e-ISSN 2281-6100

Ricerche giuridiche
Vol. 9 – Num. 2 – Dicembre 2020

Money Mules and Tumblers
Money Laundering During the Cryptocurrency Era

Sofia Del Monaco
Dottoressa triennale in Commercio Estero nell'Università Ca' Foscari Venezia, Italia

Abstract Money laundering activities related to the cryptocurrency market have seen an exponential increase over the last fifteen years as a consequence of technological developments and economic distresses, as the 2008 crisis and the 2020 pandemic. This essay will analyse the European Union legislation created in order to tackle this phenomenon, dwelling on the Fifth Anti-Money Laundering Directive and its similarities among international laws. In particular, it will display the importance of intermediaries, such as money mules and mixing services, to ease money laundering and increase the anonymity. In this framework, the European Union finds itself almost powerless: the legality of the virtual currency source is assessed only when entering and exiting the virtual market and not during in-market transactions as well as a complete lack of legislation on mixing services activities. Therefore, how can the European Union steam the misuse of such intermediaries with *ex-ante* and *ex-post* interventions? And, finally, are the European privacy policies so important to outrank the risk related to money laundering activities? This paper shows that one way to prevent cryptocurrency money laundering pullulation is launching sensitization and awareness programmes since young age through educational institutions and, most importantly, a narrower legislation is required, implementing those laws that proved to be effective in other countries, in defiance of privacy policies.

Keywords Money laundering. 5th Anti-Money Laundering Directive. Mixing service. Money mule. Virtual Currency. EMMA. Dark Web.

Edizioni Ca'Foscari

Citation Del Monaco, S. (2020). "Money Mules and Tumblers. Money Laundering During the Cryptocurrency Era". *Ricerche giuridiche*, 9(2), 217-230.

DOI 10.30687/Rg/2281-6100/2022/01/004

1 Introduction

In the past thirty years the digitalization of operations has seen a concrete increase in everyday life. Many firms and organizations have embraced this new era, enhancing cross border operations and the electronic payments. As a consequence of this shift in carrying out activities and making transactions, criminals have evolved their business too, exploiting banks and financial institutions in order to disguise the illicit origin of their properties. This is what led the European Union to issue Directives «on the prevention of the use of the financial system for the purpose of money laundering» (Directive 91/308/EEC). However, the creation, and later diffusion, of virtual currencies undermined the transparency of the financial system with a pullulation of money laundering and scam activities. Virtual Assets have the perk of removing intermediaries, such as banks and financial institutions, in transferring funds. This system allows a reduction in commission fees on one side, and a subsequent decrease of transparency on another. As a result, in 2018 the 5th Anti-Money Laundering Directive was drafted in order to tackle the huge impact of crypto-assets illegal operations on the virtual economy. In particular, the Directive tries to uncover what make cryptocurrency so special for the user: the anonymity.

However, criminals have found a way to clean their funds through transactions with other firms ("shell companies"), institutions and people which have nothing to do with the original source of the money, deceiving the legislations. Is it possible to stem money laundering activities by sensitising citizens from the risk they are incurring in investing and exchanging crypto assets? How can the European Union Anti-Money Laundering legislation improve in order to tackle these cryptocurrency intermediaries? And, finally, are the European privacy policies so important to outrank the risk related to money laundering activities? This paper will analyse the risks related to the usage of virtual currencies in particular for those citizens that most of the time are not even aware of being accomplice of a felony. Firstly, the paper will analyse what a cryptocurrency is and the European legislation created in order to prevent money laundering activities, dwelling on the latest Fifth Anti-Money Laundering Directive of 2018, analysing pros and cons, and its transposition in the various European member states. Secondly, the essay will examine the money mules' figure and its core role as intermediator in the money laundering transactions, exploring the EMMA operations and the pullulation of money mules during the COVID-19 pandemic. Finally, the paper will explain the cryptocurrency mixing services, their controversial role in the virtual currency exchange and their requirements imposed by the different legislations across the European Union and the United States of America.

2 Cryptocurrencies

It is not easy to define what cryptocurrencies are. The European Union, in the 5th Anti-Money Laundering Directive of 2018 (5AMLD), tried to find a suited definition for the macro category to which they belong. Initially, the 5AMLD tried to cover all the potential uses and misuses of virtual currencies by defining them in negative (art. 10), underlining what they are not: «Virtual currencies should not to be confused with electronic money…nor with in-games currencies, that can be used exclusively within a specific game environment…nor with…». Finally, the 18 Amendment to Directive 2015/849 declares virtual currencies as a «digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but it is accepted by natural or legal persons as a medium of exchange and which can be transferred, stored and traded electronically». The singularity and the growing importance of cryptocurrencies lays on the way in which transactions are carried out. In order to have a clearer idea, a comparison with electronic payment system will help. Imaging wanting to buy a toy in a shop: the shop worker provides the card details to the bank which checks the records in the owner's bank account to verify if he has enough money; if that so, the bank gives the authorisation to the worker to proceed with the sale, updating the records of both accounts and taking a commission. On the other hand, the virtual currency system represents a good compromise to avoid bank fees and be sure that accounts will not be altered or cheated in any way. The idea behind this system lays on a decentralized record of transaction, thus having many identical ledgers around the world for which every time a transaction is carried out, every ledger will update consequently. In this case, for buying a toy with cryptocurrencies, the shop worker provides the details to all the bookkeepers (computers) which will checks all their records to verify if he has enough money; if that so, all the computers give the authorisation to proceed with the sale, updating all the records. In this manner, transaction fees are insignificant, and it is unlikely to succeed in forging the owner's financial availability, resulting in a rejection of the payment authorization request. Moreover, virtual currencies are easy to set up and fast, being constrained only by the processing speed of the computers upon what they are based on.

However, as much as cryptocurrency is one of the quickest and most transparent media of exchange, it has also contraindications. As a matter of fact, all transactions are recorded permanently, which means that are irreversible. This implies that operational risk represents a very concrete part of the usage of virtual currencies, with transactions that may never be executed, and erroneous transactions

cannot be reversed. In addition, even though the decentralized system helps in securing transactions, in the first half of 2019, attacks against cryptocurrency exchanges and infrastructure passed $ 480 million[1]. Finally, another peculiarity of virtual currencies is the anonymity[2]. Although cryptocurrencies ledgers are completely open for the public to view, what they lack is the openly available identity data: all transactions are conducted between unique wallet addresses, which can be considered pseudonyms. Therefore, once two owners' wallet account identities are revealed, according to virtual currencies transparency features, it is possible to potentially reveal all transaction history between those two owners. However, the possibilities to trace back the identity of a wallet address, are negligible. This is the reason behind the increasing importance of virtual currencies among criminals, who have in this way the possibility to conceal or disguise the illicit origin of their funds, thus facilitating money laundering and terrorist financing[3].

3 EU Anti-Money Laundering Legislation

The first step in containing and combating money laundering activities at global level was taken with the creation of the Financial Action Task Force (FATF) in 1989[4]. This policymaking body was established by the Ministers of its Member jurisdictions and, nowadays, it counts with more than 200 countries and jurisdiction committed to implement the international standards created. The inter-governmental body has developed a series of recommendations and promotes effective implementation of legal, regulatory, and operational measures for ensuring a co-ordinated global response to prevent money laundering, terrorist financing and corruption, holding countries accountable for their compliance to the requirements of the international financial system. In addition, it helps authorities to follow the flows of money of criminals dealing in illegal drugs, human trafficking, and other crimes.

Since 1989, the European Union has adopted the FATF recommendations by redacting five Directives[5], as a consequence of the contin-

1 Ciphertrace, *Cryptocurrency Crime and Anti-Money Laundering Report*, 2020, *https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/*.

2 Bryans, Danton, *Bitcoin and Money Laundering: Mining for an Effective Solution*. *89 Ind. L.J. 441*, 2014, *https://ssrn.com/abstract=2317990*.

3 Silva, *Criminals hide billions in cryptocash*, in *bbc.com*, 2018, *https://www.bbc.com/news/technology-43025787*.

4 FATF website, *https://www.fatf-gafi.org/*.

5 Dir. Un. Eur. Directive 91/308/EEC, Directive 2001/97/EC, Directive 2006/70/EC, Directive (EU) 2015/849 and Directive (EU) 2018/843.

uous review of new money laundering and terrorist financing techniques and strengthen its standards to address new and relatively unknown risks. As a matter of fact, the 5th Anti-Money Laundering Directive, which had to be transposed into national legislations by the 10th January 2020, represents an important new legislative step in the treatment of virtual currencies. Although much of the Directive updates the Directive (EU) 2015/849, it introduces clearer and stricter measures. In preventing and combating money laundering, it considers two new obliged entities: virtual currency exchange platforms and custodian wallet providers, which both represent the providers «engaged primarily and professionally in exchange services between virtual currencies and legally established currencies as well as offering custodial services of credentials necessary to access virtual currencies»[6]. These subjects are facing the same CFT/AML regulations already in place for financial institutions, credit institutions, auditors, real estate agents, casinos and notaries and legal professionals in exercising business and management related representation[7]. In fact, virtual currency exchange platforms and custodian wallet providers have the duty to perform customer due diligence (CDD), submit suspicious activity reports (SAR), record-keeping and internal controls. In addition, the 5AMLD grants additional power to the Financial Intelligence Unit (FIU), giving it the authority to obtain the addresses and identities of owners of virtual currency and, in so doing, to steam the anonymity associated with the use of cryptocurrency[8]. The FIU, one for each member countries, has the duty: to collect suspicious transactions reports, to analyse them an confront them in its database, pinpointing anomalous conducts and providing guidelines, as well as transmitting suspicious transactions report to the National Finance Police for further investigations and notifying the judicial authorities of any penal relevant findings. Finally, the Directive (EU) 2018/843 introduces the requirement for providers of cryptocurrency exchange and wallets to be registered with the competent authorities in their domestic location, as BaFin is in Germany.

In any case, a large majority of member states failed to introduce or to fully transpose by the 10th January 2020 the 5th AML Directive. Therefore, at the beginning of February, the European Commission sent a formal notice to Austria, Belgium, Czech Republic, Estonia, Greece, Ireland, Luxemburg and Poland, warning them that they have only partially implemented the latest Directive. On the other

6 Dir. Un. Eur. 12/2016 Committee on Legal Affairs opinion (PE594.003) 4 art. 2, co. 5, Directive (EU) 2015/849.

7 Dir Un. Eur. art. 2, co. 5, Directive (EU) 2015/849.

8 Quintel, *Follow the money, if you can - Possible solutions for enhanced FIU cooperation under improved data protection rules*, 2019, *http://dx.doi.org/10.2139/ssrn.3318299*.

hand, countries like Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain, have not transposed any of the 5AMLD measures at all[9]. As a consequence, any state that fails to provide a satisfactory response to the European Commission's latest letters within four months, will be sent a reasoned opinion, as to say, a formal request to comply with the EU Directive, explaining the reason why the Commission considers a country breaching the EU law. If the breaching country still does not comply, the Commission may decide to refer the matter to the Court of Justice and ask it to impose penalties[10].

3.1 Similarities with international legislations

It is important to mention that the establishment of a laws at European level followed the lead of many national governments in the Asian Pacific region (APAC), as Hong Kong and Singapore, which by mid-2019 had already made legislative progress in integrating cryptocurrency with financial markets, including new licencing rules and oversight the virtual currencies trading[11]. This approach is completely different from the Chinese one. In the Chinese Republic, the cryptocurrency market is indeed legal, but financial institutions are not permitted to facilitate Bitcoins transactions, prohibiting them from handling virtual currencies; moreover, since January 2018, People's Bank of China (PBOC) banned Bitcoin mining operations[12]. On the other hand, the United States of America reserve an almost equivalent legislation to the European Union in relation to the virtual currency Anti-Money Laundering legislation[13]. According to an Allen & Overy report[14], two of the main differences lie on the fact that: a giv-

9 Act London, 17 EU countries fail to implement 5AMLD, *http://www.act.london/17-eu-countries-fail-to-implement-5amld/*.

10 European Commission website, infringement procedure, *https://ec.europa.eu/info/law/law-making-process/applying-eu-law/infringement-procedure_en*.

11 Lee, *Will the FIFA bribery scandal spur money laundering law reform in Hong Kong? Comparing Hong Kong's anti-money laundering regime with the Financial Action Task Force recommendations*, in *Peking University Law Journal*, vol. 4, n. 1, 2016, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2768584*.

12 Regulation of Cryptocurrency: China; Library of Congress, *https://www.loc.gov/law/help/cryptocurrency/china.php*.

13 Frasher, Agnew, *Multinational banking and conflicts among US-EU AML/CTF compliance & privacy law: operational & political views in context*, SWIFT Institute Working Paper No. 2014-008, 2016, *https://ssrn.com/abstract=2803944*.

14 Stettner, Holman, *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*, in *Allen & Overy*, 2019, *https://www.allenovery.com/en-gb/global/news-and-insights/publications/the-international-comparative-legal-guide-to-anti-money-laundering-2019*.

en cryptocurrency may alternatively be considered a currency, a security, a commodity or more than one option at once, according to the overlapping US regulatory regimes; and, the US declared obliged entities all money transmitters and anonymizing services, as to say mixer services (*v. supra*, par. 4), that do a substantial amount of business in the U.S.

3.2 Pitfalls in the 5AMLD

The Directive (EU) 2018/843, as presented in the *v. supra*, par. 2, has improved the transparency in an almost unregulated market. However, in order to apply all measures requested, crypto firms are facing an increase in compliance costs. In the wake of this grow, smaller crypto firms also face the possibility of consolidation with larger firms, or closure under the burden of heightened administrative costs, provoking market failures. According to a Coin Desk report, 2018 saw a collapse of around 2000 cryptocurrencies leading to 80% loss of their aggregate market cap, combined with the devaluation in particular of Bitcoin after its 2017 rise[15].

In addition to a rise in administrative costs for cryptocurrency firms, the 5AMLD presents a judicial pitfall too, which could possibly undermine the efficacy of the Directive. Provided that the new obliged entities are the ones related to the authorization in accessing to virtual currency and converting them in legally established currencies, an owner account is monitored only when holders enter or exit from the virtual currencies' markets. In so doing, their ledgers will not be controlled every time a transaction is carry out, since it is possible to purchase goods and services without requiring an exchange into a legally established currency[16]. This blind spot may potentially lead to a proliferation of money laundering activities on the already established virtual currency accounts, which, at the moment, are not affected by the Directive (EU) 2018/843.

4 Money mules

How can criminals clean their illegally acquired money? There are many ways for doing so, as using shadow financial infrastructures:

15 Casey, *Crypto Winter Is Here and We Only Have Ourselves to Blame*, in *CoinDesk*, 2018, *https://www.coindesk.com/markets/2018/12/03/crypto-winter-is-here-and-we-only-have-ourselves-to-blame/*.

16 Potts, *Blockchain and government*, in *Data61 'Future of Blockchain' Report*, 2019, *http://dx.doi.org/10.2139/ssrn.3404406*.

funds will be transferred through various front enterprises (often called "shell companies") whose purpose is to make losing tracks of the origin of money flows. However, offenders can rely on other people too to disguise the source of their cash. These intermediaries are called "money mules" as to say people who serve as middlemen for criminals and criminal organizations in exchange for a commission, a reward for helping them in transferring the money[17]. However, not always a money mule is aware of being part of a larger money laundering scheme. This category falls into the unwitting or unknowing money mules. They are usually being asked by someone they have never met to use their established personal bank or virtual currency accounts or open a new account in their true name in order to receive a transfer of money. It is very common for them to be solicited via, for example, an online job scheme or emails. On the other hand, there are also the witting or complicit mules who can be wilfully blind to their money movement activity or advertise their service as a money mule on the Darknet, describing what they are willing to do and at what prices. Nevertheless, money mules, just like fraudsters, are guilty of illegally transporting fraudulently gained money and can be prosecuted for this. Europol underlined that the most targeted individuals in money mulling are newcomers to the country, often selected soon after the arrival, as well as unemployed people, students and those in economic hardship. In particular, the most likely targets are people under 35 years old, even though recently criminal groups have begun recruiting younger generations, from 12 to 21 years old.

In 2019, according to Europol, 90% of money mulling in the European Union territory was related to cybercrime, mainly cryptocurrency, enabled by a dynamic underground economy. In this framework, many illegal products and services are typically sold on Dark Web marketplaces which offer a wide range of items, ranging from drugs to digital products, such as malware kits, stolen data, hacking for hire or money laundering services. Even though a law enforcement took down three of the main Dark Web marketplaces in 2017[18], many higher-skilled cyber-criminals employ their own website to sell services. The main payment medium on the Dark Web is cryptocurrency, for which Bitcoin remains the most popular one, followed by Litecoin and Dash, respectively useful for its speed (four times fast-

17 Oerlemans et al., *Cybercrime and Money Laundering: Bitcoins, Payment Service Providers and Other Methods of Laundering Banking Malware and Ransomware Profits*, in *Cybercrime En Witwassen: Bitcoins, Online Dienstverleners En Andere Witwasmethoden Bij Banking Malware En Ransomware*, Onderzoek en beleid WODC no. 319, 2018, *http://dx.doi.org/10.2139/ssrn.3118269*.

18 EUROPOL, *Massive blow to criminal dark web activities after globally coordinated operation, https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation*.

er than Bitcoin) and its privacy focused[19].

4.1 Operation EMMA

In the European Union, between 2016 and 2019, five European Money Mule Actions (EMMA) have been carried out by law enforcement authorities from 31 countries with the support of Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Taskforce (J-CAT), Eurojust, the European Banking Federation (EBF), 650 banks and 17 bank associations, as well as other financial institutions. The EMMA is a pilot operational project under the flag of EMPACT Cybercrime Payment Fraud Operational Action Plan, designed to combat online and payment card fraud. EMMA is created upon a Dutch operation successfully carried out in recent years in the Netherlands. These actions have represented «a successful example of public-private cooperation at the closest level through and effective partnership between the police, the prosecution and the banking sector at the national and international level» according to the chief executive of the European Banking Federation Mijs. In this wake, the latest operation, EMMA 5, which ran from September to November 2019, reported 75,200 illegal money mule transactions, preventing a total loss of € 12.9 million. According to Europol's press release, it resulted in the identification of 3,833 money mules, alongside 386 money mule recruiters, of which 228 were arrested. 1,025 criminal investigations were open and many of them are still ongoing.

4.2 COVID-19 Scams

As mentioned in *v.supra*, par. 3, criminals target people in financial distress. The new 2020 pandemic represented the perfect timing for increasing the number of unwitting and witting money mules[20]. In the United States, the fear and uncertainty for the financial stability of families was leveraged, according to an FBI press release, «to steal money and launder it through the complex cryptocurrency ecosystem»[21]. The FBI, in fact, registered an increase in blackmail

19 Barysevich, Solad, *Litecoin Emerges as the Next Dominant Dark Web Currency*, 2018, RecordedFuture, *https://www.scmagazine.com/news/cryptocurrency/litecoin-emerges-as-popular-bitcoin-alternative-among-dark-web-underground-community*.

20 Esoimeme, *How banks can detect money mules in the time of COVID-19*, in *Financial Regulation International*, June 2020 special issue, vol. 23, n. 5, *http://dx.doi.org/10.2139/ssrn.3513558*.

21 FBI, *FBI and Secret Service Working Against COVID-19 Threats*, *https://www.fbi.gov/news/press-releases/press-releases/fbi-and-secret-service-working-against-covid-*

attempts, work from home scams, paying for non-existent treatments or equipment and investment scams COVID-19 related. A similar scenario happened in the United Kingdom in which scammers claimed to be affiliated with, for example, the World Health Organization (WHO). Scammers purported to have a list of COVID-positive residents, where the victim can only gain access if they either go to a credential-stealing page or make a donation using a Bitcoin account[22].

5 Cryptocurrency Mixing Services

Money mules are not the only intermediaries in illegal transactions. In fact, there are services that help to protect the anonymity of transactions: the mixing (or tumbler) services[23]. They swap many cryptocurrency owners' streams with each other in order to obscure the trail back to the fund's original source and making impossible to establish a link between a sender and a receiver[24]. This system was born as a consequence of the complete transparency of virtual currency transactions. In fact, as stated in *v. supra*, par 1, once a criminal transaction has been discovered, it becomes incredibly easy to find all the previous interactions between those two accounts. With the tumblers' intermediation there will be no connection between the two original addresses. It is important to underline that the transaction can be split up in many small partial payments spread over a longer period of time, helping the anonymity. The tumbler service usually charges a fee that could range from 0.25% to 3% of the total amount to be mixed. At the moment, there is no legislation in the European Union that regulates and states whether mixing services are illegal or not. Surely, cryptocurrency owners can ask to tumbler their funds to increase their privacy[25]; however, it is impossible to deny that virtual currencies mixing services are handful for criminals who want to clean their funds. In June 2019 the Dutch Financial Crime Investigative Service, seized the website of a popular Bitcoin mixing service: *Bestmixer.io*. The service started in May 2018 and achieved a turnover of at least $ 200 million in a year's time and

19-threats.

22 Fintechnews Switzerland, *Crypto Scams Rampant in the UK Amidst COVID-19*, *https://fintechnews.ch/blockchain_bitcoin/crypto-scams-rampant-in-the-uk-amidst-covid-19/34044/*.

23 Phillips, *What is a Bitcoin tumbler? Are they legal?*, *https://blocksdecoded.com/what-is-bitcoin-tumbler/*.

24 Custers et al., *Banking malaware and the laundering of its profits*, in *European Journal of Criminology*, 2019, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3411486*.

25 Dir. Un. Eur. The General Data Protection Regulation (EU) 2016/679.

guaranteed that the customers would remain anonymous. Europol stated that most of the cryptocurrency passing through Bestmixer had «a criminal origin or destination» and, helped by the authorities, seized six services based in Luxembourg and the Netherlands[26].

However, in spite of the money laundering risk associated with cryptocurrency mixing services, tumblers are used for lawful activities more often than for illegal ones. In fact, according to Elliptic, a blockchain analysis firm, only 16% of the funds going through a mixer service came from an illicit activity: the remaining 84% was due to cryptocurrency owners wanting to improve their privacy[27].

5.1 Unregulated Cryptocurrency Exchanges

The most of virtual currencies money laundering activities is carried out through an unregulated cryptocurrency exchanges, instead of using a cryptocurrency tumbling service. With this system, a criminal has the possibility to send illicit funds to an unregulated exchange, swap them among several other types of virtual currencies, and send them to an anonymous account. According to CipherTrace's cryptocurrency Anti-Money Laundering report[28], between January 2009 and September 2018, 97% of illegal Bitcoin has been processed using unregulated exchanges which, in particular, receive 36 times more criminal Bitcoins if stationed in countries where AML legislation is either weak or not enforced. Contrary to the European Union non-regulation of money mixers services, on 19th August 2018 the US FinCEN remarked that businesses that provide anonymizing services, which try to disguise the source of the transaction of virtual currency, are money transmitters (regulated by the BSA legislation) when they accept and transmit convertible virtual currency[29]. In doing so, they have regulatory obligations under the BSA. With this declaration, the US made tumblers subjected to the Anti-Money Laundering/Combating the Financial Terrorism requirements of the Bank Secre-

26 D'Elia, *Sequestrato uno dei più grandi cryptocurrency mixer*, in *Tom's Hardware*, *https://www.tomshw.it/altro/riciclaggio-bitcoin-sequestrato-uno-dei-piu-grandi-cryptocurrency-mixer/*.

27 Moiseienko, Kraft, *From Money Mules to Chain Hopping*, in *RUSI*, 2018, *https://rusi.org/explore-our-research/publications/occasional-papers/money-mules-chain-hopping-targeting-finances-cybercrime*.

28 Ciphertrace, *Cryptocurrency Anti-Money Laundering Report*, cit.

29 Financial Crime Enforcement Network, *Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at Morehouse College, https://www.fincen.gov/index.php/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-morehouse-college*.

cy Act (BSA) and its implementing regulations[30]. On 13th February 2020, the US Department of Justice announced that Larry Harmon, the operator of a Dark Web site cryptocurrency laundering service that was mixing Bitcoins called Helix, had been arrested based on a federal indictment that charged him with money laundering conspiracy, operating an unlicensed money transmitting business and conducting money transmission without a District of Columbia licence. The mixing service operated from 2014 to 2017, allowing customers, for a fee, to send Bitcoin to other Bitcoin accounts in a manner that was impossible to distinguish the source or the owner of the money[31]. This tumbler service was advertised in the Dark Web as a mean of concealing transaction from law enforcement. In four years, Helix moved more than $ 300 million, as to say 350,000 Bitcoins, on behalf of customers, with the largest volume of Bitcoin coming from Dark Web markets, as AlphBay, later seized by law enforcement in 2017.

6 Conclusion

In this paper, it has been analysed the role of the European Directives in preventing and prosecuting money laundering activities through intermediaries such as money mules and mixing services. The transparency required by the Anti-Money Laundering legislations has been challenged by the pullulation of the crypto assets' importance as a medium of exchange. Its anonymity makes hard for the authorities to verify the legitimacy of the transactions. The correlation between financial distress and rise in money mulling is undeniable. During the COVID-19 pandemic it has been glaring how many scam text messages and email an individual might receive over a certain period of time, especially if there are financial sufferings. However, it is possible to raise awareness and sensitising citizens from this type of frauds, teaching them how to protect themselves and what to do if they become victims. It is important to explain these illegal activities since the young age, possibly through educational institutions and events on how to prevent these scams, not only through the already implemented #DontbeaMule hashtags. However, even though money mulling activities are illegal, hence the only way to reduce their amount is to combat them (ex-post), the European Union can still intervene at legislative level (ex-ante) to tackle those mixing service activities that can potentially launder money. By regulating on-

30 Office of the Comptroller of the Currency website, *https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html*.

31 United States Department of Justice, News, *https://www.justice.gov/usao-sdny/pr/operators-global-cryptocurrency-ponzi-scheme-and-attorney-charged-fraud-and-money*.

ly those entities that handle the exchanges between cryptocurrencies and legally established currencies, the European Union keeps out from being regulated all those exchanges that can still happen inside the virtual currency markets, without being transformed in legal tenders. In fact, an implementation of requirements for tumbler services, such as the US licencing according to the BSA regulation, could steam the illegal money exchanges happening every day in the cryptocurrency markets. Privacy, especially identity and personal data, in the European member states plays a fundamental role in every transaction and contracts, as well as in the communication system. Nevertheless, the European Union should ponder the actual benefits of this cryptocurrency privacy with the imminent and concrete risk that clean money will flow into the underground economy and subsequently decide which will be a smaller impact in European people's life. To conclude, until now the European Union has followed the changes in the market, trying to contain the threats as they arise. Financial markets are changing constantly, and crypto assets might become of vital importance in the next future. Acting with small changes in the legislation, during a long period of time, will not help stopping money laundering. The European Union needs to understand the crypto currency market and make it its own, by implementing measures that help in preventing illegal activities in a non-transparent trading system in the most efficient way.