ANTI-MONEY LAUNDERING IN THE DIGITAL AGE: A CASE STUDY OF NIGERIA

Boluwatife Faturoti[1]

and

Marcus Ayodeji Araromi, PhD.[2]

Abstract

This paper examines money laundering in Nigeria in general, conceptualising it and identifying the gaps in the legal framework designed to tackle this menace. Special focus is given to using the digital platforms to carry out money laundering in Nigeria and the challenges created through these platforms in combating or preventing it. The emergence of digital innovation and technology has a big impact on money laundering in Nigeria. Because digital currencies are virtual and therefore outside the authority of any one state, they are especially useful for the layering step of money laundering. This makes it possible to convert between various cryptocurrencies and fiat currencies, send money internationally without difficulty, and make trading and investing activities easier. Financial criminals can move money across borders until the link to the initial crime is effectively broken by using cryptocurrencies to effectively hide the origin of their unlawful funds. The regulatory developments in the wake of cyber laundering in Nigeria is considered. In the end suggestions for reforms are made, which include enhanced legal and regulatory frameworks, strengthening international cooperation, investment in technological solutions, and encouragement of responsible innovations, among others.

1.0 INTRODUCTION

A cursory flip through Nigeria's history books would immediately divulge the fact that money laundering has been a persistent challenge within the nation's financial landscape, with its roots extending as far back as the 1980s. Just between the mid-1980s and 1999, Nigeria suffered a staggering loss of US$100 billion to money laundering.[3] Furthermore, the

[1] Department of Public Law, Faculty of Law, University of Ibadan, Ibadan.
[2] Department of Public Law, Faculty of Law, University of Ibadan, Ibadan.

subsequent decade, from 2000 to 2010, witnessed the indictment of at least 15 former State governors, 5 bank executives, and 4 firms, facing charges related to corruption and money laundering, involving an estimated $270 billion.[4] These disquieting statistics underscore the gravity of money laundering, which continues to plague Nigeria even in contemporary times.

It is essential to recognize that the interconnectedness of nations in the era of globalization has transformed money laundering into a transnational crime, posing a pervasive threat not just to Nigeria's economy and security, but to the global economy and the stability of nations worldwide. Globalization has created an avenue for money launders to exploit gaps in international financial systems, capitalizing on cross-border fund movements, the proliferation of offshore financial centres, and the emergence of digital currencies, allowing criminals to effortlessly navigate various legal frameworks while evading detection within their home states.[5]

The danger of money laundering is further highlighted by its ranking as the number one global crime threat in INTERPOL's first-ever Global Crime Trend report.[6] As a result of its transnational nature, there is a duty of care and obligation on countries imposed by the Financial Action Task Force (FATF), which is the primary international organization saddled with the responsibility of preventing money laundering and terrorism financing, to establish effective legal frameworks for combating money laundering. Nigeria, like other countries, has the responsibility of establishing an effective legal framework for combating money laundering in Nigeria.

Money laundering has undergone significant transformations in the digital age due to technological advancements. The growth in technology over the years has brought in the concept of cyber laundering – transitioning of traditional money laundering into cyberspace.[7]

---

[3] O M Bakare, 'Money laundering and trans-organised financial crime in Nigeria: Collaboration of the local and foreign capitalist elites' (2007). EBS Working Papers, University of Essex. WP 07/03.
[4] K G Kingston, 'Churches and Private Educational Institutions as Facilitator of Money Laundering in Nigeria' (2011) 1(1) African Journal of Education and Technology 30-38.
[5] R C Hellvig and C A Blanaru, Impact of globalization on money laundering. (2023) XI (32) SEA - Practical Application of Science 91-95
[6] INTERPOL,. 'Financial and cybercrimes top global police concern, says new INTERPOL report.' (19 October, 2022) Retrieved Sept. 20, 2023, from <https://www.interpol.int/en/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report#:~:text=Financial%20crime%2Das%2Da%2Dservice&text=Respondents%20ranked%20money%20laundering%20as,most%20(72%20per%20cent)>.
[7] M W Calafos. and G Dimitoglou, 'Cyber laundering: Money laundering from fiat money to cryptocurrency' ResearchGate (2022) DOI:10.1007/978-3-031-10507-4_12 <https://www.researchgate.net/publication/365641007_Cyber_Laundering_Money_Laundering_from_Fiat_Mo

The proliferation and accessibility of online platforms present criminal enterprises with novel avenues to enhance their money laundering endeavours.[8] In particular, the rise of virtual currencies has been significantly linked to cyber laundering.[9] Virtual currencies have been defined by the Financial Action Task Force (FATF), which is the primary international organization saddled with the responsibility of preventing money laundering and terrorism financing, as a digital form of value that is tradable online and serves as (1) a means of exchange; and/or (2) a standard unit for measuring value; and/or (3) a method of storing value however, it does not hold legal tender status, meaning it is not recognized as a valid and legally binding form of payment when presented to a creditor in any jurisdiction.[10]

The ramifications of this transformation are extensive. Regulatory bodies face the formidable challenge of updating their frameworks to efficiently oversee and address illegal financial activities carried out via digital means. Additionally, the rise of cyber laundering threatens the stability of Nigeria's financial system and its broader economy, as well as national security. This paper seeks to examine the changing environment of money laundering enabled by digital currencies, emphasizing the urgent necessity for thorough strategies to tackle these issues and the imperative for Nigeria to establish strong regulatory measures to protect against money laundering and associated illicit activities.

2.0 MEANING OF MONEY LAUNDERING

Money laundering is a multifaceted financial crime that permeates both domestic and global financial systems. It represents the process through which illegally obtained funds, often referred to as "dirty money," are transformed into seemingly legitimate assets or funds, known as "clean money." This transformation is undertaken with the primary aim of concealing the illicit origins of the funds, thus allowing those involved in criminal activities to enjoy the proceeds without attracting suspicion or legal repercussions.

---

ney_to_Cryptocurrency#:~:text=Cyber%20laundering%20provides%20quick%2C%20easy,blockchain%20make%20it%20technically%20complex>.

[8] Ibid.

[9] D Bryans and F J Anema, 'Bitcoin and money laundering: mining for an effective solution' 2014 Bryans 89 Ind. L.J. 441. Retrieved on Sept. 20, 2023 from <https://ssrn.com/abstract=2317990>

[10] FATF Report. June 2014. 'Virtual currencies key definitions and potential AML/CFT risks.' Retrieved on March 22, 2024 from <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf>

The concept of money laundering encompasses a series of deliberate and complex transactions designed to obscure the source, ownership, control, or destination of illicitly acquired wealth. This illegal practice undermines the integrity and transparency of financial systems, posing severe threats to the stability of economies and security on both national and international scales. Like many legal concepts in law, there is a lack of consensus on the definition of the term money laundering. Money laundering has been defined by several individuals, organizations and academics in different ways.

While the FATF definition of money laundering defined above is commendable for its simplicity and accessibility, it may benefit from expansion and refinement to encompass the full spectrum of money laundering activities, address emerging challenges, and achieve greater global consensus. Such improvements could enhance the effectiveness of international anti-money laundering efforts.

Article 6 of the United Nations (UN) Convention against Transnational Organized Crime defines money laundering as:

> 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 helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; or the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime participation in, association with or conspiracy to commit, attempt to commit and aiding and abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.[11]

In Nigeria, the Money Laundering (Prevention and Prohibition) Act (MLA), 2022 in defining money laundering as an offence provides that money laundering occurs where any person or body corporate, whether within or outside Nigeria, who, directly or indirectly, conceals or disguises the origin of, converts or transfers, removes from the jurisdiction, or acquires, uses, retains, or takes possession or control of any fund or property. This must be done intentionally, knowingly, or in circumstances where reasonable knowledge should have been possessed,

[11] General Assembly Resolution 55/25 of November 15, 2000 (New York: United Nations, 2004).

indicating that such fund or property is, or forms part of, the proceeds of an unlawful act. Money laundering, under this Act, encompasses a wide range of actions aimed at obscuring the origins of unlawfully obtained funds or assets.[12]

The Nigerian courts have also attempted a definition of money laundering. The Court of Appeal in *Orji Uzor Kalu & Ors v Federal Republic of Nigeria*,[13] the court adopted the definition of money laundering offered by Graham et al. in the book 'Money Laundering as "varied means used by criminals to conceal the origin of illicit activities. The term 'laundering' is used because these techniques are intended to turn 'dirty' money into 'clean' money, but laundering is not confined to cash"'[14]

All these definitions share common elements, highlighting the deliberate concealment of illegally obtained funds and their transformation into seemingly legitimate assets. However, the evolving nature of money laundering necessitates ongoing efforts to refine and adapt legal definitions and frameworks to address emerging challenges. Comprehensive definitions and international cooperation remain essential in the ongoing fight against money laundering and its broader implications for the global financial landscape.

3.0 STAGES OF MONEY LAUNDERING

The primary objectives of money launderers revolve around two key aspects. Firstly, they endeavour to conceal the illicit origins of the wealth generated through criminal activities, creating hurdles for law enforcement agencies attempting to trace the source. Secondly, they strive to furnish criminals with the means to enjoy their unlawfully acquired riches by funnelling them into legitimate investments, thus conferring an appearance of legitimacy. These dual aims underpin the complex and clandestine world of money laundering.[15] Consequently, for criminals to successfully launder money, it must go through three main stages – Placement, Layering, and Integration.

3.1 Placement

The first stage is placement which starts the moment the illegal proceeds enter the financial markets. This process often involves discreetly reintroducing the funds into circulation

[12] Section18 (2).
[13] (2014)1 NWLR (pt 1389) 479 at 529 CA.
[14] T Graham , E Beil, and N Elliot, *Money Laundering* (Butterworths Lexis- Nexis.2002) 3.
[15] G Stessens, *Money laundering: a new international law enforcement model* (Cambridge University Press 2000) 83.

through formal financial institutions, both at home and abroad.[16] This can be accomplished through single or multiple transactions, utilizing one or several bank deposits or the acquisition of easily tradable assets like bonds or shares.[17] The primary objective of the money launderer during this phase is to distance the cash from its initial point of acquisition, evading detection by authorities, and subsequently converting it into different forms of assets.[18]

In cases where criminal activities yield substantial profits, those involved must devise strategies to manage the funds discreetly, without drawing attention to the illicit activities or the individuals implicated. Given the transnational nature of money laundering, cash can often be moved across borders, with a common technique at the placement stage involving the division of funds into smaller sums for effortless deposit into multiple accounts.[19] However, it is important to note that there are a variety of techniques that money launderers use in placing illicit gains into the system as they are constantly on the lookout for new ways to defeat anti-money laundering regimes.

While placement is generally seen as the first stage of money laundering, it is not always the case, especially in cases such as cybercrime which do not require placement because they sit directly at the heart of the financial system.[20] Placement becomes a pivotal concern when there's a necessity to funnel illicit funds into the legitimate financial framework, as financial institutions play a pivotal role in money laundering schemes.[21] This initial stage aims to transition unlawfully acquired assets from their source into alternative forms that can be subsequently layered and veiled, representing a fundamental element of the money laundering process.

Placement can occur by mixing unlawfully obtained funds with legally acquired ones, like depositing cash gained from corrupt activities into lawful businesses;[22] smurfing, which involves breaking down large sums of currency into smaller amounts and depositing them

---

[16] J Ulph, *Commercial fraud: civil liability, human rights and money laundering* (Oxford University Press 2006).
[17] J McNally, 'Money laundering methodology' in Toby Graham (Ed.) *International Guide to Money Laundering Law and Practice.* (2nd edn, Elsevier Science 2003) 2.
[18] M O Amali, 'Curbing Money Laundering: Global Reception and Implementation of International Anti Money Laundering Standards- A case study on Nigeria.' (PhD thesis, University of Huddersfield 2016).
[19] Ibid
[20] FATF. July 2018. FATF report: professional money laundering. Retrieved on Oct.7, 2023 from <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Professional-money-laundering.html>
[21] M A Nasir, 'Money laundering: Analysis on the placement methods' (2016) 11(5) International Journal of Business, Economics and Law 32-40.
[22] R Booth et al., *Money laundering law and regulation: A practical guide* (Oxford University Press 2011) 3.

across multiple bank accounts to circumvent reporting regulations;[23] acquiring a sequence of financial instruments, such as cashier's checks or money orders, and subsequently gathering them for deposit into accounts at different locations or financial institutions; importing goods at intentionally inflated prices, with the actual price being deposited offshore and subsequently repatriated at the discretion of the perpetrators;[24] and smuggling or shipping large quantities of currency out of a country.[25]

In order to effectively combat money laundering, heightened vigilance is crucial to prevent or detect money laundering during the placement stage. Increased vigilance at this stage is essential to safeguard and uphold financial integrity within the Nigerian financial system. This can be accomplished through strict adherence to necessary due diligence measures, including robust implementation of "know your customer," customer due diligence, and enhanced due diligence as essential practices that must be rigorously followed.

3.2 Layering

The second stage after placement is layering. This involves the creation of a sophisticated web of financial transactions designed to be layered one after the other, with the aim of evading detection. Various methods are employed during this stage as money launderers may opt to invest in high-value assets like automobiles or jewellery and export them to different jurisdictions. Alternatively, they may purchase shares of companies on the stock market. It's the phase where the true source of the money is concealed, making it challenging to uncover. Once cash is successfully integrated into the financial system, money launderers can engage in a myriad of complex transactions, underscoring the importance of the placement stage in combating money laundering. Subsequently, the layering phase allows launderers to commingle illicit proceeds with legitimate ones through intricate financial manoeuvres, creating layers of transactions to obscure the money's origin.[26]

The layering stage plays a crucial role in concealing the money's true origin, rendering it challenging to detect or uncover. Layering is of paramount significance in the money laundering process as it marks the initial steps toward legitimizing unlawfully acquired

[23] E E Esoimeme, *The money laundering laws/regulations in Nigeria, United States and United Kingdom* (DSC Publishing 2014) 3.
[24] E P Akpala and H O Amusu, 'Money laundering and other financial crimes' (Paper presented at the Bank Examination Conference held at CBN Training Centre on 9th October, 1997).
[25] A J Ikpang, 'A critical analysis of the legal mechanisms for combating money laundering in Nigeria' (2011) 1 (1) *African Journal of Law and Criminology* 116 -130.
[26] A Bachus, 'From drugs to terrorism: The focus shifts in the international fight against money laundering after September 11, 2001' (2004) 21(3) *Arizona Journal of International & Comparative Law* 842.

funds.[27] In essence, the concept revolves around making the illicit funds appear legitimately acquired through intricate transactions. A money launderer who has succeeded in the initial placement stage often progresses to this more intricate phase. This underscores the thesis's argument that the first stage offers authorities a better opportunity to detect money laundering activities. The layering stage, on the other hand, can be exceedingly complex, making it challenging and, in some instances, impossible to identify the money launderer and their activities.

3.3 Integration

Integration is the last stage in the money laundering process. At this stage, the unlawfully acquired proceeds have been securely placed, mixed with lawful funds, and stand prepared to be reintroduced to the launderer via lawful channels, emerging as clean and entirely legal assets. This furnishes the criminal with a credible source of wealth to reference in the event of scrutiny by law enforcement or regulatory authorities. Therefore, the third and final stage in the money laundering cycle, known as the integration stage, serves as a mechanism through which the unlawful gains re-enter the economy, portraying themselves as entirely legitimate. Consequently, this disrupts the efforts of law enforcement to discern between illegal and legal funds, rendering the illicit proceeds virtually.[28]

In the integration phase, the launderer may opt to allocate the funds into real estate, financial endeavours, or luxury assets. As the integration stage unfolds, discerning between legal and illicit wealth becomes exceptionally challenging. This stage offers the launderer the opportunity to augment their wealth using the proceeds of unlawful activities. Detection of integration activities is generally elusive unless significant disparities emerge between an individual's or company's legitimate employment, business, or investment undertakings and the individual's wealth or the company's income and assets.[29]

Important to note that while placement, layering, and integration are commonly referred to as the stages of money laundering, they are not conclusive of the process of money laundering. There are numerous instances of money laundering deviating significantly from the conventional money laundering cycle, especially with the rise of cyber laundering. Along

[27] F Schneider, 'Money laundering: Some fact' (2008) 26(3) *European Journal of law and Economics* 387.
[28] Amali. (2016) op. cit.
[29] U Nwosu-Iheme, 'A critical assessment of the efficacy of the Nigerian anti-money laundering legal and institutional frameworks for politically exposed persons' (PhD thesis, *Durham University* 2021). Available at Durham E-Theses Online: http://etheses.dur.ac.uk/14121/

with the development of cyber laundering comes innovative ways of laundering money. Rather than the common stages of money laundering – placement, layering, and integration, new techniques are employed to obfuscate digital footprints in illicit transactions. These methods include the utilization of mixing/tumbler services, encryption, proxy servers, and virtual private networks (VPNs).[30]

4.0 HISTORICAL ROOTS OF MONEY LAUNDERING IN NIGERIA

The exact date money laundering started in Nigeria cannot be ascertained, however, there is evidence to show that money laundering has been in Nigeria as far back as the 1980s during the period marred by the oil boom's downturn due to plummeting global oil prices and the subsequent implementation of austerity measures tied to the country's structural adjustment program.[31] The regime of General Sani Abacha (1993 to 1998) ushered in a notorious era of money laundering in Nigeria.

Throughout General Sani Abacha's rule from 1993 to 1998, Nigeria's financial system experienced a profound crisis. This turmoil stemmed from the inability of financial oversight bodies and law enforcement agencies to thwart the systemic abuse driven by the military and their associates.[32] During Abacha regime funds were frequently funnelled out of the central bank.[33] Approximately between three billion to five billion US dollars ($3,000,000,000 - $5,000,000,000) were believed to have been embezzled by General Abacha, his family, and their associates and these ill-gotten gains were subsequently laundered through bank accounts in Switzerland, the United States of America, and various European nations.[34]

In a bid to counter the tarnished reputation of Nigeria as a transit country for drug trafficking, which posed a threat to its financial system, the military regime took action by signing and ratifying the United Nations Convention on Illicit Trafficking of Drugs and Psychotic Substances (the 1988 Vienna Convention). This pivotal moment led to the introduction of the

---

[30] L Troeller, 'Bitcoin and Money Laundering' (2016) 36(1) Boston University - Review of Banking & Financial Law 159–174.

[31] U Kama, 'The economic effects of money laundering on the Nigerian economy: some emerging issues' (2005) 43(1) Economic and Financial Review 23-50.

[32] E Monfrini, 'The Abacha's Case,' in *Recovering Stolen Assets*, Mark Pieth (ed.), Peter Lang, Bern (2008). Retrieved on Oct. 8, 2023 from <https://mbk.law/useruploads/ordonsfiles/081130_-_monfrini_article_for_recovering_stolen_assets_-_the_abacha_case.pdf>

[33] N L Mbonu, 'A critical appraisal of the legal and institutional framework for combating money laundering in Nigeria.' (LL.M Thesis. University of Buckingham Law School 2016). Retrieved on Oct. 5 2023 from <https://www.academia.edu/35736660/A_CRITICAL_APPRAISAL_OF_THE_LEGAL_AND_INSTITUTIONAL_FRAMEWORK_FOR_COMBATING_MONEY_LAUNDERING_IN_NIGERIA>

[34] J Rupert, 'Corruption flourished in Abacha's regime' *Washington Post*, June 1998. Retrieved on Oct. 8, 2023 from <http://www.washingtonpost.com/wp-srv/inatl/longterm/nigeria/stories/corrupt060998.htm>

first anti-money laundering legislation during their rule. Additionally, the government enacted the National Drug Law Enforcement Agency (Establishment) Decree 1995, tasked with enforcing both anti-drug trafficking and anti-money laundering provisions within the decree. This agency was created under the National Drug Law Enforcement Agency to combat these illicit activities effectively.[35] However, despite the enactment of this law, little was done in regard to its implementation and no one was convicted for the offence of money laundering.

Sanctions imposed by the Financial Action Task Force (FATF) led to Nigeria's placement on the Non-Cooperating Countries and Territories list (NCCT) due to its inadequate anti-money laundering measures. The government aimed to remove Nigeria from the NCCT list to restore its international reputation, marred by its inability to combat organized crime, including drug trafficking, money laundering, advanced fee fraud, cybercrime, and illegal oil bunkering.[36] As a response to these concerns, Nigeria enacted the Independent Corrupt Practices Commission Act (ICPC) in 2000 and the Economic and Financial Crimes Commission Act (EFCC) in 2003. These Acts led to the establishment of the ICPC and EFCC as the primary agencies responsible for enforcing anti-money laundering laws and other related economic and financial crimes regulations.[37] The subsequent response, including the establishment of anti-corruption agencies, reflects Nigeria's ongoing efforts to combat money laundering and related financial crimes.

5.0 GAPS IN THE MONEY LAUNDERING (PREVENTION AND PROHIBITION) ACT, 2022

The Money Laundering Prohibition (Prevention and Prohibition) Act (MLA) 2022 is not a sacrosanct law and it is replete with some gaps which make it generally insufficient to tackle money laundering generally. This is without prejudice to the main focus of this paper which has to do with the commission of money laundering offence in the digital space, and it is going to be separately addressed below with its own peculiar challenges. The noticeable gaps in the MLA which show its current inadequacies in combating money laundering generally are discussed as follows:

1. **Obscure Reporting Obligations for International Transfers under Section 3(1) and (2)**

[35] N L Mbonu op. cit.
[36] Ibid.
[37] Ibid.

One notable gap within the MLA 2022 revolves around the reporting obligations associated with international transfers of funds and securities exceeding US $10,000.00. Sections 3(1) and (2) of the Act establish the imperative to report such transactions to regulatory bodies, namely the Central Bank of Nigeria (CBN), the Securities and Exchange Commission, or the Economic and Financial Crimes Commission (EFCC) within one day of the transaction.

However, a critical ambiguity emerges as the Act fails to expressly specify the entity or entities legally obligated to fulfil this reporting requirement. This lack of clarity raises significant uncertainties regarding whether the duty to report substantial transactions is incumbent upon the sender, the recipient, or the relevant financial institution involved in the transaction. Consequently, this ambiguity introduces a potential loophole that could be exploited by individuals seeking to circumvent mandatory disclosure requirements. The loophole might be exploited under the pretext that they anticipated other involved parties to discharge the reporting obligation.

In contrast, Sections 3(3) and (4) of the Act delineate a distinct reporting responsibility, assigning the task of reporting the transportation of cash or negotiable instruments exceeding US$10,000.00 by individuals to the CBN and the EFCC. [38] Despite this specificity, the broader lack of clarity on reporting obligations for international transfers poses a significant challenge to effective enforcement and may undermine the Act's objectives in combating money laundering.

This identified gap underscores the pressing need for precise statutory provisions, outlining the responsible party or parties obligated to report international transfers, aligning the Act with international standards, and fortifying its efficacy in combatting money laundering activities.

2. Lack of protection for whistle-blowers

Whistle-blowers play a crucial role in exposing illicit financial activities, including money laundering. They often have insider information that can lead to the detection and prevention of financial crimes. One noteworthy instance of whistleblowing in Nigeria involves a young individual who disclosed information leading to the recovery of funds at Flat 7B Osborne Towers, Ikoyi, Lagos State, on April 7, 2017.[39] The recovered funds, comprising foreign and

[38] FRN v Bashir Abdu (unreported FHC/KN/CR/210/2012); FRN v Umar Musa Kibiya (unreported FHC/KN/CR/193/2012) and FRN v Idris Hamza (unreported FHC/KN/CR/196/2012)

[39] E Okogba, 'Courts orders Forfeiture of Ikoyigate Apartment, $43m cash' (Vanguard, Nov. 9, 2017). Retrieved on Jan 11, 2023 from <https://www.vanguardngr.com/2017/11/court-orders-forfeiture-ikoyigate-

domestic currencies, were valued at ₦13,000,000,000.00 at that time. Thus, whistle-blowers play a crucial role in exposing financial crimes, including money laundering, by bringing forth vital information that authorities may otherwise not discover. However, the absence of adequate protection for whistle-blowers poses a significant challenge to the effectiveness of the Money Laundering Act. The reluctance of individuals to blow the whistle, stemming from the fear of reprisals and lack of legal safeguards, undermines the objectives of the Money Laundering Act.

The real-life cases of Joseph Akeju and Joseph Ameh, who faced persecution, dismissal, and personal hardships after exposing corruption within their organizations highlight the effect of whistleblowing. When Akeju, a former bursar at Yaba College of Technology, initially declined to participate in a "loot" in 2009, he got into trouble. After being fired for his "principled stance," Akeju was eventually restored in 2016 by then-education minister Adamu Adamu seven and a half years after. He suffered a second dismissal when he raised an alarm that a whooping sum of 1.6 Billion Naira was missing from the coffer of the college and consequently suffered many tribulations.[40] Ameh, an architect, was terminated from his position after petitioning against alleged contract fraud within his institution.[41] These cases vividly illustrate the harsh consequences whistle-blowers endure, creating a chilling effect on others contemplating exposing financial misconduct. The lack of explicit legal protections makes potential whistle-blowers vulnerable to threats, job loss, and personal harm, discouraging them from reporting suspicious activities related to money laundering.[42]

To enhance the effectiveness of the Money Laundering Act, it is imperative to institute robust whistle-blower protection measures. A legal framework that shields whistle-blowers from retaliation, ensures anonymity, and provides avenues for redress can encourage individuals to come forward with crucial information. By fostering a safe environment for whistle-blowers, authorities can tap into a valuable resource that strengthens the fight against money laundering and upholds the integrity of financial systems.

3. Overlooking the Impact of Technological Advancements

apartment-43-m-cash/>

[40] D Shibayan, 'Inside Story: Death threats, job losses – Nigerian whistleblowers who risked everything for public interest' (Premium Times March 16, 2023). Retrieved on Jan 11th 2024 from <https://www.premiumtimesng.com/news/top-news/587877-inside-story-death-threats-job-losses-nigerian-whistleblowers-who-risked-everything-for-public-interest.html>

[41] Ibid.

[42] Ibid.

While the Act's incorporation of virtual assets[43] represents a positive step forward, by recognizing the digital nature of these assets and their potential role in financial crimes. However, there is a need for more detailed provisions to specifically address the challenges posed by cryptocurrencies and other virtual assets, ensuring effective regulation and prevention measures. Given the evolving nature of financial crimes, continuous updates and adaptation to new technologies used in money laundering are essential. A comprehensive analysis reveals that the Act may still overlook certain crucial aspects related to technological advancements and their impact on money laundering.

Firstly, despite the Act's acknowledgement of virtual assets, it falls short in providing specific provisions on the impact of blockchain technology. Blockchain, integral to many virtual assets, plays a vital role in ensuring or compromising transaction transparency. The Act should address this gap by incorporating measures that recognize and regulate the use of blockchain in financial transactions. Furthermore, while the recent amendments focus on virtual assets, the Act lacks explicit provisions to counter the use of AI and machine learning in illicit activities. Criminals increasingly leverage these technologies to automate money laundering processes. Enhancing the Act to include measures against AI-driven financial crimes will bolster its effectiveness in combating evolving threats.

The Act's expansion to include virtual assets is a positive step, but it still overlooks the specific challenges posed by digital identities and deep fakes. Money launderers can manipulate identities and create false personas, leading to illicit financial activities. Strengthening provisions related to digital identities will fortify the Act's ability to combat identity-related money laundering. Lastly, while the Act emphasizes risk management, it lacks explicit provisions related to robust cybersecurity measures. Given the rise of cyber-enabled financial crimes, especially involving virtual assets, incorporating specific cybersecurity provisions is essential to protect against potential threats and breaches.

The inclusion of virtual assets in the Money Laundering Act is a positive development, however, there is room for improvement to address specific technological aspects. Regular updates, amendments, and a comprehensive approach that considers blockchain, AI, cybersecurity, and data analytics will ensure the Act remains resilient in combating increasingly sophisticated money laundering tactics facilitated by evolving technologies. This

[43] Section 30, MLA 2022

comprehensive analysis calls for a forward-looking approach to legislation, aligning it with the rapid pace of technological advancements in the financial landscape.

4. Absence of provisions for international collaboration

The absence of provisions for international collaboration within the Money Laundering Act constitutes a significant gap that can substantially impede the effectiveness of the legislation. Here are several ways in which the lack of international cooperation provisions can hinder the efficacy of the Money Laundering Act. Firstly, money laundering often involves the movement of funds across multiple jurisdictions. Without specific provisions for international collaboration, the act may struggle to trace and monitor cross-border transactions effectively. Criminals can exploit jurisdictional gaps, making it challenging for authorities to follow the flow of illicit funds across borders.

In addition, international cooperation is essential for sharing intelligence and information on money laundering activities. Criminal networks frequently operate on a global scale, and effective collaboration between states enables the pooling of resources and expertise. The absence of provisions for such collaboration hampers the timely exchange of crucial information, hindering the ability to uncover and dismantle transnational money laundering operations.

Complex money laundering schemes often require joint investigations involving law enforcement agencies from multiple countries. In the absence of provisions facilitating international collaboration, the Money Laundering Act may lack the mechanisms to support seamless cooperation between different jurisdictions. This limitation can result in fragmented efforts and hinder the thorough investigation of transnational financial crimes.

Furthermore, money launderers frequently move assets across borders to conceal their illicit gains. Without provisions for international collaboration, efforts to trace and recover these assets become less effective. Coordination between states is crucial for freezing and repatriating funds acquired through money laundering activities, and the absence of such provisions hampers these efforts. Criminals may exploit regulatory differences between countries, engaging in regulatory arbitrage to take advantage of jurisdictions with weaker anti-money laundering controls. The absence of provisions for international collaboration leaves regulatory disparities unaddressed, creating opportunities for money launderers to exploit gaps in the global regulatory framework.

The absence of provisions for international collaboration among states in the Money Laundering Act undermines its effectiveness by limiting the ability to trace cross-border transactions, share critical intelligence, conduct joint investigations, trace and recover assets, address regulatory disparities, and maintain a strong deterrent against transnational financial crimes. Addressing this gap is crucial for creating a comprehensive and robust legal framework to combat money laundering on a global scale.

6.0 MONEY LAUNDERING IN THE DIGITAL AGE

In the past, money laundering was primarily linked to complex transaction networks, shell corporations, and offshore bank accounts. However, the landscape has significantly transformed with the advent of technology and digital advancements, empowering criminals to exploit these developments and discover innovative methods to launder their illicit funds. Consequently, the financial sector faces fresh financial risks, with the prevalence of money laundering extending into the realm of technological innovations. This expansion includes digital currencies, e-wallets, prepaid cards, and mobile and internet payment services.[44]

Technological advancements have reshaped the landscape of money laundering, enabling criminals to operate with unprecedented sophistication and anonymity. The rise of digital currencies, e-wallets, and innovative payment services has added new dimensions to this financial crime, allowing illicit actors to exploit the ease of cross-border transactions and evade traditional Anti-Money Laundering regulations. As financial regulators grapple with the challenges posed by decentralized platforms and anonymous digital transactions, it becomes evident that adapting anti-money laundering strategies to this evolving landscape is essential. Money laundering is a phenomenon that has posed challenges to many nations of the world and the fight against it in the digital age requires a coordinated international effort, robust regulatory frameworks, and innovative solutions to safeguard the integrity of global financial systems.[45]

Technological innovations have interconnected the world, providing criminal organizations with the ability to commit crimes globally, taking advantage of regions with lax AML

[44] U Anichebe, 'Combating money laundering in an age of technology and innovation' SSRN (2020). Available at <https://dx.doi.org/10.2139/ssrn.3627681>

[45] M A Araromi, 'Regulation of virtual currencies in select jurisdictions: giving Nigeria a sense of direction' (2018) 24(1) Computer and Telecommunications Law Review 13-26, 22.

regulations and enforcement. Technology facilitates the inconspicuous transfer of dirty money across multiple global regions with ease, ushering in a structural shift in black market operations. Global money laundering syndicates can now efficiently employ virtual currencies for transaction layering.

The case of Ramon Abbas, known as Ray Hushpuppi, serves as a compelling illustration of global money laundering. Abbas, a prominent social media figure, received an 11-year prison sentence and was mandated to provide substantial restitution for his role in laundering millions of illicitly obtained dollars. The FBI's Los Angeles division characterized him as "among the most prolific money launderers worldwide." Abbas, of Nigerian origin, along with a Canadian associate, engaged in money laundering stemming from various online criminal activities, including cyber heists and business email deceptions. These unlawful pursuits involved infiltrating email accounts, misleading victims, and rerouting funds to deceptive repositories.[46]

A particularly noteworthy incident involved their participation in laundering $14.7 million pilfered by North Korean hackers from a Maltese bank, with the funds being discreetly channelled through financial institutions in Romania and Bulgaria. Additionally, Abbas contributed to the laundering of substantial sums of British pounds embezzled from a UK corporation and a professional football club. He was also implicated in defrauding an individual in Qatar who had been seeking a loan for a school project.[47] This case underscores the inherently transnational character of money laundering, where wrongdoers capitalize on worldwide financial networks and digital platforms to transfer illegal funds beyond borders.

6.1 Virtual and Digital Currencies

When it comes to money laundering in the digital age, several methods have been devised, however, the most predominant method is the use of virtual and digital currencies. Virtual and digital currencies are typically the preferred choice in scenarios where anonymity and transaction privacy are highly regarded, particularly in illegal trade activities. The FATF defined virtual currencies as:

---

[46] 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams,' DOJ, United States Attorney's Office, Central District of California Press Release, Nov. 7, 2022. Retrieved on Feb. 12, 2024 from <https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions>

[47] Influencer 'Ray Hushpuppi' jailed over plan to launder $300m.' (*The Guardian*. Nov. 8, 2022). Retrieved on Oct. 17, 2023 from <https://www.theguardian.com/law/2022/nov/08/influencer-ray-hushpuppi-jailed-money-laundering-ramon-abbas-fbi>

> a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.[48]

The FATF further defines digital currencies as *a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency"[49]* While digital currencies such as cryptocurrencies are unlikely to supplant the traditional banking system, their increasing prevalence introduces a range of novel security concerns.[50] In contrast to "fiat" currencies, which are recognized as legal tender and are the primary medium of exchange within issuing nations, virtual currencies exist without a sovereign backing and lack physical form.[51]

Rather than relying on traditional financial institutions and centralized structures, cryptocurrencies utilize a digital ledger, called a blockchain, to maintain stability and ensure transaction integrity.[52] Blockchain possesses several key characteristics: decentralization, persistence, and anonymity. Unlike traditional centralized systems where a central authority (e.g., a central bank) validates transactions, blockchain eliminates the need for a third party, using consensus algorithms to ensure data consistency across the distributed network and avoiding cost and performance bottlenecks. Users interact with the blockchain using generated addresses that do not disclose their real identities.[53]

Digital currency like eCache, a digital gold currency, offers money launderers the advantage of operating in the shadows of anonymity, as it doesn't mandate users to furnish personal

---

[48] 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' FATF Report 2014. Retrieved on May 25, 2024 from <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf>
[49] Ibid
[50] C Leuprecht, C Jenkins, and R Hamilton, 'Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency' (2023) 30(4) Journal of Financial Crime 1036-1054.
[51] Ibid
[52] D Adachi and J Aoyagi, 'Blockchain and economic transactions' *Cryptocurrency and Blockchain Technology* (De Gruyter. 2020) 9-22.
[53] Z Zheng et al.. 'An overview of blockchain technology: architecture, consensus, and future trends' (*ResearchGate* 2017) Retrieved on May 28, 2024 from <https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends/citation/download>

information.[54] Similarly, even though all bitcoin transactions are permanently recorded in its underlying technology, the blockchain, users of bitcoin, the pioneering, renowned, and lucrative cryptocurrency, often maintain anonymity. This anonymity is achieved by leveraging various technologies that conceal online activities, such as dark wallets and onion routers, which obscure the internet protocol addresses of bitcoin users, effectively shielding their identities.[55]

The digital era continues to reveal the shortcomings of AML regulations. Unlike legitimate exchanges, many digital platforms, including cryptocurrency exchanges, lack administrators or central authorities and often neglect to implement sufficient KYC (Know Your Customer) procedures for their users. This deficiency significantly contributes to money laundering, as cryptocurrencies move across markets and flow into unregulated exchanges without proper user identity verification. Presently, financial regulators in various jurisdictions are struggling to keep pace with the technological progress underpinning digital currencies. States grapple with tracking covert transactions in these systems. Traditional financial institutions adhere to regulations, enabling scrutiny of suspicious transactions. In contrast, digital currencies elude this oversight, hindering access to records and fund tracing due to their decentralized nature, and lack a central authority.[56]

The recent case of Eze Harrison Arinze exemplifies the challenges faced by law enforcement agencies in combating money laundering through digital currencies. His sophisticated scheme, involving the fraudulent acquisition of bitcoins from victims across 13 countries, underscores the cross-border nature of cryptocurrency-based financial crimes.[57] Arinze allegedly received $382,000 worth of bitcoins from his victims, which were obtained through fraudulent means, constituting the initial phase of money laundering. The victims were deceived into withdrawing their funds and depositing them into Arinze's Bitcoin accounts, believing they were engaging in legitimate transactions. In reality, they were facilitating the laundering of illicitly obtained funds. Bitcoin transactions offer a level of anonymity, making it challenging to trace the source and destination of funds. The victims in this case were from 13 different

[54] U Anichebe (2020) op. cit.
[55] Ibid
[56] R C Hellvig & C A Blanaru, 'Impact of globalization on money laundering' (2023) XI (32) SEA – Practical Application of Science 93.
[57] R Anyebe '$382,000 Fraud: How suspected fraudster duped his victims from 13 countries in Bitcoins scam' *Kanyidaily.com*. Retrieved on Oct. 23, 2023, from <https://www.kanyidaily.com/2023/05/382000-fraud-how-suspected-fraudster-duped-his-victims-from-13-countries-in-bitcoins-scam.html?feed_id=8536&_unique_id=645a7e35ec956>

countries, demonstrating the cross-border nature of cryptocurrency-based money laundering. This characteristic complicates tracking and detection efforts.

Arinze was accused of using multiple Bitcoin wallet addresses to receive and transfer funds. This fragmentation of transactions across various wallets can obscure the flow of funds and hinder tracking efforts - a common tactic in cryptocurrency-based money laundering. Arinze is alleged to have impersonated the owner of an investment platform to solicit funds from victims for cryptocurrency investments. These investments were obtained under false pretences, and the funds were subsequently laundered through Bitcoin transactions. Arinze faces legal charges related to money laundering, false pretence, and fraud, which are indicative of the illegal and fraudulent nature of his activities. These charges are typically associated with cryptocurrency-based money laundering schemes. Arinze's case is being prosecuted by the Economic and Financial Crimes Commission (EFCC), emphasizing the importance of law enforcement agencies in investigating and prosecuting cryptocurrency-related financial crimes.[58]

This case underscores the challenges law enforcement faces in combating money laundering through digital currencies. The inherent features of cryptocurrencies, such as anonymity and cross-border transactions, make it a preferred choice for money launderers. Effective regulation and international cooperation are crucial to addressing the illicit use of digital currencies in financial crimes.

7.0 IMPLICATIONS FOR NIGERIA

The advent of technology and digital innovation has significant implications on money laundering in Nigeria. Digital currencies such as cryptocurrency are particularly advantageous for the layering stage of money laundering due to its virtual nature, which places it beyond the control of any single jurisdiction. This allows for the seamless international transfer of funds, conversion between different cryptocurrencies or fiat currencies, and facilitates trading or investment activities. By leveraging cryptocurrency, financial criminals can effectively obscure the origin of their illicit funds, moving money across borders until the connection to the original crime is effectively severed.[59]

[58] Ibid.
[59] C Leuprecht, C Jenkins, and R Hamilton, 'Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency' (2023) 30(4) Journal of Financial Crime 1036-1054.

The global reach of virtual currencies significantly heightens their potential AML/CFT risks. These systems, accessible via the Internet and mobile devices, enable cross-border payments and fund transfers. Virtual currencies often depend on complex infrastructures involving multiple entities across various countries to transfer funds or execute payments. This fragmentation of services can obscure responsibility for AML/CFT compliance and enforcement. Additionally, customer and transaction records are frequently dispersed among different entities in various jurisdictions, complicating access for law enforcement and regulators.[60] The challenge is further intensified by the rapidly evolving nature of decentralized virtual currency technologies and business models, including the diverse and changing participants in virtual currency payment systems. Components of these systems may be situated in jurisdictions with inadequate AML/CFT controls. Centralized virtual currency systems might intentionally operate in areas with weak regulatory regimes. Decentralized, convertible virtual currencies facilitate anonymous person-to-person transactions, potentially existing in a digital realm beyond the reach of any single country's regulatory framework.[61]

In the context of Nigeria, these transnational implications pose significant challenges for the country's financial system and regulatory authorities. Nigeria's growing digital economy and increasing adoption of cryptocurrencies make it a potential hotspot for money laundering activities. Criminals can exploit the lack of uniform international regulations and Nigeria's less stringent enforcement to move illicit funds in and out of the country. This not only undermines Nigeria's financial integrity but also exposes it to international sanctions and loss of investor confidence. Therefore, it is crucial for Nigerian authorities to enhance their AML/CFT frameworks, collaborate with international bodies, and adopt advanced technological solutions to effectively monitor and combat cross-border money laundering facilitated by digital currencies.

8.0 REGULATORY DEVELOPMENTS IN NIGERIA IN THE WAKE OF CYBER LAUNDERING

[60] 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' FATF Report 2014. Retrieved on May 25, 2024 from <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf>

[61] 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' FATF Report 2014. Retrieved on May 25, 2024 from <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.coredownload.pdf>

While Nigeria's regulatory landscape regarding digital currencies has evolved significantly in response to the challenges posed by cyber laundering, it is important to note that Nigeria does not have a defined law that governs digital currencies. The regulation of digital assets, including cryptocurrencies, is an area of law and policy that is developing swiftly. In Nigeria, this regulatory framework is still in its infancy, with the Central Bank of Nigeria (CBN) and the Securities and Exchange Commission (SEC) spearheading the efforts.[62] This lack of regulatory clarity has created a challenging environment in which digital currencies are being utilized without clear legal guidance.

1. The Central Bank of Nigeria

The Central Bank of Nigeria (CBN) in February 2021 issued a circular that effectively banned banks and financial institutions from providing services to cryptocurrency exchanges and users.[63] This move was primarily motivated by concerns related to money laundering, fraud, and other illicit activities associated with cryptocurrencies. While the intention behind these regulations was to address these concerns, the result was a shift in the cryptocurrency landscape. Instead of comprehensive regulations, the CBN's circular created a void in which cryptocurrency-related transactions and activities operated with limited oversight, often via peer-to-peer trading.

In response to these developments, the CBN released new guidelines in December 2023 aimed at Virtual Assets Service Providers (VASPs), introducing stringent standards and requirements for banking relationships within the digital asset sector.[64] By establishing minimum standards for risk management and monitoring of VASPs' activities, the CBN seeks to enhance the integrity of the financial system and mitigate the risks of money laundering associated with virtual assets. These guidelines demonstrate the CBN's commitment to adapting regulatory frameworks to address emerging challenges posed by the digital age, particularly in combating financial crimes facilitated by digital currencies. Furthermore, the alignment of these guidelines with international standards, such as the recommendations of the Financial Action Task Force (FATF), underscores Nigeria's efforts to stay abreast of

[62] 'Cryptocurrency Trading: CBN Orders Banks to Close Operating Accounts' CBNUPDATE. ISSN No 2695-2394 Vol. 3 No. 2, February 2021. Retrieved on Oct. 24 2023 from <https://www.cbn.gov.ng/out/2021/ccd/volume%203%20number%202%20cbn%20update%20february%202021.pdf>
[63] Ibid
[64] J Emejo and N Ekeghe, 'CBN issues fresh guidelines on cryptocurrency operation' (Jan. 4, 2024). Retrieved on March 21, 2024 from <https://www.arise.tv/cbn-issues-fresh-guidelines-on-cryptocurrency-operation/>

global regulatory trends and enhance its anti-money laundering capabilities in the digital realm.

Furthermore, the CBN introduced a regulatory sandbox in 2023 to support innovation in blockchain and fintech payment systems.[65] This sandbox offers a controlled environment where fintech startups and financial institutions can test new blockchain-based products and services while ensuring adherence to existing guidelines. This initiative demonstrates the CBN's commitment to embracing fintech innovation and promoting the development of blockchain technology. Additionally, the regulatory sandbox helps mitigate potential money laundering risks by allowing thorough testing and regulatory compliance checks before new technologies are fully implemented in the financial system.

However, the critical need for clear and comprehensive legislation regarding the use of digital currencies in Nigeria remains evident. While the CBN's actions were aimed at curbing money laundering and fraud, the unintended consequence was a potential resurgence of unregulated and anonymous cryptocurrency trading, creating opportunities for bad actors. Effective regulation would provide a framework to address money laundering concerns, enforce anti-money laundering (AML) measures, and set guidelines for cryptocurrency exchanges to follow KYC (Know Your Customer) procedures.

In the era of blockchain innovation, governments are introducing digital fiat currencies like the eNaira (Nigeria) and the Sand Dollar (Bahamas). The Central Bank of Nigeria (CBN), discerning these from privately issued cryptocurrencies, has placed restrictions on crypto transactions through domestic banks and financial institutions, citing their intrinsic volatility and absence of government support. Importantly, the deliberate exclusion of traceable digital fiat currencies from the virtual asset definition is a strategic measure. This recognizes their traceability, guaranteeing thorough coverage of reporting requirements, especially when surpassing specified thresholds, under the Act and pertinent legislation.[66]

2. The Securities and Exchange Commission

[65] Olisa Agbakoba Legal (OAL), 'Blockchain and cryptocurrency regulations: navigating the evolving landscape in Nigeria' (March 21, 2024). Retrieved on May 21, 2024 from <https://oal.law/blockchain-and-cryptocurrency-regulations-navigating-the-evolving-landscape-in-nigeria/#_ftn8>

[66] 'An overview of the Key Provisions of the Money Laundering (Prevention and Prohibition) Act 2022' PWC (2022). Retrieved on Dec. 20, 2023 from <https://www.pwc.com/ng/en/assets/pdf/regulatory-alert-an-overview-of-the-money-laundering-act-2022.pdf>

To regulate innovation within the digital asset sector, the Securities and Exchange Commission (SEC) introduced the New Rules on Issuance, Offering Platforms, and Custody of Digital Assets, which were published on 21st May 2022. This regulation represents a positive move towards ensuring that digital assets are exchanged and securely maintained in compliance with the law. The rules address the following areas:

a) Issuance of Digital Assets as Securities
b) Registration Requirements for Digital Asset Offering Platforms (DAOPs)
c) Registration Requirements for Digital Asset Custodians (DACs)
d) Virtual Asset Service Providers (VASPs)
e) Digital Asset Exchanges (DAX)[67]

PART A of the Rules governs the issuance of digital assets as securities, applying to all issuers seeking to raise capital through such offerings. Digital assets are defined as "digital tokens representing assets such as a debt or equity claim on the issuer." Issuers must register these assets in accordance with the Rules, beginning with an initial assessment under Rule 4. If the SEC determines that the digital assets qualify as securities under the ISA 2007, they must be registered following Rule 5, which involves submitting an application with the requisite information and documents. This process is crucial for preventing fraud and ensuring compliance with anti-money laundering (AML) regulations. PART B outlines the registration requirements for Digital Asset Offering Platforms (DAOPs), which must be registered with the SEC. Applicants must meet requirements including the payment of fees, submission of SEC Forms, and evidence of a minimum paid-up capital of N500 million with a fidelity bond covering at least 25% of this amount. These measures ensure that DAOPs are financially robust and adhere to regulatory standards, supporting effective AML measures.

PART C addresses the registration requirements for Digital Asset Custodians (DACs), defined as entities providing safekeeping services for virtual assets. DACs must comply with the general requirements for Virtual Asset Service Providers (VASPs) and specific custodial regulations. The SEC may register foreign DACs if they are authorised in their home jurisdictions and those jurisdictions have comparable regulatory arrangements with the SEC, ensuring stringent AML standards. PART D focuses on VASPs, entities involved in exchanging, transferring, and safeguarding virtual assets, as well as providing related

[67] A Omolumo, 'An overview of SEC's rules on issuance, offering platforms and custody of digital assets 2022' (Feb. 8, 2023) *Mondaq*. Retrieved on May 22, 2024 from <https://www.mondaq.com/nigeria/fin-tech/1280304/an-overview-of-secs-rules-on-issuance-offering-platforms-and-custody-of-digital-assets-2022>

financial services. VASPs must be structured as corporate bodies and obtain SEC licenses to operate legally, with the registration process detailed in Rule 4. These regulations enhance AML efforts by ensuring VASPs operate within a regulated framework. Finally, PART E outlines rules for Digital Asset Exchanges (DAX), requiring operators to comply with DAX-specific and general VASP requirements, including financial stability measures like a minimum paid-up capital of N500 million and a fidelity bond. These stringent requirements promote transparency and accountability, supporting AML initiatives by reducing the risk of money laundering in digital asset transactions.

On March 15, 2024, the SEC released its proposed amendments to its existing rules on the issuance, offering platforms, and custody of digital assets. The Proposed Rules by the SEC introduce several key measures to bolster AML regulations in the digital age. They mandate that all virtual asset service providers (VASPs) be registered with the SEC, extend the definition of virtual assets to include cryptocurrencies, and require local incorporation with the Chief Executive Officer (CEO) or Managing Director resident in Nigeria for better regulatory oversight. The rules also call for business separation for existing Capital Market Operators (CMOs) and higher financial thresholds for DAOPs and DAXs, ensuring only well-capitalized entities operate. Additionally, the rules stipulate that DAX operators must prevent self-dealing by ensuring the same account holder is not on both sides of a transaction and require the use of the CBN's official exchange rate for foreign currency conversions. Lastly, entities seeking to register as digital asset custodians must demonstrate their capacity to safeguard assets effectively. These measures collectively enhance transparency, accountability, and security in the digital asset market, significantly mitigating the risk of money laundering.

3. The Money Laundering (Prevention and Prohibition) Act, 2022

The legislative milestone of the Money Laundering (Prevention and Prohibition) Act, 2022, signed into law by then-President Muhammadu Buhari on May 13, 2022,[68] represents a significant step forward in enhancing Nigeria's anti-money laundering framework. Notably, the Act recognizes virtual assets and expands the definition of Financial Institutions (FIs) to encompass Virtual Asset Service Providers (VASPs), reflecting the transformative landscape of fund transfers amid technological disruptions. Section 30 of the Act defines virtual asset as

[68] 'President Buhari assents to three bills to combat financial crimes, terrorism' (May 19, 2022) Policy and Legal Advisory Centre. Retrieved on March 21, 2024 from <https://placng.org/Legist/president-buhari-assents-to-three-bills-to-combat-financial-crimes-terrorism/>

a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes but does not include digital representations of fiat currencies, securities and other financial assets. However, it's crucial to note that this excludes digital representations of fiat currencies, securities, and other financial assets.

The Act further broadens its reach by expanding the definition of Financial Institutions (FIs) to encompass Virtual Asset Service Providers (VASPs). Recognizing the transformative landscape of fund transfers amid technological disruptions, this expansion bridges critical gaps left by the repealed Act.

4. Government Action Against Crypto Firms

Recently, the Nigerian government, through the Nigerian Communications Commission (NCC), blocked the online platforms of Binance and other cryptocurrency firms like Forextime, OctaFX, Crypto, FXTM, Coinbase, and Kraken. This measure aims to prevent ongoing forex market manipulation and the illicit movement of funds. Nigerian authorities have accused Binance of manipulating exchange rates through speculation and rate-fixing, contributing to the naira's devaluation. Additionally, it was reported that the Federal Government detained at least two senior Binance executives who had arrived in Nigeria following the ban on their website. These executives were arrested by officials from the Office of the National Security Adviser, and their passports were confiscated.[69]

Notably, in March 2024, speculations on Nigeria fining Binance, a global cryptocurrency company, up to $10bn reached the news, after Nigerian authorities alleged that the company engaged in exploitation, depreciation of the national currency, and money laundering.[70] These allegations highlight the regulatory challenges faced by Nigerian authorities in overseeing cryptocurrency activities and underscore the importance of robust frameworks to address potential exploitation and illicit financial activities.

The evolving regulatory environment in Nigeria highlights the critical need for more robust and comprehensive regulations to effectively address the challenges posed by digital currencies. Many countries have taken significant steps to implement regulations aimed at combating money laundering in the digital age. The UK has implemented the Digital Asset

---

[69] D Aina, 'FG detains two Binance executives' (Feb. 29, 2024) *Punch*. Retrieved on May 22, 2024 from <https://punchng.com/fg-detains-two-binance-executives-report/>

[70] T Obiezu, 'Nigeria's cryptocurrency crackdown will have consequences, experts say' (March 11, 2024) VOA. Retrieved on March 21, 2024 from <https://www.voanews.com/a/nigeria-s-cryptocurrency-crackdown-will-have-consequences-experts-say/7523302.html>

Anti-Money Laundering Act, which includes stringent requirements for the registration and regulation of digital asset service providers to enhance transparency and accountability in digital transactions. The U.S. has introduced the Anti-Money Laundering Act of 2020, which expands the definition of financial institutions to include virtual asset service providers (VASPs) and mandates comprehensive reporting and compliance obligations to prevent illicit activities involving cryptocurrencies. Japan has established a robust regulatory framework through the Payment Services Act[71] and the Financial Instruments and Exchange Act,[72] requiring cryptocurrency exchanges to register with the Financial Services Agency (FSA) and adhere to strict anti-money laundering (AML) and know-your-customer (KYC) protocols. Switzerland's Financial Market Supervisory Authority (FINMA) has set forth guidelines for the regulation of digital assets, emphasizing AML compliance and requiring VASPs to conduct thorough KYC checks and report suspicious activities. The EU has adopted the Fifth Anti-Money Laundering Directive (5AMLD), which extends AML obligations to cryptocurrency exchanges and wallet providers, requiring them to register with national authorities and implement KYC and reporting procedures.

These examples underscore the necessity for Nigeria to develop clear and enforceable laws to ensure the integrity of its financial system and protect against illicit activities facilitated by digital assets. Effective regulation will provide a framework to address money laundering concerns, enforce AML measures, and set guidelines for cryptocurrency exchanges to follow KYC procedures, thereby enhancing the overall security and stability of the digital financial ecosystem.

CONCLUSION

In conclusion, the evolving landscape of money laundering in the digital age presents significant challenges for Nigeria's financial system and broader economy. From the historical roots of money laundering to its transformation in cyberspace, the gravity of this illicit activity cannot be overstated. The proliferation of cyber laundering, coupled with the rise of digital currencies, underscores the urgent need for comprehensive strategies and robust regulatory measures to combat financial crimes effectively.

---

[71] No. 59, 2009.
[72] Enacted in 2006 but became effective in April 20008.

As Nigeria grapples with regulatory developments and enforcement challenges in the wake of cyber laundering, it is imperative to prioritize the following recommendations:

1. **Enhance Regulatory Frameworks**: Nigeria must develop clear and comprehensive legislation governing the use of digital currencies. These regulations should include stringent anti-money laundering (AML) measures, know-your-customer (KYC) procedures, and guidelines for cryptocurrency exchanges to ensure compliance and accountability.
2. **Strengthen International Cooperation**: Collaboration with international organizations, law enforcement agencies, and other jurisdictions is essential in combating cross-border money laundering activities. Nigeria should actively participate in initiatives for information-sharing, mutual legal assistance treaties, and joint task forces to enhance global efforts against financial crimes.
3. **Invest in Technological Solutions:** Embracing technological innovations such as blockchain analytics and artificial intelligence can strengthen Nigeria's capabilities in detecting and preventing money laundering in the digital age. Investing in training and resources for law enforcement agencies and regulatory bodies is crucial to leverage these tools effectively.
4. **Promote Public Awareness and Education**: Educating the public about the risks associated with digital currencies and cyber laundering is essential in fostering a culture of compliance and vigilance. Public awareness campaigns, workshops, and educational programs can empower individuals to recognize and report suspicious activities.
5. **Encourage Responsible Innovation**: While regulating digital currencies is necessary, Nigeria should also encourage responsible innovation in the fintech sector. Supporting legitimate cryptocurrency projects and fostering an ecosystem of compliant and transparent financial services can promote financial inclusion while mitigating risks of illicit activities.

In implementing these recommendations, Nigeria can strengthen its anti-money laundering framework, safeguard the integrity of its financial system, and contribute to global efforts in combating financial crimes. The challenges posed by money laundering in the digital age are formidable, but with proactive measures and concerted efforts, Nigeria can navigate this evolving landscape and emerge stronger and more resilient.