An Analysis on Prevalence of Money Laundering with the Challenges of Emerging Technologies in the context of the United Kingdom

Zeenia Hossain
Advocate, Supreme Court of Bangladesh (High Court Division), Bangladesh

Abstract: Money Laundering is a kind of financial crime that converts proceeds of crime and further disguises the illicit origin of money brought in the economic system of a State. The scope of money laundering is extensive especially conceived as in recent times by taking into account the emerging challenges arising from digital technologies being used in deriving the illegal sources of money and integrating it back to the financial resources of the states. The article aims to analyze on the prevalence of money laundering in the United Kingdom by dealing with the emerging issues confronted by it in this digital age of technology. The article recognizes how new aspects of this economic crime are being created by abusing digital technology through internet and social media and emphasizes on the current AML legal framework in the United Kingdom.

Keywords: Money Laundering, Anti-Money Laundering laws in UK, Crypto Money Laundering, Cryptocurrency.

I. INTRODUCTION

With the emergence of digital technologies and popularity of social media, it has become impossible to restrict the possibilities of money laundering and hence it is said to run ‘from cults to marathons and beyond’ (Beare, 2015) which indicates the range of the methods of laundering from the small-time drug dealers to the highly influential politically exposed persons (PEPs) and independently by anyone with the abuse of the advancement of technology and opportunities arising from the development of digital age with cryptocurrencies (Ferguson, 2018); (European Central Bank, 2012).

Money Laundering is any activity in relation to the proceeds of crime by concealing and disguising the true origin and ownership of any property, including even passive activity, i.e. mere possession of such property, having knowledge during the receipt of the property to be the proceeds of corruption, drug trafficking, online gambling, terrorist financing and relevant criminal offences and criminal activities [Section 327-329 of Proceeds of Crime Act (POCA) 2002]; (Working Group, 1995); (Hatchard, 2014); (African Union, 2013)].

Cryptocurrencies, though not globally defined, is a type of unregulated, digital representation of value used as like as any currency, issued and usually controlled by its developers, used and accepted among the members of a specific virtual community” (European Central Bank, 2012). As per Rule 14A (3) (a) of The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, which amended the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, after it being laid before the Parliament on 20 December 2019, of which most of the provisions came into force very recently on 10 January 2020 with some exceptions, “cryptoasset” means a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically”. Thus cryptoassets include all cryptocurrencies and even non-currency assets, i.e. security tokens and utility tokens (FCA, 2019).

The amended EU Directive of 2018 defines “virtual currencies” as ‘a digital representation of value that is not issued or guaranteed by a central bank or a public authority’, and thus it is neither referred as a legally established currency, nor deemed to possess a legal status of currency, but refers to a means of exchange that can be transferred, stored and traded electronically (EU Directive, 2018). Henceforth, it involves decentralized system having peer-to-peer transactions and users conduct it with anonymity where true identities are in disguise, having very limited verification for Anti-Money Laundering checks when the transactions are recorded on the blockchain and available to the public in ledgers (European Central Bank, 2012).

Therefore, crypto-assets, being digital currency and a new form of exchange being decentralized from the control of central banks, are significantly playing a ‘potential role in money laundering’ recently leading to business loss to the investors in trading with cryptocurrencies and consistently increasing the risks of money laundering as well as the associated risks of financial crime.
laundering (Monaghan, 2018). The emerging demand and higher prices of bitcoins up to 900% since 2017 also alert the abuse of such assets in trading for offenders’ nefarious motives in recent times are indeed potential challenge aiding money laundering that is to be regulated efficiently as urged by the UK Treasury Select Committee in its report (Monaghan, 2018; Sey, 2019).

II. PREVALENCE OF MONEY LAUNDERING WITH EMERGING TECHNOLOGIES

The National Crime Agency (NCA) of the United Kingdom (UK) records show that Britain alone launderers money that amounted to £90 billion each year, about four percent of the Gross Domestic Product (GDP) including the secretive tax havens in it (Mitchell MP, 2018).

The offence of money laundering is often associated with off-shore financial centres known as ‘secrecy jurisdictions’, creating shell companies in the British overseas territories (BOT), being in disguise of beneficial ownership behind the disclosed corporate entity (Hatchard, 2014). The prevalence of money laundering in the UK has been interconnected with the corruption, enhanced supervision and customer diligence measures in the banking systems and the financial institutions; the obscure beneficial ownership of shell companies located in the BOT; lack of effectiveness in the Anti-money laundering (AML) regime of banks, financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs), Designated Non-Financial Institutions (DNFIs) and money transfer services (Council of Europe, 2019).

However, there had been rise to a considerable extent of crypto money laundering all over the developing countries, as per CipherTrace, world’s first US based blockchain forensics team to fight crypto money laundering by dealing to provide solution and developing Anti Money Laundering (AML) framework in cryptocurrencies (CipherTrace, 2020). The fraudsters and scammers caused misappropriation of funds and made over an approximate sum of $4.26 billion from cryptocurrency users, exchanges, investors in 2019 (CipherTrace, 2020). The crypto money laundering amounted to £3.4 billion until November 2019, as per the report of CipherTrace, indicates the increased prevalence of money laundering used by the criminals to raise their funds in recent years (CipherTrace, 2019).

In the UK, the prevalence of money laundering in UK have risen since the victimization of the genuine bank account holders through the abuse of digital technology and social media by being subject to ‘money mules’ (Europol, 2019). Money mules is being equated with money laundering and refer to the activity of the people who transfer money acting on others’ behalf, after acquiring it illegally, either in person, electronically, through a courier service or money transfer agency and use others’ account information in deriving the proceeds through the process and thus causing to close thousands of bank accounts and the account holders to be sentenced in prison for several terms (BBC, 2019; Monaghan, 2019). The most recent prevalence of money mules in the European member states of European Union (EU) demonstrated in its fifth European Money Mule Action (EMMA 5) that was held during September – November 2019, those 3833 money mules were active and had been identified to lure the online job hunters for obtaining fast cash within hours, in addition to 386 money mule recruiters, of which 228 were arrested (Europol, 2019). There had been reports of 7520 fraudulent money mule transactions and upon the AML efforts and regime by 650 banks and over 17 financial institutions, €12.9 million have been saved from loss (Europol, 2019).

However, as per the records, even in 2009, the UK residents were victimized by the use of digital technology by only 100 money mule recruitment sites having 50 active mules (Osborne, 2009). Both the older people in between 41-60 years old and teenagers and young people under 25s were found to be recruited through social media sites such as Instagram and Snapchat to launder money for the gangs in order to make money within less span of time (BBC, 2019). This is intended due to it being quite easier to make people of such ages to agreeing to share their bank details either due to their unawareness or not being educated in such issues of modern age, so that as the next step, the cash can be deposited into their account for them to follow instructions. Then the process involves sending it into another bank account by them and since younger people usually may not have criminal history in financial crimes and henceforth they are more likely to be trusted by the banks except otherwise suspicious transactions are found (Hughes, 2019). Thus the records in 2017 demonstrated that, several UK banks have found 8,500 money mule accounts owned by youngsters under the age of 14-21 and also a 35% rise in such involvement among those aged between 41 and 60, without knowing the repercussions of money laundering crimes through their facilitation of human trafficking, drugs and terrorism (Hughes, 2019; BBC, 2019; Sey, 2019).

In addition, recently as per CipherTrace, 65% of the most popular 120 Cryptocurrency exchanges have poor and weak KYC requirements (CipherTrace, 2019). Moreover, the cryptocurrencies have led to over 100-200 gambling sites on the Internet which allow gambling through such virtual currency and therefore, many crimes committed in the dark web are paid in this form (CipherTrace, 2018; Sey, 2019).

In demonstrating the prevalence of digital currency, social media site known as Facebook had also communicated the governor of Bank of England and contracted with the Head for public affairs of Standard Chartered to join as director of public policy in the company for introducing the transactions and payments in
virtual currencies to be named as “stablecoin” and regulating them since the US derivatives regulators were concerned whether the company could stick to the strict money laundering and Know Your Customer (KYC) measures imposed on the financial institutions (Morris, 2019; Sey, 2019).

In the past two years, the money laundering risks rose from such crypto crimes in UK as reported by Action Fraud in June-July 2018, where 203 reports of cryptoasset scams occurred causing the victims losing over £2 million in total where the fraudsters cold call victims and use social media platforms to advertise ‘get rich quick’ investments scams (The HM Treasury, 2018; Sey, 2019). Thus during the previous year 2018-19, the fraud and scams occurred in online trading platforms using cryptocurrencies such as bitcoins and litecoins has tripled to launder money up to total loss of £27 million to the victims, the fraudsters being those who facilitate cybercrimes and drugs, guns and other illicit items trafficking all over the world (Jones, 2019; Gibbs, 2019; Sey, 2019).

Although, in October 2018, in the report prepared by the HM Treasury, FCA & Bank of England in UK, it is concluded that crypto assets are not widely used in the UK, having only 15 cryptoassets exchanges headquartered, compared to the existing 206 global cryptoasset exchanges worldwide, the use and interest in the cryptoassets in the transactions in UK in recent times and the leading money laundering risks to the consumers and cyber-based crime cannot be denied (The HM Treasury, 2018; Sey, 2019). Therefore, in the Taskforce report, the chief financial regulators of UK concluded that the use of cryptoassets for money laundering is growing, despite it was low in use, and thus guiding the public in general towards awareness and understanding that the emergence of technologies has to be evaluated in terms of its use and advantages for combating money laundering (The HM Treasury, 2018; Sey, 2019).

Henceforth, the HM Treasury, FCA & Bank of England are working together to regulate the cryptoassets in the financial transactions and therefore concluded that the digital currencies do not still pose threat to the financial stability of the UK (The HM Treasury, 2018). The emergence of cryptocurrencies has entirely changed the ways of keeping records of crypto activity in this digital age, since the blockchain does not store the relevant information required to identify the account holder and also because here are other networks to conceal true identity of the user (Sprenger, 2018; Sey, 2019). Moreover, the FCA has taken steps to improve public awareness of the risks associated with all types of cryptoassets through media appearances (Ahmed, 2017; Sey, 2019) and by warnings to the consumers and firms about the risks of ML in the crypto industry (Ahmed, 2017; Sey, 2019). This is essential since the unemployed youngsters and many other people are not informed about the ML risks associated with it and in order to derive benefits from the illicit proceeds originated through it they are being the victims of such fraud and scams.

The UK and other EU governments and the Financial Conduct Authority (FCA) has been also considering a ban on using cryptocurrencies for trading due to its lack of regulation and consumer protection leading to consequences like money laundering, terrorist financing and tax evasion (Kollewe, 2017; Kollewe, 2018, Sey, 2019).

III. DISCUSSION

The concepts of Money laundering have been developed with the emergence of time starting from the processes and ways of laundering money originated from commission of serious offences by concealing their illicit source to appear it to be derived from lawful origin to the version of currencies being digitalized and virtually converted with the evolution of cryptocurrencies and notion of crypto money laundering (Olasupo, 2018)(CipherTrace, 2019).

Analyzing the significant notions of all the six EU Money laundering Directive till date, money laundering referred as the conversion of property, derived from serious crime, for concealing the true nature, source, location, disposition, movement, rights with respect to, or ownership of property and disguising its illicit origin or of assisting any person who is involved in committing such an offence to avoid the legal consequences of his action; it beginning from financial institutions, casinos, money service businesses, corporate service providers, investment policies and insurance companies, ranging from professionals, i.e. lawyers, accountants and dealers in high value goods to the electronic verification of customers in the financial institutions, use of prepaid cards, notion of enhanced customer due diligence, concern for registration of foreign-owned assets (Bowcott, 2019) and regulation of virtual currencies and crypto money laundering (The Economist, 2019); (Kingsley Napley, 2018); (Tim Edmonds, 2018) (Sey, 2019)

The widely recognized three money laundering stages include: firstly, introducing the proceeds of crime in the financial system, i.e. placement; secondly, disguise the property trail through complex and repeated financial transactions to ensure anonymity by layering and finally integrating the funds fully and unidentifiably to the legitimate economic system by integration (GOPAC, 2012). The stages of money laundering activities are particularly evolving and distinct from one another among financial institutions, shell companies, off-shore banking and secrecy jurisdictions, online trading platforms or through legal practitioners and other professionals (Banerjee, 2019). However, with the emergence of crypto money laundering, the three-stage process has become
more complicated to identify at what stage or point does the laundering takes place as it occurs without direct involvement of financial intermediaries and third parties such as banks and other financial institutions except exchanges (Forgang, 2019). The crypto money laundering crime as a predicate crime here involved raising funds through illegal activity by selling illegal goods or services in exchange for crypto-assets. Thus the first stage of placement included converting crypto-assets into fiat currencies within a prevalent financial system; layering includes converting fiat assets into crypto-assets, exchanging crypto-assets and splitting large amounts of crypto-assets into smaller sums stored in many custodian wallets by moving, converting or placing illegal funds to distance them from their source (ICAEW, 2019). The launderer might choose to invest the funds into real estate, luxury assets, or business ventures (Sey, 2019). The method of using crypto cleansing is by purchasing a basic cryptocurrency at a digital exchange or by cash or by debit card at a digital currency ATM using anonymity and buying primary coins, i.e. Bitcoin, Etherum or Litecoin, in exchange of fiat currency and obfuscate the primary coin’s audit trail by layering tactics, known as mixing an tumbling and finally integrate by severing the audit trail into the traditional financial system and thus withdraw money from digital currency to receive fiat currency (European Central Bank, 2019; Sey, 2019).

Therefore, the laundering through crypto currencies are being carried on virtually using the same traditional schemes of casinos but that which is online, accepting bitcoins in order to exchange the cryptocurrency for cash using bank accounts and cards and by smurfing, where offenders used the exchange to convert their illicit proceeds into bitcoins, then change the cryptocurrency into cash and deposit it into bank accounts (European Central Bank, 2019; Sey, 2019).

The very basic legislation relevant to money laundering in UK as mentioned in the introducing the definition of the offence, is Proceeds of Crime Act (POCA) 2002, which describes the stages that account for commission of the offence, and also includes the powers and functions of the law enforcement agencies to investigate and seize the illicit proceeds, derived from commission of several other kinds of crimes (Edmonds, 2018). As per Sections 327-329 of POCA 2002, money laundering offences firstly include any activity by a person: i) conceals, disguises, converts, transfers or removes from the jurisdiction any property knowingly or in suspicion that it represents proceeds of crime; ii) enters into or becomes concerned in an arrangement knowingly or in suspicion which will facilitate another person to acquire, retain, use or control criminal property and the person knows or suspects that the property is criminal property and iii) acquires, uses or has possession of property which he knows or suspects represents the proceeds of crime. Thus as per Section 334 of the POCA 2002, these offences are either punishable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum in the Magistrate’s Court or on conviction on indictment in the Crown Court by a maximum of 14 years imprisonment and/or a fine. According to Section 340(3) POCA, 2002, proceeds of crime is the property that constitutes a person’s benefit from criminal conduct or represents such benefits and the alleged offender knows or suspects that it represents such benefits (GettingtheDealThrough, 2019; Sey, 2019).

Moreover, by the insertion of Section 37 of the Serious Crime Act 2015, POCA was amended in Section 338 where it was provided that when authorized disclosure submitting suspicious activity reports (SAR) to the NCA is made in good faith, no civil liability arises in respect of the disclosure against the person making it (Sey, 2019).

Besides POCA, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (MLRs) 2017 applies to the transactional activities of the companies, businesses, and professionals known as ‘relevant persons’. It sets up the standards to be complied with by the relevant business entities, financial institutions, auditors, insolvency practitioners, accountants and tax advisers, lawyers and other professionals, trust or company service providers, estate agents, high value dealers and casinos (Regulation 8). However, very recently on 20 December 2019, after being laid down before the Parliament, the provisions of Money Laundering and Terrorist Financing (Amendment) Regulations 2019 has been amended in Sections 4(1)(b), 4(6) and 4(3), to include crypto-asset exchange providers, custodian wallet providers and crypto-asset automated teller machines and letting agency for high value deals and to art market participants for transactions that exceed €10,000 into the relevant MLR 2017 regulations respectively as mentioned in the amended part. Therefore, it emphasizes the pressing need to control crypto money laundering by making the definition of “crypto-asset” is made wider in context as compared to the equivalent “virtual currency” definition provided by the 5th EU Directive in 2018 which only meant digital representation of value being in decentralized state without any status of a legal currency (Shearman, 2020).

The MLR 2017 require the relevant controlling authorities like HM Treasury, UK Home Office and other relevant investigative and supervisory authorities to conduct risk-based assessments (Regulation 16-19) in their businesses, identifying AML vulnerabilities and establishing policies, controls and procedures to mitigate and manage effectively those risks and undertake adequate client due diligence (CDD) measures when there are suspicions of money laundering or doubts as to the veracity or adequacy of identification documents previously obtained (Regulation 27). However, under the changes introduced by the 2019 Regulations, letting agency

DOI: 10.9790/0837-2501064754 www.iosrjournals.org 50 |Page
businesses and art market participants, as well as crypto-asset exchange providers and custodian wallet providers, will also be required to apply CDD measures and are subject to all other obligations of this MLR 2017. Due to the changes in the Financial Action Task Force (FATF) standards, the CDD requirements have been strengthened in 2019 Regulations, as it imposed obligations upon relevant individuals to take reasonable measures to understand, control and verify the ownership of the involved wealth and identities of the managing officials in cases of suspicious beneficial ownership of a corporate entity (Shearman, 2020), in addition to the MLR 2017, where there were laid down appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is PEP in order to apply enhanced customer due diligence measures against them.

The Regulations creates criminal offences for failing to comply with the rules given and also relating to prejudicing or obstructing investigations and makes disclosure that prejudices the investigation and also providing false and misleading information during investigation, under the Regulations 86, 87 and 88. The Financial Conduct Authority (FCA) or any supervisory authority may impose civil financial penalties of such amount as they consider appropriate.

In addition, The Sanctions and Anti-Money Laundering Act 2018, drafted to ensure that the UK can continue to impose, update and lift sanctions provided for by the UN post-Brexit and pursuant to other international obligations, created a significant influence to carry on making provision in relation to anti-money laundering, specifically to effectively detect, investigate and prevent money laundering and terrorist financing, including by implementing internationally recognized FATF recommendations and standards published from time to time relating to combating threats to the integrity of the international financial system (GettingtheDealThrough, 2018; Sey, 2019).

Furthermore, the European Union has been an important regulatory framework as there have been four ML EU Directives (5MLD) which are transposed into national laws such as POCA 2002, MLRs 2017 and TACT 2000, and similarly the 5th EU Directive 2018 has been recently transposed in the MLR 2019 on 10th January 2020, except the CDD measures only regarding anonymous prepaid cards and requests for beneficial information about accounts and safe-deposit boxes, that is intended to come into force on 10 July 2020 and 10 September 2020 as agreed upon respectively (Shearman, 2020). The significant features of 5MLD relate to existence of public registers of the beneficial ownership details of companies to be available to the authorities; greater verification of entries on the national beneficial owner registers has to be made; reduced monetary limits before verification of identity is required for the use of prepaid cards; extending the scope of AML regulation to virtual currencies creating an obligation to report suspicious transactions, tax-related services and works of art; mandatory measures to be taken for customers from “high risk” countries, including those which have no or low beneficial ownership details and who do not cooperate in the exchange of information, to be only available to the authorities (O Connor, 2017; Sey, 2019).

The 5MLD has specifically provided for the first time requirements for cryptoassets exchanges and custodian wallet providers and the UK government along with the FCA and Bank of England through the Cryptoassets Taskforce developed a comprehensive policy and regulatory approach to cryptoassets and distributed ledger technology (DLT) and its report highlighted growing risks for the customers and markets from the use of cryptoassets for illicit activity leading to money laundering (The HM Treasury, 2018; Sey, 2019).

Therefore, the transposition of all the EU Directives into UK legislation has been done due to keeping the UK AML legal framework up to date, effective and proportionate along with the FATF recommendations (The HM Treasury, 2018; Sey, 2019).

The offence of money laundering has impacted the global economy and in UK, being an extensive national crisis as well in all its jurisdictions, requires collective solution from the complex networks and different stakeholders involved in the global financial system (Eves, 2019); (Sey, 2019). However, due to the loopholes in the legal and enforcement framework and vulnerabilities among the relevant stakeholders involved in the process, the perpetrators tend to exploit and hence the laundering opportunities escalates with time that caused UK to spend £37 billion each year in dealing with serious and organized crime as a consequence (Eves, 2019). For instance, in the Mutual Evaluation Report by FATF in 2018, regarding technical compliance with its recommendations, it is found that UK FinancialIntelligence Unit’s (UKFIU) role is curtailed due to its lack of proper resources and limitation in its capabilities being unable to perform effectively by sharing information with foreign FIUs (Sey, 2019).

Furthermore, at the European and international levels, effectiveness and implementation of national AML regimes has to be more strengthened with enhanced co-operation and intense supervision by FATF and Council of Europe’s AML expert committee (Council of Europe, 2019; Sey, 2019).

IV. CONCLUDING REMARKS

Money laundering is considered to be a ‘serious threat to democratic stability, human rights and the rule of law’ (Council of Europe, 2019) of any state and it has been linked to the notion of corruption as its
proceeds are being laundered internally (GIABA, 2010) by the countries all over the world (Hatchard, 2014). The prevalence of the economic crime and its emerging risks are really one of the most concerning issues of hindering third world countries from achieving their sustainable development goals in strengthening their criminal justice system and the UK is affected by the consequences of this economic crime. The UK has been constantly developing its AML regime along with the EU support, however, it is yet a matter of concern regarding the emergence of crypto money laundering and also the arrangements agree upon due to post-Brexit and henceforth tackling this crime with the existing money laundering risks prevalent for ages.

REFERENCES

An Analysis on Prevalence of Money Laundering with the Challenges of Emerging Technologies in...


DOI: 10.9790/0837-2501064754 www.iosrjournals.org 54 |Page