency like Bitcoin. The first and second types of virtual currencies pose close to no risk of money laundering; however, the third type is the one that poses the most risks in terms of money laundering and is the hardest to regulate.[61]

---

59 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

60 Renda, A. and Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. Journal of Money Laundering Control, 27(2), 363-382. [Online] Available at: https://www.emerald.com/insight/1368-5201.htm.

61 Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. computer law & security review, 33. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302060.

Cryptocurrencies can be traded through exchanges where users can buy and sell cryptocurrencies like bitcoins for fiat currencies. There are two types of exchange platforms: centralized and decentralized. Centralized platforms will generally involve platforms with a central authority managing the transactions. To use these platforms, users first have to register and go through verification processes. Decentralized platforms will be peer-to-peer and allow users to trade directly with other users without having to go through any verification process.[62]

Bitcoin, the most well-known cryptocurrency, was created in 2009 by Satoshi Nakamoto, a pseudonym whose real identity still remains unknown. It can best be described as a peer-to-peer electronic cash payment system that allows a payment to be sent directly and anonymously without going through a financial institution like a bank. Bitcoins can be obtained through mining or purchase and exchange. Bitcoins are created and added to blockchains through mining. This means that the miner, with some extremely powerful hardware, will try to resolve a mathematical problem, and the first one who solves the problem is awarded the found Bitcoins. Mining has, however, become increasingly difficult as the complexity of the mathematical problems to solve has risen due to the high number of people who mine them. As a result, miners can no longer work alone but work instead in groups to solve the mathematical problem. The complexity of the mathematical problems rises in parallel with the rising scarcity of bitcoins, given that there are only 21 million bitcoins, and once they have all been mined, they will only be available through purchase and trade.[63]

2. Characteristics and functionalities

Several characteristics differentiate cryptocurrencies from fiat currencies. The main characteristics and functionalities will be presented here. The first and one of the most important differences from fiat currencies comes through its decentralized nature. In fact, cryptocurrencies do not operate around a bank, financial institution, or other authority but are instead peer-to-peer currencies that operate on a global network of computers.[64] Secondly, and

---

62 Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. International Journal of Law and Information Technolog, 29, 332–363.

63 Moreno, S. and Seigneur, J. M. and ; Gotzev, G. (2021). A Survey of KYC/AML for Cryptocurrencies Transactions. In: Handbook of research on cyber crime and information privacy. [Online] Available at: https://archive-ouverte.unige.ch/unige:150576.

64 Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. International Journal of Law and Information Technolog, 29, 332–363..

contrary to belief, cryptocurrencies are rather transparent given that all transactions made with cryptocurrencies are automatically encrypted on a blockchain, which operates as a sort of public ledger. As a result, everyone can access information such as the transaction's origin, amount, and destination.[65] However, despite this transparency, cryptocurrencies remain largely private as the identities of the actors participating in the transaction are anonymous. The parties and all the account holders use pseudonyms instead of their real identities to shield themselves from any potential attack.[66] Because cryptocurrencies are encrypted, it is incredibly difficult for an account to be hacked, thereby guaranteeing a high level of security, which cannot always be guaranteed by banks and financial institutions. The transactions, once done, are also immutable and irreversible unless you make a new transaction. This makes any type of fraud or double transaction difficult, if not impossible.[67] Importantly, cryptocurrencies are completely fungible, which makes the use of mixers and tumblers very useful.

Passing onto the main functionalities of cryptocurrencies, some similarities and differences appear compared to fiat currencies. Firstly, cryptocurrencies serve as a medium of exchange as they can be used to buy goods and services. Moreover, and more importantly, they are used to store value and as an investment medium. Bitcoins, more particularly, are used as a way to store value and to make a safe investment. The hope is that the value of cryptocurrencies will increase over time, making an exchange back to fiat currencies through sale very fruitful. Cryptocurrencies are also often used to make global transactions due to their rapidity and anonymity.

3. Overview of regulatory approaches

The Internet has given criminals a high degree of flexibility, making cybercrime a global phenomenon. The use of the Internet and the advent of new technologies have allowed new forms of payment, such as cryptocurrencies,

---

65 Hafke, L. and Fromberger, M. and Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the short comings of the fifth AML Directive (EU) and how to address them, Journal of Banking Regulation 21, 124-138.

66 Shaneav, S. and Sharma, S. and Ghimire, B. and Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market research in International Business and Finance, 51. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531919305963.

67 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

to be used.[68] Nearly all transactions that are made on the dark market/web are done in cryptocurrencies. This allows users to effectively hide their origin with the help of mixers, chain hopping, privacy coins, and anonymous peer-to-peer exchanges, which will be explained further in the next part.[69] Because of this, 46% of the transactions made with Bitcoins are made in the context of illegal activities.[70] This makes Bitcoin the only currency used on the darknet.[71]

Regulating cryptocurrencies in the context of money laundering has now become a paramount objective globally. Nevertheless, given their globalized and decentralized nature, regulating them is proving to be difficult, making them perfect vehicles for laundering money. If regulation exists, its implementation by the obliged entities is extremely difficult.

Only in the U.S. was the cryptocurrency industry fined over $5.8 billion over insufficient AML programs. According to the Financial Times, these fines were imposed due to violations of the BSA, substantial security shortcomings, not registering as a money-transmitting business, not conducting proper CDD procedures, and failing to uphold sanctions.[72] The main issue when it comes to cryptocurrency firms is the ambiguity of the regulations. Many firms dealing with cryptocurrencies are persuaded that such AML obligations do not apply to them, leading them to not properly apply the CDD procedures and not file any STR to the authorities.[73]

---

68 Oldrich, M. and Mc Ewen, G. (2019), Innovations in Law Enforcement – Implications for practice, education and civil society (Special Conference Edition). [Online] CEPOL. Available at: http://bulletin.cepol.europa.eu/index.php/bulletin/article/view/355/300.

69 Moreno, S. and Seigneur, J. M. and ; Gotzev, G. (2021). A Survey of KYC/AML for Cryptocurrencies Transactions. In: Handbook of research on cyber crime and information privacy. [Online] Available at: https://archive-ouverte.unige.ch/unige:150576.

70 Shaneav, S. and Sharma, S. and Ghimire, B. and Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market research in International Business and Finance, 51. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531919305963.

71 Kenton, W. (2024), Anti-Money Laundering (AML): What It Is, Its History, and How It Works. [Online] Investopedia. Available at: https://www.investopedia.com/terms/a/aml.asp#:~:text=Anti Money Laundering in the U.S.&text=Financial institutions were required to,and maintain records of transactions.

72 Comply Advantage. (2024). The biggest AML fines in 2023). [Online] Available at: https://complyadvantage.com/insights/aml-fines-2023/.

73 Holman, D, and Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency [Online] A&O Shearman Available at: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.allenovery.com/global/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenovery.pdf?la=en-gb&hash=6D8F26DB73634846A427983AD2F217A7&ved=2ahUKEwjD8czemtSGAxWtm_0HHTQBAjoQFnoECBMQAQ&usg=AOvVaw2LvA9mynMG6eJGFcjHKuTP.

B. Digital technologies

1. Artificial Intelligence

In the past few years, the market for AI has increased exponentially, with an estimated market value of $202.57 billion in 2026.[74] It has now become one of the most researched and lucrative fields, used in everything from education to medicine, law, and even regulatory purposes.

AI is science mimicking human thinking abilities to perform tasks typically requiring human intelligence. AI, just like a person, can recognize recurring patterns and can make predictions, recommendations, and decisions based on such recognized patterns. AI typically uses computational techniques to automatically solve problems and execute tasks in a fraction of the time required by a person to perform such a task. AI can have different levels of autonomy based on the algorithm on which it is based.[75]

Machine learning is a subset of AI that trains computer systems to learn from data to identify patterns and make decisions with minimal intervention by humans. Machine learning will generally design a sequence of actions to solve a problem automatically through experience and through evolving pattern recognition algorithms. Machine learning distinguishes itself with its ability to learn from past actions, which reduces the need for manual input to monitor its actions. This ability to learn from past successes or mistakes reduces the recurrence of false positives. Its adaptability and learning ability allow machine learning to identify any anomalies and duplicates of information to improve its data quality and analysis. For example, deep learning, a type of machine learning, is based on algorithms that are inspired by the working of the human brain and which, when performing a task several times, will at each repetition make a little modification to improve the outcome sought which effectively renders human intervention obsolete. Because of its qualities, it is increasingly being issued to monitor accounts and undertake a proper KYC and CDD. Moreover, machine learning and other AI-based tools allow for real-time, quick, and more

---

74 Fortune business insights. (2024). Artificial Intelligence Market. [Online]. Available at: https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-market-100114.

75 FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities And Challenges Of New Technologies For Aml/Cft&ie=UTF-8&oe=UTF-8.

accurate data analysis, which offers an alternative way of identifying risks in potential bank customers and transactions.[76]

2. Blockchain

Another type of technology that has seen a rise in popularity in these past years is blockchain. First introduced in 2009 with the creation of Bitcoin, it has now become a widely used technology beyond the cryptocurrency sphere. Blockchain functions as a payment mechanism that facilitates an open and transparent financial system accessible to all individuals without relying on a central body.[77]

At its core, a blockchain is a series of blocks, each containing chronological transaction records, which makes it a type of distributed ledger.[78] Each block thus created is immutable and secured through cryptogenic techniques. Because blockchains, like bitcoins, are decentralized, they cannot be controlled by a single entity.

Blockchain functioning can be divided into three steps. In the first step, a user broadcasts to a network of computers that it has initiated a transaction, which is more commonly referred to as "nodes". Secondly, the nodes will validate the transaction using a proof of work mechanism like for bitcoins.[79] During this step, miners must solve a mathematical problem to validate the transaction and then add it to the blockchain. Finally, once the transaction is validated, it is added to other transactions in a block after all nodes have agreed to its validity.[80]

---

76 FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities And Challenges Of New Technologies For Aml/Cft&ie=UTF-8&oe=UTF-8.

77 Renda, A. and Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. Journal of Money Laundering Control, 27(2), 363-382. [Online] Available at: https://www.emerald.com/insight/1368-5201.htm.

78 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

79 Robby Houben, R. and Snyers, A. (2018). Cryptocurrencies and Blockchain, Legal context and implications for financial crime, money laundering and tax evasion [Online] European Commission. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf.

80 World Bank Group. (2017). Distributed Ledger Technology (DLT) and Blockchain. [Online]. Available at: https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

Blockchains are public but are based on pseudonyms, which makes the identification of the beneficiary easier and harder at the same time. Blockchain analysis and monitoring tools enable financial institutions and law enforcement to identify and investigate suspicious crypto transactions.[81] This makes blockchain an invaluable tool in the fight against money laundering, given that it allows direct access to transaction lists as well as the origin, destination, and amount of the transaction. The only hurdle that needs to be overcome is the de-encryption of the user's pseudonyms.

C. Risks and illustrations of money laundering through cryptocurrencies

1. Money laundering risks

After the pandemic, crypto crime has reached an all-time high, with the illicit volume of crypto assets reaching $20.6 billion. During the pandemic, criminals were able to bypass control and compliance mechanisms set up by banks, a trend that has also continued after the end of the pandemic. For this reason, money laundering, especially through crypto services, has become one of the most important crime threats globally.[82]

In a DELPHI study, several criminogenic features were identified that make cryptocurrencies a great risk for AML efforts. In this study, professionals determined that the anonymity, decentralizations, diversity of exploitable actors or entities available to spread across risks, and the exceptionally low cost of exploiting such risks created considerable challenges for regulating cryptocurrencies with an AML objective.[83] Several risks were identified for users, market, investors, and service providers.[84] These risks originated from the

---

81 Kenton, W. (2024), Anti-Money Laundering (AML): What It Is, Its History, and How It Works. [Online] Investopedia. Available at: https://www.investopedia.com/terms/a/aml.asp#:~:text=Anti Money Laundering in the U.S.&text=Financial institutions were required to,and maintain records of transactions.

82 Renda, A. and Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. Journal of Money Laundering Control, 27(2), 363-382. [Online] Available at: https://www.emerald.com/insight/1368-5201.htm.

83 Akartuna, E. A. and Johnson, S. D. and Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting & Social Change, 19. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0040162522001640?via=ihub.

84 Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. computer law & security review, 33. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302060.

volatility of the cryptocurrency value as well as from the pseudonymization of the wallet holders. This makes illicit transactions considerably harder to distinguish, which makes, in turn, the value of such currencies extremely volatile as well, making these two characteristics intrinsically linked.[85] Because of the volatility of cryptocurrencies, it is also extremely easy to justify unexpected wealth growth, given that exchange rates can evolve incredibly quickly due to unexpected circumstances or declarations that can influence their market value.[86]

Because cryptocurrencies and blockchain are completely transparent and accessible by everyone, some services may be used to obfuscate the trail of cryptocurrencies, making it harder for both law enforcement agencies and hackers to identify and situate a transaction. One such service offered is Tumbler (or Mixer) Services. Tumbling services are software that will be used to break down cryptocurrency transactions into small parts, known as fragments, to mix them up with other transactions and coins, both of licit and illicit nature, to send them to the final customer. The customer will then receive the same number of coins sent to be tumbled, but the coins will now originate from completely different wallets. Such services are not necessarily malicious and illegal as Tumblers will be used for two reasons: to prevent hackers from accessing a wallet and to subtract coins and for law enforcement not to be able to follow the trail of coins.[87]

Crypto dusting makes tracing cryptocurrency even more difficult. In this case, Bitcoin users are sent minuscule amounts of crypto tokens with very little monetary value and a message promoting the tumbler's activities[88]. Crypto dusters will generally take advantage of the transparency and accessibility of blockchains and will strategically send small amounts of cryptocurrency to specific wallets.[89] By dusting wallet addresses with these small amounts of

---

85 Akartuna, E. A. and Johnson, S. D. and Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting & Social Change, 19. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0040162522001640?via=ihub.

86 United Nations Toolkit on synthetic drugs. Money Laundering Methods. [Online] United Nations. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html.

87 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

88 Hafke, L. and Fromberger, M. and Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the short comings of the fifth AML Directive (EU) and how to address them, Journal of Banking Regulation 21, 124-138.

89 Blockchain Intelligence group. (2024) Crypto Dusting Attack – What You Need To Know. [Online] Available at: https://blockchaingroup.io/crypto-dusting-attack-what-you-need-to-know/.

cryptocurrencies, dusters seek to confuse authorities and hackers by creating a multitude of minuscule trails, making following the trail of suspected money laundering harder.

Traditional AML frameworks are designed for centralized financial institutions. However, cryptocurrencies, especially Bitcoin, are decentralized, which makes traditional AML frameworks inadequate to deal with the challenges brought forth by cryptocurrencies. Traditional AML frameworks focus especially on the determination of the beneficial owner and on the origin of the money to determine whether the money is being laundered or not. However, it is extremely difficult to retrieve this information given the absence of a central authority that supervises cryptocurrency, which can require the communication of said information. Moreover, cryptocurrencies being largely pseudonymized prevents the determination of the origin and identity of the wallet owner.

2. Illustrations

The most notable case that led law enforcement and regulatory authorities to target cryptocurrencies is the *Silk Road* case. This case concerns an online black market website on which one could buy drugs, arms, hitmen, and many more illegal and criminal goods and services. This website was launched by Ross Ulbricht in 2011, who also used the pseudonym "Dread Pirate Roberts". This website quickly gained popularity due to its Bitcoin-only payment policy, which ensured the complete anonymity of its users. The first anonymization step occurred through the use of the Tor network to access the website, which made tracking its user's server location quite difficult. During that time, Bitcoins' value rose considerably, partly because of the attention Bitcoins received due to Silk Road. However, this increased media attention also attracted the attention of the U.S. Government, which made it its mission to track, shut down the site and arrest Ulbricht. The government began to open accounts on Silk Road to monitor its activities and created a fake identity on the website. During its downfall, Ulbricht also contacted several hitmen in order to eliminate people who, in his opinion, were endangering the existence of his website. Payment for such services was made solely in bitcoins. On October 1st 2013, Ulbricht was arrested in a library, and Silk Road was consequently shut down by the U.S. Government authorities. Immediately after the site shut down, the value of Bitcoin dropped from $140 per Bitcoin to $110. This case showed that Bitcoins could have a double purpose. On the one hand, it became clear that criminals could use Bitcoins to try and hide their illicit proceeds. On

the other hand, however, it also showed to law enforcement authorities that the very nature of Bitcoins, and blockchain in general, was an invaluable tool to track illegal transactions.[90]

In 2015, Ulbricht was sentenced to life in prison for money laundering, computer hacking, and conspiracy to traffic narcotics.[91] This case was a perfect example of the challenges that cryptocurrencies may create when fighting crime.

However, the Silk Road case was not the only instance that led to an arrest or website shutdown. There are currently five most popular methods criminals use for laundering funds on the blockchain. Criminals will generally use nested services such as the Lazarus project; they will use gambling platforms on which payments via cryptocurrencies are allowed; they will use mixers such as chip mixer and tornado cash, and will use fiat exchange platforms and pay-for services headquartered in high-risk jurisdictions that also have strong bank secrecy regulation.[92]

More recently, in 2019, Europol, working with the Dutch Financial Crime Investigative Service, shut off a website providing mixing services called Bestmixer.io. Investigations had, in fact, revealed that around 27.000 Bitcoins, all originating from criminal activities and destined for criminal's wallets, had been mixed.[93] Another instance of tumbler services being shut down occurred in 2020 when the U.S. Department of Justice charged a person for the operation of a tumbler associated with a Darknet market called Helix. In 2021, the same department pursued a person who had been associated with a very popular mixer, Bitcoin Fog.[94]

These cases illustrate the dangers created not only by the use of Bitcoins but also by its associated services, such as mixers, which are currently being used to hide the illegal origin of coins and their destinations.

---

90 Adler, D. (2018). Silk Road: The Dark Side of Cryptocurrency. Fordham Journal of Corporate and Financial Law. [Online] Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/.

91 U.S. Immigration and Customs Enforcement. (2015). Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website. [Online] Available at: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating.

92 Grau, D. (2023). What Law Enforcement Needs to Know About Crypto Money Laundering. [Online] Cognyte. Available at: https://www.cognyte.com/blog/anti-money-laundering-cryptocurrency/.

93 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

94 Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

IV. New developments in Anti Money Laundering

A. Legislative solutions

1. The U.S.

Given the several risks that have been previously identified, it is relevant to inquire how they are being addressed by the U.S. government. The U.S. is pursuing a very aggressive campaign against cryptocurrencies and all associated services. The efforts have notably intensified after one of the largest crypto exchange firms in the U.S., FTX, filed for bankruptcy in 2022.[95]

The AMLA had already expanded the scope of the BSA by making businesses that trade in non-traditional value subject to the BSA. Cryptocurrencies, capable of holding value and exchangeable, are now subject to registration and compliance requirements set in the BSA. As a result, cryptocurrency exchanges are now required to register as money services businesses and comply with AML requirements.[96]

In the U.S., several regulations currently address cryptocurrency based on whether it is considered a currency, a security or a commodity. As a result, overlapping regulatory regimes address the same type of product. This inconsistency will, however, be addressed by the ***Lummis-Gillibrand Responsible Financial Innovation Act*** (RFIA). This act was first introduced in 2022 and reintroduced with some modifications in 2023. It is still being reviewed and has not yet been approved by the Senate. However, if this Act is approved, it will introduce several changes to the cryptocurrency industry. Notably, it will define several important items such as digital assets, digital assets intermediary, distributed ledger technology, payment stablecoins, and smart contracts.[97] The aim is to remove any ambiguity that may exist on both law enforcement and providers' or users' sides. Importantly, virtual currencies will be considered commodities, which would make the CFTC the sole authority that would have jurisdiction over any matter arising from them. An intangible and fungible dig-

---

95 Renda, A. and Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. Journal of Money Laundering Control, 27(2), 363-382. [Online] Available at: https://www.emerald.com/insight/1368-5201.htm.

96 Congressional Research Service. The Financial Crimes Enforcement Network (FinCEN): Anti-Money Laundering Act of 2020 Implementation and Beyond (2022). [Online]. Available at: https://crsreports.congress.gov/product/pdf/R/R47255.

97 Lummis-Gillibrand Responsible Financial Innovation Act, Section 101. Definitions.

ital asset would be considered an "ancillary asset", and its issuers would have to comply with some disclosure requirements, such as the disclosure of basic corporate information concerning the issuer and the information regarding the ancillary asset itself.[98] A loophole, however, remains given that once an ancillary asset reaches a certain level of decentralization, the issuer would escape the disclosure requirements while retaining the commodity status.[99]

The aim of the legislation is to introduce more transparency by taking out the pseudonymization currently benefitting cryptocurrencies.

2. The EU

The 4th AMLD did not address cryptocurrencies specifically. In 2015, however, the EU formulated an extensive regulatory package that aimed to address money laundering and planned several legislations that should aid in the pursuit of the fight against money laundering. The legislations are the following: the 5th AMLD and its subsequent amendment, the 6th AMLD, the Traceability of Transfer of Funds Regulation (TFR), the Markets and Crypto Assets Regulation (MiCA) and the Anti Money Laundering Authority Regulation (AMLA). These legislations were formulated to tackle all aspects of money laundering and to create a homogenous and incorporated approach that is EU-wide.

The 5th AMLD, launched in 2016, clearly and definitely included cryptocurrency in its scope of application. First, the 5th AMLD clearly defined virtual currency exchange platforms and custodian wallet providers as obliged entities, which means they are now required to undertake CDD when they exchange virtual currencies for fiat currencies.[100] Moreover, when establishing a business relationship or carrying out a transaction, they will not have to verify the identity of their customers, just like other obliged entities. This aims to end the anonymity typically associated with these types of exchanges.[101] The 5th AMLD also proposed a clear definition for the term "virtual currency" whereby they are a "digital representation of value that is neither issued by a central

98 Lummis-Gillibrand Responsible Financial Innovation Act, Section 41. Securities Offerings Involving Certain Intangible Assets.

99 Arciniegas, J. and Conner, W. T. (2022). The investment lawyer, 29(10), 9-18.

100 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Art. 1.

101 Godinho Silva, P. (2019). Recent developments in EU legislation on anti-money laundering and terrorist financing. New Journal of European Criminal Law, 10(1), 57-67.

bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically".[102]

Under the 5th AMLD, there are now five conditions that determine whether a currency is covered by the AMLD obligations. Firstly, they must not represent a digital value issued by a public authority. Secondly, any representation of value which holds the legal status of currency or money is not a virtual currency. This would effectively remove the digital euro from its scope. Thirdly, tokens do not need to be legally established. Fourth, and passing onto positive requirements, virtual currency needs to be able to be transferred, stored, and traded electronically. Finally, it must be accepted by natural or legal people as a means of exchange.[103] It is clear from this that the term "virtual currency" seeks to encompass as many types of tokens as possible.

The TFR, enforced in 2023, seeks to establish the information of payers and payees by ensuring that the transfer of funds is accompanied by the name of the payer, the payer's account number, its address, its date of birth and customer identification number, the name of the payee and its account number.[104] The main issue of the TFR, however, is that the definition of "funds" did not include cryptocurrencies.[105] The TFR, as amended in June 2023 and will become applicable on the 30th of December 2024, will extend the provision of information to virtual asset service providers and crypto-to-crypto transactions.[106] This will ensure the full traceability of crypto asset transfers and the identification of their holders. The FTR will then require that information on the asset's source and beneficiary of the transaction be included in the transaction.

---

102 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), Art. 1(2)(d).

103 Hafke, L. and Fromberger, M. and Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the short comings of the fifth AML Directive (EU) and how to address them, Journal of Banking Regulation 21, 124-138.

104 Regulation (EU) 2023/1113 Of The European Parliament And Of The Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849. Art. 4.

105 Robby Houben, R. and Snyers, A. (2018). Cryptocurrencies and Blockchain, Legal context and implications for financial crime, money laundering and tax evasion [Online] European Commission. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf.

106 Kaiser, R. (2024). Compliance requirements in the future EU Anti-Money Laundering and Countering the Financing of Terrorism Framework. Journal of Payments Strategy & Systems, 18(1), 20-29.

MiCA, also enforced in 2023, aims to introduce homogenous EU market rules for crypto assets and will cover all crypto assets not currently covered by other types of regulations.[107] The aim of this regulation is to introduce transparency and disclosure requirements for all entities issues crypto-currencies.[108]

B. Implications

The two regulatory initiatives undertaken by both the EU and the U.S. are quite extensive in nature and would allow for better transparency, customer protection, and fewer instances of money laundering through cryptocurrencies. They aim to achieve that by imposing information disclosure requirements for virtual currency exchange platforms and custodian wallet providers. As a result, for all transactions made through these two types of service providers, anonymity would be stripped, leaving the wallet holders vulnerable to attacks.

Despite these two service providers being covered by several legislations, mixers, miners, coin traders, and currency-to-currency exchanges are not covered. This might be a mistake. In fact, it can be argued that the highest risk in terms of cryptocurrency does not arise when a currency is being exchanged for fiat currency or when a private access key is being stored by a custodian wallet provider. Instead, the biggest risks arise when coins are mixed to hide their origin. This makes any tracking impossible, while transactions that are made through exchange platforms will actually be inscribed in a blockchain that is publicly accessible to everyone. Similarly, currency-to-currency exchanges might be done primarily to exchange coins obtained illegally for those obtained legally, thereby blurring the trail for law enforcement authorities.

Both the EU and the U.S. have adopted a strategy that is extensive but laid back at the same time. This is caused by the understanding that if they excessively regulate cryptocurrencies, criminals and users, in general, will switch to another instrument that can hold value, just like Bitcoins. In that respect, the possibilities are endless, as creating a cryptocurrency that would not be sub-

---

107 ESMA. Markets in Crypto-Assets Regulation (MiCA) [Online]. Available at: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

108 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. Art. 1.

ject to the requirements set in the AMLA, the RFIA of the 5th AMLD, is incredibly easy. A powerful approach would, as a result, be rather counterproductive as criminals would simply switch from one instrument to another.

It can also be argued that the increased focus on regulation may also be more counterproductive than one would like. By taking away the pseudonymity of wallet holders, the EU and the U.S. might push people to opt for a different type of transaction method, which, in the long term, would render the legislation useless. A point can be made that given that cryptocurrencies are transparent, there should be no need to regulate them to such an extent. As the Silk Road Case has shown, law enforcement agencies are more than capable of discovering the source and destination of a given transaction despite the use of pseudonyms.

Another question that remains open is the jurisdictional reach of such legislation. In fact, it seems unclear when a currency exchange must be registered. Is it to be registered if the person doing it is resident on European or American soil, or should the business have a physical presence in a given place? These businesses can be conducted primarily through a computer, and a fixed address is not absolutely necessary, given the digital nature of such an activity. One could, as a result, decide to move to a country that is not subject to such extensive AML requirements and which affords more secrecy protection.

One can also observe a slight switch from the risk-based approach to a rule-based one in the 5th AMLD. In fact, one can argue that the directives are taking a more rule-based approach by imposing several requirements for a virtual currency to be considered as one or by specifically defining which entities are to be considered obliged entities. This is not necessarily a bad thing as, in a way, it offers more legal certainty to the concerned obliged entities. The issue, in fact, was that many did not know they were obliged entities and that they had to comply with disclosure obligations. By defining with details who is subject to the directives and regulations, more chances are given to the service providers to actually be in line with their obligations, which in the long run will lead to more compliance and fewer AML violations.

C. Future strategies

1. Cooperations

During a recent FATF meeting, it was recognized that public law bodies working in cooperation with private bodies and civil societies have had a positive impact on the implementation of financial crime-fighting measures.[109] Through this increased collaboration, increased global cooperation has also been observed. In fact, due to their decentralized and global nature, cryptocurrencies tend to evade law enforcement and fall through the cracks. Indeed, while one state might regulate cryptocurrency in a certain way, another country will generally adopt a different legislative and regulatory approach. This allows criminals to choose the country that would be more beneficial in terms of money laundering ableism. For that reason, a global harmonized approach might actually be beneficial in the long term instead of having different pieces of legislation in every country.

Operating based on the FATF recommendations does allow for some minimum harmonization since it establishes key points to be addressed. However, how these points will be addressed on a state level will be different from one country to the other.

For that reason, the Egmont group was founded in 1995 to foster collaboration and information sharing between Financial Intelligence Units (FIUs). Currently, 174 FIUs are part of the Egmont Group, which allows countries to exchange important information regarding money laundering risks and suspected activities.[110]

2. The use of digital technologies

A few issues have been observed while enforcing both EU and U.S. regulations. Both the EU and the U.S. have formulated extensive and far-reaching regulations that require banks and financial institutions, as well as some cryptocurrency service providers, to put extensive measures in place. Of course, these measures are sorely needed to comply with all AML requirements, but they create considerable costs for these firms. The result is that they will often pre-

---

109 FATF (2024). Urgent action needed to fight money laundering and terrorist financing, say heads of FATF, INTERPOL and UNODC. [Online] Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-Call-to-action.html.

110 Egmont Group of financial intelligence units. [Online]. Available at: https://egmontgroup.org/#:~:text=The Egmont Group provides FIUs,financing, and associated predicate crimes.

fer being fined instead of complying with the unending requirements, as the fines are often cheaper than the costs generated through compliance. One could indeed say that the regulations in place have a quite counterproductive effect. One way of managing such risks would be to use the same technologies currently increasingly used by criminals to evade AML obligations, such as digital technologies like AI, blockchain, and machine learning.

Several non-negligible benefits exist from using digital technologies for AML purposes. For starters, their use would considerably lower the costs needed in manpower, which would indirectly and directly, through the application of the program, reduce human error. The AML protocols would be applied faster while lowering the occurrence of false positives. However, when applying such digital protocols based on algorithms, it would be difficult to apply a risk-based approach as these programs' algorithms need to be precise and list points to be checked when a money laundering risk arises, which would make them rather a rule-based, thus affording a higher level of legal certainty.[111]

The use of digital tech, also called regulatory tech or RegTech, would allow the supervision of numerous entities simultaneously, would identify and understand risks associated with different sectors in a heartbeat, and would be able to monitor compliance in real time. Data collected could be stored, processed, and reported on larger sets of supervisory data. By using blockchain as storage, for example, the exchange of information would be automatic and relatively easy, which would make the results of the monitoring more reliable and considerably easier to communicate.[112]

It can also be said that several disadvantages exist. The autonomation of the process would considerably reduce human oversight and create a risk of displacement based on the regulatory strategy adopted through the base algorithm.[113] Moreover, there would be a severe lack of transparency as access to such algorithms would not be available for everyone but only for those operating these RegTech instruments. Understanding this type of instrument is also not easy for everyone, which creates challenges when adopting them.

---

111 FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities And Challenges Of New Technologies For Aml/Cft&ie=UTF-8&oe=UTF-8.

112 FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities And Challenges Of New Technologies For Aml/Cft&ie=UTF-8&oe=UTF-8.

113 Akartuna, E. A. and Johnson, S. D. and Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting & Social Change, 19. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0040162522001640?via=ihub.

V. Conclusion

A. Summary of key findings

The aim of this paper was to highlight the risks created by the use of cryptocurrencies in the fight against money laundering the potential inadequacy of the traditional AML framework as well as the consequences of the new legislation. As already explained throughout this paper, a considerable amount of money and criminal proceeds are being laundered through the use of cryptocurrency, which makes the adaptation of the legal and regulatory framework essential.

Money laundering is a three-step process that starts with placement, continues with layering, and ends with integration. The techniques used for these purposes are potentially endless. However, American and European legislators have come up with complex procedures that aim to disrupt the placement, layering, and integration of illegally obtained proceeds. It was shown that both the American and European legislators did not come up with a definite body of law from the start but have both instead gone through a comparable evolution. It started in both cases in the 1970s and 1980s when money laundering was concerned mainly with tax-evading persons and businesses. The purpose of the regulations was thus to establish a paper trail that would allow law enforcement authorities to relocate the money being laundered as well as the perpetrators. In the 2000s, the focus switched to the fight against terrorism financing, which led to the requirement of extensive CDD and KYC procedures to be applied by the banks. The purpose of the first section was to present money laundering and how it is being fought by the authorities.

Moving onto the next part, it was necessary to thoroughly present cryptocurrencies, their characteristics, their functioning, how they are obtained, and how they can be traded or exchanged to highlight the shortcomings of traditional AML regulations. These become rather clear when going through such an explanation. Cryptocurrencies are decentralized, anonymous, scarce, and fungible. This makes the application of traditional AML regulation practically impossible. On the other hand, it was also necessary to point out that the same technologies used to launder money can be used to fight money laundering when properly mastered. This paper focused on AI, machine learning, and blockchain as they can make identifying money laundering instances easier and quicker, while blockchain, a ledger, makes following transactions relatively easy. Several money laundering risks were identified through the use of cryptocurrencies.

In the last part, new regulatory efforts were introduced to fight money laundering through the deanonymization of some service providers' and users' identities. Both the EU and the U.S. have formulated extensive legislation which seeks to take away the anonymization of cryptocurrencies. However, it is not clear whether that is a good strategy given that one can decide to stop using cryptocurrencies and switch to a different one, which would not be subject to regulation, as quickly as one created the user account in the first place.

B. Limitations of the study and avenues for further research

This paper was not able to determine with certainty what the impact of the different legislative innovations will be. The RFIA has not yet been approved, and some of the European legislation has not yet been fully implemented. It was in this case only possible to conjecture how these regulations may apply and their possible shortcoming. A future study enquiring into the definite changes that these regulations have brought to the cryptocurrency sphere would have to be undertaken in a few years once the effects can be quantified and analyzed.

C. Concluding remarks

Anti-money laundering regulations pursue a noble cause as they seek to not only stop the occurrence of money laundering but, by doing so, seek to tackle the underlying crimes committed in the first place. Money laundering will be undertaken to be able to use proceeds coming from criminal activities in the financial system once they have gone through the last step of the money laundering cycle. By allowing money laundering to take place, enforcement authorities would be sending the message that it is acceptable to commit crimes to obtain these proceeds in the first place. Criminals are generally motivated by greed and will pursue any means possible to make use of the money they have obtained illegally. Given the seemingly unlimited methods that one could use to launder money and especially the endless possibilities that criminals can create to launder money if a method is not as effective, a balance needs to be struck in the realm of cryptocurrency anti-money laundering. On the one hand, one must want to tackle money laundering done through cryptocurrencies; however, excessive regulation will have one effect only: criminals will switch to a different method to launder money digitally. Moreover, by imposing exacting transparency requirements, it is not only criminals who will be deterred from using cryptocurrencies but the larger, non-criminal population. This could cause incredible losses to firms operating in the cryptocurrency field, which could potentially disrupt the wider financial scene.

VI. Bibliography

Adler, D. (2018). Silk Road: The Dark Side of Cryptocurrency. Fordham Journal of Corporate and Financial Law. [Online] Available at: https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Akartuna, E. A. and Johnson, S. D. and Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting & Social Change, 19. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0040162522001640?via%3Dihub

Arciniegas, J. and Conner, W. T. (2022). The investment lawyer, 29(10), 9-18.

Blockchain Intelligence group. (2024) Crypto Dusting Attack – What You Need To Know. [Online] Available at: https://blockchaingroup.io/crypto-dusting-attack-what-you-need-to-know/

Comply Advantage. (2020). History of Anti Money Laundering Directive: A Summary – Part One. [Online]. Available at: https://complyadvantage.com/insights/brief-history-amlds-part-one/

Comply Advantage. (2020). A Brief History of the AMLDs: Part Two. [Online]. Available at: https://complyadvantage.com/insights/brief-history-amlds-part-two/

Comply Advantage. (2024). The biggest AML fines in 2023). [Online] Available at: https://complyadvantage.com/insights/aml-fines-2023/

Comply Advantage. A Guide to the US Anti-Money Laundering Act (AMLA). [Online] Available at: https://complyadvantage.com/insights/a-guide-to-the-us-anti-money-laundering-act-amla/#:~:text=The%20AMLA%20contains%20provisions%20prohibiting,fines%2C%20imprisonment%2C%20or%20forfeiture

Congressional Research Service. The Financial Crimes Enforcement Network (FinCEN): Anti-Money Laundering Act of 2020 Implementation and Beyond (2022). [Online]. Available at: https://crsreports.congress.gov/product/pdf/R/R47255

Dill, A. (2021) Anti-Money Laundering Regulation and Compliance. [Online] ElgarOnline. Available at: https://china-elgaronlinecom.mu.idm.oclc.org/monochap/9781788974837.00009.xml

Egmont Group of financial intelligence units. [Online]. Available at: https://egmontgroup.org/#:~:text=The%20Egmont%20Group%20provides%20FIUs,financing%2C%20and%20associated%20predicate%20crimes.

ESMA. Markets in Crypto-Assets Regulation (MiCA) [Online]. Available at: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

European Commission, Money laundering [Online] Available at: https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/money-laundering_en

Europol, (2015). *Why is cash still king?*. [Online] Available at: https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf

Europol. Money laundering. [Online] Available at: https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering

Europol. Money laundering. [Online] Available at: https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering

FATF (2024). Urgent action needed to fight money laundering and terrorist financing, say heads of FATF, INTERPOL and UNODC. [Online] Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-Call-to-action.html

FATF, (2021). Opportunities And Challenges Of New Technologies For Aml/Cft. [Online] Available at: https://www.google.com/search?client=safari&rls=en&q=Opportunities+And+Challenges+Of+New+Technologies+For+Aml%2FCft&ie=UTF-8&oe=UTF-8

Financial Crimes Enforcement Network. History of Anti-Money Laundering Laws. [Online] Available at: https://www.fincen.gov/history-anti-money-laundering-laws

Fortune business insights. (2024). Artificial Intelligence Market. [Online]. Available at: https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-market-100114

Godinho Silva, P. (2019). Recent developments in EU legislation on anti-money laundering and terrorist financing. New Journal of European Criminal Law, 10(1), 57-67.

Grau, D. (2023). What Law Enforcement Needs to Know About Crypto Money Laundering. [Online] Cognyte. Available at: https://www.cognyte.com/blog/anti-money-laundering-cryptocurrency/

Hafke, L. and Fromberger, M. and Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the short comings of the fifth AML Directive (EU) and how to address them, Journal of Banking Regulation 21, 124-138.

Holman, D, and Stettner, B. (2018). Anti-Money Laundering Regulation of Cryptocurrency [Online] A&O Shearman Available at: https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.allenovery.com/global/-/media/sharepoint/publications/publications/en-gb/documents/aml18_allenovery.pdf%3Fla%3Den-gb%26hash%3D6D8F26DB73634846A427983AD2F217A7&ved=2ahUKEwjD8czemtSGAxWtm_0HHTQBAjoQFnoECBMQAQ&usg=AOvVaw2LvA9mynMG6eJGFcjHKuTP

Huang, J.H. (2015). Effectiveness of US anti-money laundering regulations and HSBC case study. Journal of Money Laundering Control, 18(4), 525-532.

Kaiser, R. (2024). Compliance requirements in the future EU Anti-Money Laundering and Countering the Financing of Terrorism Framework. Journal of Payments Strategy & Systems, 18(1), 20-29.

Kenton, W. (2024), Anti-Money Laundering (AML): What It Is, Its History, and How It Works. [Online] Investopedia. Available at: https://www.investopedia.com/terms/a/aml.asp#:~:text=Anti%20Money%20Laundering%20in%20the%20U.S.&text=Financial%20institutions%20were%20required%20to,and%20maintain%20records%20of%20transactions.

Lauman, A. (2019). The History of Anti-Money Laundering – Events, Regulations, and Adaptations in the United States [Online] Kroll. Available at: https://www.kroll.com/en/insights/publications/compliance-risk/history-anti-money-laundering-united-states

Moreno, S. and Seigneur, J. M. and ; Gotzev, G. (2021). A Survey of KYC/AML for Cryptocurrencies Transactions. In: Handbook of research on cyber crime and information privacy. [Online] Available at: https://archive-ouverte.unige.ch/unige:150576

Office of the comptroller of the Currency. Suspicious Activity Report (SAR) Program [Online] Available at: https://www.occ.treas.gov/publications-and-resources/forms/sar-program/index-sar-program.html

Oldrich, M. and Mc Ewen, G. (2019), Innovations in Law Enforcement – Implications for practice, education and civil society (Special Conference Edition). [Online] CEPOL. Available at: http://bulletin.cepol.europa.eu/index.php/bulletin/article/view/355/300

Premti, A. and Jafarinejad, M. and Balani, H. (2021). The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks. Research in International Business and Finance, 57. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531921000180#:~:text=After%20examining%20the%20effect%20of,the%20beta%20of%20EU%20banks.

Ramalho, D. S. and ·Matos, I.N. (2021). What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. ERA Forum, 22, 487–506.

Renda, A. and Caneppele, S. (2024). Compliant or not compliant? The challenges of anti-money laundering regulations in crypto assets: the case of Switzerland. Journal of Money Laundering Control, 27(2), 363-382. [Online] Available at: https://www.emerald.com/insight/1368-5201.htm

Reyonlds, J. A. (2002). The New US Anti-Money Laundering Offensive: Will It Prove Successful?. Cross Cultural Management, 9(3), 3-31.

Robby Houben, R. and Snyers, A. (2018). Cryptocurrencies and Blockchain, Legal context and implications for financial crime, money laundering and tax evasion [Online] European Commission. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf

Scharfman, J. (2022). Cryptocurrency Compliance and Operations, Digital Assets, Blockchain and DeFi. Palgrave MacMilan.

Schmidt, A. (2021). Virtual assets: compelling a new anti-money laundering and counter-terrorism financing regulatory model. International Journal of Law and Information Technolog, 29, 332–363.

Shaneav, S. and Sharma, S. and Ghimire, B. and Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market research in International Business and Finance, 51. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0275531919305963

Sullivan, K., (2015). *Anti–Money Laundering in a Nutshell.* Apress.

Tomas, J. P. and Roppolo, W.P. (2019). Chapter 41 United States of America. In Srivastava, A. and Simpson, M. Richard Powell.; (Eds.), International Guide to Money Laundering Law and Practice (5th Ed. Pp. 1143-1496). Bloomsbury Publishing.

U.S. Immigration and Customs Enforcement. (2015). Ross Ulbricht, aka Dread Pirate Roberts, sentenced to life in federal prison for creating, operating 'Silk Road' website. [Online] Available at: https://www.ice.gov/news/releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-life-federal-prison-creating

United Nations (2020) Tax abuse, money laundering and corruption plague global finance [Online] Available at: https://www.un.org/development/desa/en/news/financing/facti-interim-report.html

United Nations General Assembly (UNGA) United Nations Convention against Transnational Organized Crime (2001) UN Doc A/RES/55/25

United Nations Office on Drugs and Crime [Online] Available at: https://www.unodc.org/unodc/en/money-laundering/overview.html

United Nations Toolkit on synthetic drugs. Money Laundering Methods. [Online] United Nations. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/methods.html

United Nations Toolkit on synthetic drugs. Money Laundering Methods. [Online] United Nations. Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/moneylaundering.html

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. computer law & security review, 33. [Online] Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364916302060

World Bank Group. (2017). Distributed Ledger Technology (DLT) and Blockchain. [Online]. Available at: https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

VII. List of Legislation

Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

Directive (EU) 2015/849 Of The European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance).

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.

Directive 2005/60/Ec Of The European Parliament And Of The COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Lummis-Gillibrand Responsible Financial Innovation Act.

Public Law 107 – 56 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

Regulation (EU) 2023/1113 Of The European Parliament And Of The Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Next Generation

This thesis explores the growing challenges of combating money laundering in the face of emerging technologies like cryptocurrencies, artificial intelligence, and blockchain. It examines how traditional anti-money laundering (AML) frameworks in the U.S. and the EU struggle to address these challenges, particularly the anonymous and decentralized nature of digital currencies. By analyzing recent regulatory developments in both regions, the thesis aims to assess how effectively new measures target digitalized money laundering and whether they address the gaps in existing AML approaches.

Céline Carucci