SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

THE LIMITS OF MONEY LAUNDERING LAWS AND RISK CONTROL MEASURES

A COMPARATIVE ANALYSIS OF APPROACHES TO IMPLEMENTING THE FINANCIAL ACTION TASK FORCE RECOMMENDATIONS

By Ehi Eric Esoimeme

A DISSERTATION

Presented to the Department of

International Public Law program

at Selinus University

Faculty of Arts & Humanities

in fulfillment of the requirements for the degree of

Doctor of Philosophy in International Public Law

2022

ABSTRACT

A diverse mix of regulations and standards have been developed to counter money laundering and terrorist financing. Most significant amongst these are the Recommendations of the Financial Action Task Force (FATF), an inter-governmental body established in 1989 at the G7 summit in Paris as a result of the growing concern over money laundering.

Although countries have followed the advice of the FATF by enacting laws that require financial institutions and designated non-financial businesses and professions (DNFBPs) to implement certain measures that can combat money laundering and terrorist financing, the approaches adopted in these different countries are not identical.

This research compared the approaches adopted in Nigeria, the United States and the United Kingdom in relation to money laundering offences, customer due-diligence measures, politically exposed persons, cash couriers, record keeping, reporting requirements, compliance officers and confiscation measures. The aim of this comparison is to determine the best approach. This is likely the one that protects the integrity of the financial system against money launderers and terrorist financiers, and reduces the risk of money laundering and terrorist financing to the barest minimum.

This research determined that legal and strategic reforms were necessary to strengthen Nigeria's anti-money laundering and countering the financing of terrorism (AML/CFT) measures to make it more effective. This research concludes that effective implementation of anti-money laundering measures, including customer due diligence, enhanced due diligence, recordkeeping, account monitoring and suspicious activity reporting with artificial intelligence enabled systems will protect the financial system

against money launderers and terrorist financiers, and reduce the risk of money laundering and terrorist financing to the barest minimum.

KEYWORDS: Money Laundering, Terrorist Financing, Customer Due Diligence, PEPs, Cash Couriers, Record Keeping, Reporting, Compliance Officer, Plea Bargain, Artificial Intelligence, Independent Testing

TABLE OF CONTENT

INTRODUCTION

The Financial Action Task Force (FATF) Recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction.

Although countries have followed the advice of the FATF by enacting laws that require financial institutions and designated nonfinancial businesses and professions (DNFBPs) to implement certain measures that can combat money laundering and terrorist financing, the approaches adopted in these different countries are not identical.

A. RESEARCH QUESTIONS

This research intends to explore the following questions:

1. Are the present anti-money laundering and countering the financing of terrorism (AML/CFT) measures of Nigeria problematic?
2. If yes, what lessons can Nigeria learn from other Jurisdictions whose AML/CFT systems have been rated very high in effectiveness by the Financial Action Task Force (FATF)?
3. What are the additional measures that financial institutions in Nigeria can adopt to strengthen their AML/CFT systems and controls?

B. OBJECTIVES OF THE STUDY

This research compares the approaches adopted in Nigeria, the United States and the United Kingdom in relation to money laundering offences, customer due-diligence measures, politically exposed persons, cash couriers, record keeping, reporting requirements, compliance officers and confiscation measures. The aim of this comparison is to determine the best approach. This is likely the one that protects the integrity of the financial system against money launderers and terrorist financiers, and reduces the risk of money laundering and terrorist financing to the barest minimum.

C. RESEARCH METHODOLOGY

This research will rely on primary and secondary sources drawn from the public domain.

In order to understand the present AML/CFT measures in Nigeria, this research will review information from primary sources e.g., legislative bills, statutes and guidelines. Information from secondary sources e.g. academic writings and media writings will also be reviewed to determine if the present AML/CFT measures in Nigeria are effective.

In order to fully understand the AML/CFT measures in the United Kingdom and the United States, this research will analyse information from primary sources e.g. statutes, regulations, strategies, administrative decisions, etc., relevant to the AML/CFT measures in those jurisdictions. Information from Secondary sources e.g. research articles and media writings will also be reviewed to determine the level of effectiveness of the prohibitive and preventive measures. If the laws or measures are working, this research will recommend it for implementation in Nigeria. The United Kingdom and the United States were chosen based on the fact that most of the proceeds of corruption from

Nigeria are laundered there.[1] The countries were also chosen because of their risk scores on the 2021 Basel AML Index published by the Basel Institute on Governance.[2] The Basel AML Index measures the risk of money laundering and terrorist financing (ML/TF) in jurisdictions around the world.[3]

D. ORIGINALITY/VALUE

Several books have been published on Money Laundering and Terrorist Financing. Notable amongst them are Nicholas Ryder's *Money Laundering–An Endless Cycle?: A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada* (Routledge 2013); Ehi Eric Esoimeme's *A Comparative Study of the Money Laundering Laws/Regulations in Nigeria, the United States and the United Kingdom* (Eric Press 2014); Waleed Alhosani's *Anti-Money Laundering: A Comparative and Critical Analysis of the UK and UAE's Financial Intelligence Units* (Palgrave Macmillan 2016); and Ehi Eric Esoimeme's '*Deterring and Detecting Money Laundering and Terrorist Financing: A Comparative Analysis of Anti–Money Laundering and Counterterrorism Financing Strategies'*, (DSC Publications Ltd 2018).

Although the aforementioned books adopted the comparative approach. Those publications focused mainly on technical compliance with the Financial Action Task Force Recommendations. This research thesis is focused on both the principles and the

[1] Daily Post (2018), *'Abacha's loot: What Nigerian govt agreed with UK, US – AGF, Malami'*, Available at: http://dailypost.ng/2018/06/20/abachas-loot-nigerian-govt-agreed-uk-us-agf-malami/ (accessed 16th of February, 2019); Reuters (2017), *'Swiss to return $321 million in stolen funds to Nigeria'*, Available at: https://www.reuters.com/article/us-swiss-nigeria/swiss-to-return-321-million-in-stolen-funds-to-nigeria-idUSKBN1DY2T1 (accessed 16th of February, 2019).
[2] Basel Institute on Governance, *'Basel AML Index 2021'*, (https://baselgovernance.org 2021), Available at: https://baselgovernance.org/publications/basel-aml-index-2021 (accessed 4 July 2022).
[3] Ibid.

practical aspect of its application. Also, this research critically reviews the most recent AML/CFT laws and risk control measures of Nigeria, the United States and the United Kingdom.

The mechanisms/measures which will be discussed extensively in this research thesis with the proposed reforms will help financial institutions to identify, assess and understand their money laundering and terrorist financing risks, and take commensurate measures in order to mitigate them.

E. THE PLAN

Chapter 1 introduces readers to what money laundering is. In addition to defining money laundering and highlighting the different international bodies charged with fighting it, the chapter breaks down the money laundering risk-assessment process in a way that anyone who is interested can understand.

Chapter 2 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to money laundering offences. The comparison is done under four subheadings: 'The Crime of Money Laundering', 'Predicate Offences for Money Laundering (Domestic Crimes)', 'Predicate Offences for Money Laundering (Foreign Crimes)' and 'Penalties'.

Chapter 3 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to customer due-diligence measures.

Chapter 4 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to politically exposed persons (PEPs) under the subheading 'Application of the PEP Definition'.

Chapter 5 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to cash couriers under the subheading 'Declaration System'.

Chapter 6 is a critical analysis of the rule-based approach that is applied to record-keeping requirements. The analysis is done under the subheading 'The Risk-Based Approach to Record-Keeping Requirements'.

Chapter 7 compares the reporting requirements in Nigeria with those of the United States and the United Kingdom to determine whether Nigeria needs to adopt the approach of these countries or if there is no need for reform. This comparison is done under five different subheadings: 'What to File', 'Where to File', 'When to File', 'Confidentiality of Suspicious Activity Reports' and 'Penalties'.

Chapter 8 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to compliance officers. The comparison is done under two subheadings: 'The Title of the Individual Responsible for Anti–Money Laundering Compliance' and 'Duties and Responsibilities'.

Chapter 9 compares the approaches in Nigeria, the United States and the United Kingdom as they relate to the application of the concept of plea bargaining**.**

The concluding chapter presents a summary of the findings and recommendations of this research. It will also expound on the additional strategies and controls that can strengthen Nigeria's anti-money laundering and countering the financing of terrorism (AML/CFT) measures to make it more effective.

CHAPTER 1

MONEY LAUNDERING AND TERRORIST FINANCING: A COMPREHENSIVE OVERVIEW

Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects. From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economies. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and ultimately, hide the actual purpose of their activity.[4]

1.1 WHAT IS MONEY LAUNDERING?

Money laundering is the criminal practice of processing ill-gotten gains, or 'dirty' money, through a series of transactions; in this way the funds are 'cleaned' so that they appear to be proceeds from legal activities.[5]

Money laundering requires an underlying, primary, profit-making crime (such as corruption, drug trafficking, market manipulation, fraud, tax evasion), along with the intent to conceal the proceeds of the crime or to further the criminal enterprise. These

[4] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 11.
[5] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 12.

activities generate financial flows that involve the diversion of resources away from economically- and socially-productive uses—and these diversions can have negative impacts on the financial sector. They also have a corrosive, corrupting effect on society and the economic system as a whole.[6]

Money laundering takes many forms, including:

i. Trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);
ii. Handling the benefit of acquisitive crimes such as theft, fraud and tax evasion;
iii. Handling stolen goods;
iv. Being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
v. Criminals investing the proceeds of their crimes in the whole range of financial products.[7]

1.2 STAGES OF MONEY LAUNDERING

Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously;

1.2.1 PLACEMENT

The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention

[6] International Monetary Fund, '*Anti-Money Laundering/Combating the Financing of Terrorism*' (https://www.imf.org) https://www.imf.org/external/np/leg/amlcft/eng/ Accessed 28th September 2014.
[7] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2022, 7.

of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises.[8]

This can be done when a person deposits an amount below ten thousand US dollars in the bank. The intention would be to evade reporting requirements.

It is worth noting that Banks are mandated to file Currency Transaction Reports when a person deposits an amount equivalent to ten thousand US dollars or more than ten thousand US dollars.

1.2.2 LAYERING

The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail.[9]

A person who was successful in the placement stage is likely to move to this stage which appears to be more complex.

Such a person is likely to transfer part of the amount deposited, into other accounts to avoid being detected.

1.2.3 INTEGRATION

The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is

[8] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 12.
[9] Ibid.

used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds.[10]

This could happen when a person who deposited illegal funds in the bank withdraws the money and uses the money to purchase a house or any other movable or immovable property.

1.3 TERRORIST FINANCING

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations.[11]

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

[10] Ibid.
[11] Ibid.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking (e.g., "hawala") have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.[12]

1.4 ANTI-MONEY LAUNDERING RISK ASSESSMENT

Financial institutions and designated non-financial businesses and professions (DNFBPs) are required to take appropriate steps to assess their money laundering and terrorist financing risks.

A well-developed risk assessment will assist in identifying the bank's Anti-Money Laundering (AML) risk profile. Understanding the risk profile enables the bank to apply appropriate risk management processes to the AML compliance programme to mitigate

[12] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 13.

risk. This risk assessment process enables management to better identify and mitigate gaps in the bank's controls. The risk assessment should provide a comprehensive analysis of the AML risks in a concise and organized presentation and should be shared and communicated with all business lines across the bank, board of directors, management, and appropriate staff; as such, it is a sound practice that the risk assessment be reduced to writing.[13]

The development of the AML risk assessment generally involves two steps: first, identify the specific risk categories (i.e., products, services, customers, entities, transactions, and geographic locations) unique to the bank; and second, conduct a more detailed analysis of the data identified to better assess the risk within these categories.[14]

1.4.1 IDENTIFICATION OF SPECIFIC RISK CATEGORIES

The first step of the risk assessment process is to identify the specific products, services, customers, entities, and geographic locations unique to the bank. Although attempts to launder money, finance terrorism, or conduct other illegal activities through a bank can emanate from many different sources, certain products, services, customers, entities, and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular product, service, or customer, the risks are not always the same. Various factors, such as the number and volume of transactions, geographic locations, and nature of the customer relationships, should be considered when the bank prepares its risk assessment. The differences in the way a bank interacts with the customer (face-to-

[13] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 22.
[14] Ibid.

face contact versus electronic banking) also should be considered. Because of these factors, risk will vary from one bank to another.[15]

1.4.1.1 PRODUCTS AND SERVICES

Certain products and services offered by banks may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents. Some of these products and services includes amongst others; Private Banking, Electronic Funds Payment Services, Trade Finance and Foreign Exchange.[16]

1.4.1.2 CUSTOMERS AND ENTITIES

The amount of corruption and abuse of public funds by some government leaders and public officials over recent years have given great cause for concern both internationally as well as in countries involved. Those people are collectively known as politically exposed persons (PEPs).[17] PEPs are individuals who are or have been entrusted with prominent public functions and an immediate family member or a known close associate of such a person.[18]

---

[15] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 23.

[16] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 24.

[17] D Hopton, *Money Laundering: A Concise Guide for All Business* (2nd Edition Gower 2009) 108

[18] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12. See also Directive 2005/60/EC of the European Parliament and of the council of 26th October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Article 3 (8). See also the Money Laundering, Terrorist Financing and Transfer of Funds (Information on

There are special challenges in entering into financial transactions and business relationships with PEPs. Typical customer due diligence (CDD) measures may prove insufficient for PEPs as financial transactions and business relationships with these individuals present a higher money laundering risk and hence require greater scrutiny than ''normal'' financial transactions and business accounts.[19]

Other customers/entities that may pose a higher money laundering risk includes amongst others: money service businesses, casinos, card clubs, brokers/dealers in securities, non-resident aliens (NRA), off shore corporations and non-governmental organizations.[20]

1.4.1.3 GEOGRAPHIC LOCATIONS

Identifying geographic locations that pose a higher risk is essential to a bank's AML compliance programme. Financial institutions/DNFBPs should understand and evaluate the specific risk associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations.[21]

Higher-risk geographic locations can be either international or domestic. International higher-risk geographic locations generally include: Countries subject to the Office of Foreign Assets Control (OFAC) sanctions, including state sponsors of terrorism, Jurisdictions or countries monitored for deficiencies in their regimes to combat money

---

the Payer) Regulations 2017, Regulation 35(4)(b). See also the Joint Money Laundering Steering Group *Guidance for the UK Financial Sector* Part 1, Paragraph 5.5.15.

[19] KKR Choo, *'Politically exposed persons (PEPs): risk and mitigation'* 2008, 11 (4) JMLC, 371 – 387'

[20] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010,* 25.

[21] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 25.

laundering and terrorist financing by international entities such as the Financial Action Task Force (FATF).[22]

Domestic higher-risk geographic locations include: High Intensity Drug Trafficking Areas (HIDTA) and High Intensity Financial Crime Areas (HIFCA)[23]

1.4.2 ANALYSIS OF SPECIFIC RISK CATEGORIES

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess AML risk.

This step involves evaluating data pertaining to the bank's activities (e.g., number of: domestic and international funds transfers; private banking customers; foreign correspondent accounts; and domestic and international geographic locations of the bank's business area and customer transactions) in relation to CDD information.

The detailed analysis is important because within any type of product or category of customer there will be account holders that pose varying levels of risk.

Specifically, the analysis of the data pertaining to the bank's activities should consider, as appropriate, the following factors:

i. Purpose of the account;
ii. Actual or anticipated activity in the account;
iii. Nature of the customer's business/occupation;

[22] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 26.
[23] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 26, 27.

iv. Customer's location;

v. Types of product and services used by the customer.[24]

1.4.3 DEVELOPING THE BANK'S AML COMPLIANCE PROGRAMME BASED UPON ITS RISK ASSESSMENT

Management should structure the bank's AML compliance programme to adequately address its risk profile, as identified by the risk assessment.

The bank's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, customers, entities and geographic locations as identified by the bank's AML risk assessment.[25]

This section explains in more detail how the risk-based approach can be applied.

It explains this by using PEPs as an example.

1.4.3.1 CUSTOMER DUE DILIGENCE

Customer Due Diligence/know your customer is intended to enable a financial institution to form a reasonable belief that it knows the true identity of each customer and, with an

[24] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 27.
[25] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 28.

appropriate degree of confidence, knows the type of transactions the customer is likely to undertake.[26]

Failure of firms taking adequate steps to identify PEPs may lead to corrupt PEPs opening accounts without being detected and in the process avoiding enhanced due diligence and on-going monitoring. For example, in the late 1980's a large multinational bank in London opened accounts for Ibrahim and Mohamed Sani Abacha, who represented themselves as ''Commodity and Oil dealers'' The bank failed to make note of the Father's position at the time as a General in the Army. By the late 1990's it was discovered that the two brothers had amassed and deposited, either for themselves or on behalf of others, approximately six hundred and sixty million dollars with the London bank. It was later revealed that Sani Abacha brothers and other members of the Abacha circle had allegedly stolen an estimated four billion, three hundred million dollars over a number of years.[27]

Another example is the Abubakar Atiku's case. According to the US subcommittee on investigations (2010) report, Abubakar used a variety of schemes through wire transfers to launder suspected funds into the United States. In many cases, these accounts were disguised by using the variant of his wife's name (Ms Douglas). The bank's profile did not identify Ms Douglas as a PEP.[28]

[26] FATF Guidance on the *Risk Based Approach to combating money laundering and terrorist financing*, (High Level principles and procedures) 2007, paragraph 3.10.
[27] OJ Otusanya: *'The Role of offshore financial centres in elite money laundering practices: evidence from Nigeria',* 2012,15(3) JMLC, 336 – 361.
[28] OJ Otusanya: *'The Role of offshore financial centres in elite money laundering practices: evidence from Nigeria.* 2012', 15(3) JMLC, 336 – 361.

In situations where the money laundering risk associated with the business relationship is increased, for example where the customer is a PEP, banks must carry out additional enhanced due diligence.[29]

1.4.3.2 ENHANCED DUE DILIGENCE

The Enhanced Due Diligence (EDD) should give firms a greater understanding of the customer and their associated risk than standard due diligence. It should provide more certainty that the customer and/or beneficial owner is who they say they are and that the purposes of the business relationship are legitimate; as well as increasing opportunities to identify and deal with concerns that they are not.[30]

It is for each firm to decide the steps it takes to determine whether a PEP is seeking to establish a business relationship for legitimate reasons. Firms should in any case take adequate meaningful measures to establish the source of funds and source of wealth. Firms may wish to refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests. Firms should note that not all declarations are publicly available and that a PEP

[29] The Financial Action Task Force (FATF): International Standards On Combating Money Laundering and the financing of terrorism and proliferation,(The FATF Recommendations) 2012, Recommendation 12, See also Directive 2005/60/EC of the European Parliament and of the council of 26th October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Article 13 (1), See also the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 33, see also Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001, s 312 (1).

[30] Financial crime: a guide for firms part 1: *A firm's guide to preventing financial crime by the Financial Services Authority* 2012 Box 3.7. See also Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001 S 312 (2) (B) I, ii which states that the enhanced due diligence policies and procedures enables firms in the United States to ascertain for any such foreign bank, the shares of which are not publicly traded, the identity of each owners of the foreign bank and the nature and extent of the ownership interest of each such owner.

customer may have a legitimate reason for not providing a copy.[31] In countries where the declarations ought to be publicly available and are not still available for example countries like Nigeria who just signed an agreement committing to publication of asset declaration with the U.S. Government,[32] firms should insist that they see the declaration and if they are not given the declaration they should not open the account. It is worth noting that despite the agreement being signed, President Goodluck Jonathan has refused to publicly declare his assets.[33] These poses problems for firms.

Once the source of wealth and source of funds are established, banks will need to analyse the information for ''red flag'' for corrupt PEP activity.[34] In all cases if a bank suspects that the funds are proceeds of criminal activity, the bank is required to file a Suspicious Transaction Report with the Financial Intelligence Unit.[35] A risk based approach for the reporting of suspicious activity under these circumstances is not applicable.[36] A risk based approach is however appropriate for the purpose of identifying suspicious activity, for example by directing additional resources at those areas a financial institution has identified as higher risk and in this case to customers who are identified as PEPs.[37]

[31] Joint Money Laundering Steering Group *Guidance for the UK Financial Sector* Part 1, Paragraph 5.5.28.
[32] O Aigbovo: *Nigerian anti-corruption statutes: an impact assessment* 2013 16 (1) JMLC 62 – 78.
[33] O Aigbovo: *Nigerian anti-corruption statutes: an impact assessment* 2013 16 (1) JMLC 62 – 78.
[34] T S Greenberg: *Stolen Asset Recovery, Politically Exposed Persons, A policy paper on strengthening preventive measures.*
[35] T S Greenberg: *Stolen Asset Recovery, Politically Exposed Persons, A policy paper on strengthening preventive measures.*
[36] FATF Guidance on the *Risk Based Approach to combating money laundering and terrorist financing*, (High Level principles and procedures) 2007, paragraph 3.16.
[37] FATF Guidance on the *Risk Based Approach to combating money laundering and terrorist financing*, (High Level principles and procedures) 2007, paragraph 3.17.

1.4.3.3 SENIOR MANAGEMENT APPROVAL

The FATF standard requires banks to obtain senior management approval for establishing a business relationship with PEPs and continuing a business relationship with a customer who is subsequently found to be a PEP or becomes a PEP.[38] The group's Anti-Money Laundering and Countering Financing of Terrorism (AML/CTF) officer should be involved in the PEP approval process since he is in the best position to say that a person should not be accepted regardless of the size of the account.[39]

1.4.3.4 ENHANCED ONGOING MONITORING

Once a business relationship has been established with a PEP, banks must conduct enhanced on-going monitoring of the business relationship. [40]

The principle aim of monitoring in a risk based system is to respond to enterprise wide issues based on each financial institution's analysis of major risks and in this case the major risks are PEPs.[41]

---

[38] The Financial Action Task Force (FATF): International Standards On Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12, See also Directive 2005/60/EC of the European Parliament and of the council of 26th October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Article 13 (4) (b), See also the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35.

[39] T S Greenberg: *Stolen Asset Recovery, Politically Exposed Persons, A policy paper on strengthening preventive measures.*

[40] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12, See also Directive 2005/60/EC of the European Parliament and of the council of 26th October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing Article 13 (4) (d), See also the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35.

[41] FATF Guidance on the Risk Based Approach to combating money laundering and terrorist financing, (High Level principles and procedures) 2007, paragraph 3.13.

1.4.4 IMPLICATIONS OF FAILURE OF A FIRM TO CONDUCT ENHANCED DUE DILIGENCE (EDD) AND ENHANCED ONGOING MONITORING (EOM)

Firms who do not conduct the required EDD and EOM with PEPs are likely to be fined by the financial supervisor in the jurisdiction concerned. For example, In March 2012, the UK Financial Conduct Authority (FCA) fined Coutts and Company eight million seven hundred and fifty thousand pounds for failing to establish and maintain effective AML systems and controls in relation to their high-risk customers including PEPs. Coutts failed to adequately assess the level of money laundering risk posed by PEPs and also failed to gather sufficient information to establish PEPs such as source of funds and source of wealth.[42]

In May 2012, FCA also fined Habib Bank five hundred and twenty-five thousand pounds and its MLRO seventeen thousand, five hundred pounds for failing to conduct adequate enhanced due diligence on higher risk customers.[43]

Failure of a bank to conduct EDD and EOM may lead to funds being laundered and regulators shutting the bank down as a result of that. An example is the Bank of Credit and Commerce International (BCCI) scandal where the bank's UK operation was closed on 19th July 1991 due to the fact that money was being laundered through the bank.[44] The rise and fall of BCCI was the greatest scandal in the history of banking.[45] The bank

[42] Financial crime: a guide for firms part 1: A firm's guide to preventing financial crime by the Financial Services Authority 2012 Box 3.15.
[43] Financial crime: a guide for firms part 1: A firm's guide to preventing financial crime by the Financial Services Authority 2012 Box 3.16.
[44] P Alldridge *Money Laundering Law, Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the proceeds of crime*. (Hart Publishing 2003) 38.
[45] Bank of credit commerce International SA v. Ali (No 2) 1999 4 ALL ER 83.

became insolvent because of the fraud perpetrated by staffs of the bank who allowed money to be laundered. This also affected the reputation of the bank and public confidence.

1.5 INTERNATIONAL BODIES/ORGANISATIONS

This section of the chapter highlights the different international bodies charged with fighting money laundering.

1.5.1 FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a “policy-making body” which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF's decision making body, the FATF Plenary, meets three times per year.[46]

1.5.2 BASEL COMMITTEE

The Basel Committee (the committee) is the primary global standard-setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability.[47]

The committee has a long-standing commitment to promote the implementation of sound AML/CFT policies and procedures that are critical in protecting the safety and soundness of banks and the integrity of the international financial system.

Following an initial statement in 1988, it has published several documents in support of this commitment. In September 2012, the committee reaffirmed its stance by publishing

[46] Financial Action Task Force, *'About us'* (http://www.fatf-gafi.org) http://www.fatf-gafi.org/pages/aboutus/ Accessed 10th September 2014.
[47] Basel Committee on Banking Supervision, *'About the Basel Committee'* (http://www.bis.org 20th June 2014) http://www.bis.org/bcbs/about.htm Accessed 10th September 2014.

the revised version of the core principles for effective banking supervision, in which a dedicated principle (BCP 29) deals with the abuse of financial services.[48]

1.5.3 THE WOLFSBERG GROUP OF INTERNATIONAL FINANCIAL INSTITUTIONS

The Wolfsberg Group is an association of eleven global banks, which aims to develop financial services industry standards, and related products, for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

The Group came together in 2000, at the **Château Wolfsberg** in north-eastern Switzerland, in the company of representatives from Transparency International, including Stanley Morris, and Professor Mark Pieth of the University of Basel, to work on drafting anti-money laundering guidelines for Private Banking. The Wolfsberg Anti-Money Laundering Principles for Private Banking were subsequently published in October 2000, revised in May 2002 and again most recently in June 2012.

The Group then published a Statement on the Financing of Terrorism in January 2002, and also released the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking in November 2002 and the Wolfsberg Statement on Monitoring Screening and Searching in September 2003. In 2004, the Wolfsberg Group focused on the development of a due diligence model for financial institutions, in co-operation with Banker's Almanac, thereby fulfilling one of the recommendations made in the Correspondent Banking Principles.

[48] Basel Committee on Banking Supervision: *Sound management of risks related to money laundering and financing of terrorism 2014,* Paragraph 2.

During 2005 and early 2006, the Wolfsberg Group of banks actively worked on four separate papers, all of which aim to provide guidance with regard to a number of areas of banking activity where standards had yet to be fully articulated by lawmakers or regulators. It was hoped that these papers would provide general assistance to industry participants and regulatory bodies when shaping their own policies and guidance, as well as making a valuable contribution to the fight against money laundering. The papers were all published in June 2006, and consisted of two sets of guidance: Guidance on a Risk Based Approach for Managing Money Laundering Risks and AML Guidance for Mutual Funds and Other Pooled Investment Vehicles. Also published were FAQs on AML issues in the Context of Investment and Commercial Banking and FAQs on Correspondent Banking, which complement the other sets of FAQs available on the site: on Beneficial Ownership, Politically Exposed Persons and Intermediaries.

In early 2007, the Wolfsberg Group issued its Statement against Corruption, in close association with Transparency International and the Basel Institute on Governance. It describes the role of the Wolfsberg Group and financial institutions more generally in support of international efforts to combat corruption. The Statement against Corruption identifies some of the measures financial institutions may consider in order to prevent corruption in their own operations and protect themselves against the misuse of their operations in relation to corruption. Shortly thereafter, the Wolfsberg Group and The Clearing House Association LLC issued a statement endorsing measures to enhance the transparency of international wire transfers to promote the effectiveness of global anti-money laundering and anti-terrorist financing programmes.

In 2008, the Group decided to refresh its 2003 FAQs on PEPs, followed by a reissued Statement on Monitoring, Screening & Searching in 2009. 2009 also saw the publication of the first Trade Finance Principles and Guidance on Credit/Charge Card Issuing and

Merchant Acquiring Activities. The Trade Finance Principles were expanded upon in 2011 and the Wolfsberg Group also replaced its 2007 Wolfsberg Statement against Corruption with a revised, expanded and renamed version of the paper: Wolfsberg Anti-Corruption Guidance. This Guidance takes into account a number of recent developments and gives tailored advice to international financial institutions in support of their efforts to develop appropriate Anti-Corruption programmes, to combat and mitigate bribery risks associated with clients or transactions and also to prevent internal bribery.

Most recently, focus has expanded to the emergence of new payment methods and the Group published Guidance on Prepaid & Stored Value Cards, which considers the money laundering risks and mitigants of physical Prepaid and Stored Value Card Issuing and Merchant Acquiring Activities, and supplements the Wolfsberg Group Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities of 2009.[49]

1.5.4 INTERNATIONAL MONETARY FUND

The International Monetary Fund (IMF) is an organization of 188 countries, working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world.[50]

During the past 14 years, the IMF's efforts in the area of AML helped shape domestic and international AML/CFT policies. They included over 70 AML/CFT assessments, multiple involvements in Article IV consultations and inputs into the design and implementation of financial integrity-related measures in Fund-supported programs, as

[49] Wolfsberg Group, *'Global Banks: Global Standards'* (http://www.wolfsberg-principles.com/) http://www.wolfsberg-principles.com/ Accessed 28th September 2014.
[50] International Monetary Fund, *'About the IMF'* (http://www.imf.org) http://www.imf.org/external/about/ourwork.htm Accessed 10th September 2014.

well as a large number of capacity development activities, and research projects. The IMF's broad experience in exercising surveillance over members' economic systems, conducting financial sector assessments, and providing capacity development to its member countries has been particularly helpful in providing financial integrity advice in the context of surveillance, evaluating countries' compliance with the international AML/CFT standard and in developing programs to help them address identified shortcomings.

In line with a growing recognition of the importance of financial integrity issues for the IMF, the AML/CFT program has evolved over the years. In 2004, the Executive Board agreed to make AML/CFT assessments and capacity development activities a regular part of IMF work. On June 1, 2011, the Executive Board discussed a report reviewing the evolution of the IMF's AML/CFT program over the past five years and provided guidance as to how to move forward in this area.

Following up on the Executive Board discussion, on December 14, 2012, a Guidance Note on the inclusion of AML/CFT in surveillance and financial stability assessments (FSAs) was issued. It provides a framework to deal with cases where money laundering, terrorism financing, and related crimes are so serious as to threaten domestic stability, balance of payments stability, the effective operation of the international monetary system—in the case of Article IV surveillance, or the stability of the domestic financial system—in the case of FSAs.

On March 12, 2014, the Board reviewed the Fund's AML/CFT strategy. It notably (i) endorsed the revised FATF AML/CFT standard and assessment methodology, (ii) encouraged staff to continue its efforts to integrate financial integrity issues into its surveillance and in the context of Fund-supported programs, when financial integrity

issues are critical to financing assurances or to achieve program objectives, and (iii) decided that AML/CFT issues should continue to be addressed in all FSAPs but on a more flexible basis.

With respect to capacity development, in April 2009, the IMF launched a donor-supported trust fund—the first in a series of Topical Trust Funds (TTF)—to finance capacity development in AML/CFT. This first phase ended in April 2014. In light of the success of the program and of continuing high demand for capacity development in this area, a new five-year phase of the TTF started in May 2014 for a new five-year period. Donors (France, Japan, Luxembourg, the Netherlands, Norway, Qatar, Saudi Arabia, Switzerland and the United Kingdom) have together pledged more than twenty million dollars over the next five years to support this new Phase. As of August 2014, nine projects have already started under the second phase. The TTF complements existing accounts that finance the IMF's AML/CFT capacity development activities in member countries.[51]

1.5.5 THE WORLD BANK

The World Bank is a vital source of financial and technical assistance to developing countries around the world. It is not a bank in the ordinary sense but a unique partnership to reduce poverty and support development. Established in 1944, the World Bank Group is headquartered in Washington, D.C.[52]

[51] International Monetary Fund, *'The IMF and the Fight Against Money Laundering and the Financing of Terrorism'* (https://www.imf.org 5th September 2014)
https://www.imf.org/external/np/exr/facts/aml.htm Accessed 28th September 2014.
[52] The World Bank, *'What we do'* (http://www.worldbank.org)
http://www.worldbank.org/en/about/what-we-do Accessed 10th September 2014.

The World Bank and International Monetary Fund developed a unique Reference Guide to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in an effort to provide practical steps for countries implementing an AML/CFT regime in accordance with international standards. The Guide, authored by Paul Allan Schott, describes the global problem of money laundering and terrorist financing on the development agenda of individual countries and across regions. It explains the basic elements required to build an effective AML/CFT legal and institutional framework and summarizes the role of the World Bank and the International Monetary Fund in fighting money laundering and terrorist financing.

The primary objective of this joint Bank-Fund project is to ensure that the information contained in the Reference Guide is useful and easily accessible by developing countries that are working to establish and strengthen their policies against money laundering and the financing of terrorism. Additionally, this Guide is intended to contribute to global understanding of the devastating consequences of money laundering and terrorist financing on development growth, and political stability and to expand the international dialogue on crafting practical solutions to implement effective AML/CFT regimes.[53]

1.5.6 THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSION

The International Organization of Securities Commissions (IOSCO), established in 1983, is the acknowledged international body that brings together the world's securities

[53] The World Bank, *'Comprehensive Reference Guide to AML/CFT'* (http://web.worldbank.org) http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAML/0,,contentMDK:20746893~menuPK:2495265~pagePK:210058~piPK:210062~theSitePK:396512,00.html Accessed 10th September 2014.

regulators and is recognized as the global standard setter for the securities sector. IOSCO develops, implements, and promotes adherence to internationally recognized standards for securities regulation, and is working intensively with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda.

IOSCO's membership regulates more than 95% of the world's securities markets. Its members include over 120 securities regulators and 80 other securities markets participants (i.e. stock exchanges, financial regional and international organizations etc.). IOSCO is the only international financial regulatory organization which includes all the major emerging markets jurisdictions within its membership.[54]

IOSCO has adopted the principle that regulators should require securities (including derivatives) market intermediaries to have in place policies and procedures designed to minimize the risk of the use of an intermediary's business as a vehicle for money laundering.[55] IOSCO subsequently endorsed principles to address the application of the client due diligence process in the securities industry (CIBO).[56]

1.5.7 INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organization of insurance supervisors and regulators from more than 200 jurisdictions in

[54] The International Organization of Securities Commissions, *'General Information'* (http://www.iosco.org) http://www.iosco.org/about/ Accessed 10th of September 2014.
[55] The International Organization of Securities Commissions: Objectives and Principles of Securities Regulation 2003, Principle 8.5.
[56] The International Organization of Securities Commissions: Principles on Client Identification and Beneficial Ownership for the Securities Industry 2004. See also The International Organization of Securities Commissions: Final Report, Anti Money Laundering Guidance for Collective Investment Schemes 2005, 3.

nearly than 140 countries. In addition to its Members, more than 130 Observers representing international institutions, professional associations and insurance and reinsurance companies, as well as consultants and other professionals participate in IAIS activities.[57]

The IAIS has given AML and CFT high priority. In October 2003 the IAIS approved and issued the *Insurance core principles and methodology*, which revised the core principles for the supervision of insurers. Compliance with the Insurance Core Principles is required for a supervisory system to be effective. In accordance with Insurance Core Principle 28, the Recommendations of the FATF applicable to the insurance sector and to insurance supervision must be satisfied to reach this objective.[58]

1.5.8 TRANSPARENCY INTERNATIONAL

In 1993, a few individuals decided to take a stance against corruption and created Transparency International. Now present in more than 100 countries, the movement works relentlessly to stir the world's collective conscience and bring about change. Much remains to be done to stop corruption, but much has also been achieved, including:

i. the creation of international anti-corruption conventions
ii. the prosecution of corrupt leaders and seizures of their illicitly gained riches
iii. national elections won and lost on tackling corruption
iv. companies held accountable for their behaviour both at home and abroad.[59]

[57] International Association of Insurance Supervisors, *'About the IAIS'* (http://www.iaisweb.org) http://www.iaisweb.org/About-the-IAIS-28 Accessed 10th September 2014.
[58] International Association of Insurance Supervisors: Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism October 2004, Paragraph 3.
[59] Transparency International, Óverview' (http://www.transparency.org) http://www.transparency.org/whoweare/organisation Accessed 10th September 2014.

CHAPTER 2

MONEY LAUNDERING OFFENCE

The Financial Action Task Force (FATF) has advised countries to do the following: (i) criminalize money laundering; (ii) apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences; (iii) extend predicate offences for money laundering to conduct that occurred in another country when it would have constituted a predicate offence had it occurred domestically and (iv) apply effective, proportionate and dissuasive criminal sanctions to natural persons convicted of money laundering.[60]

While countries followed the advice of the FATF by criminalizing money laundering and have implemented all the above recommendations, the approaches taken by these countries are different.

This chapter compares the approaches taken by Nigeria with those of the United States and the United Kingdom under four subheadings: 'The Crime of Money Laundering', 'Predicate Offences for Money Laundering (Domestic Crimes)', 'Predicate Offences for Money Laundering (Foreign Crimes)' and 'Penalties'. This chapter will also analyse issues that arise from the comparison to determine if there is need for reform.

[60] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 3

2.1 THE CRIME OF MONEY LAUNDERING

The FATF has advised countries to criminalise money laundering on the basis of the **United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (the Vienna Convention)** and the **United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).**[61]

The Vienna Convention requires each party to adopt such measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally:

i. The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with **subparagraph (a) of paragraph 1 (Article 3)**, or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;[62]

ii. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with **subparagraph (a) of paragraph 1 (Article 3)** or from an act of participation in such an offence or offences;[63]

[61] Ibid.
[62] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (b) (i)
[63] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (b) (ii)

iii. The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences established in accordance with or from an act of participation in such offence or offences;[64]

iv. The possession of equipment or materials or substances listed in Table I and Table II, knowing that they are being or are to be used in or for the illicit cultivation, production or[65]

v. Publicly inciting or inducing others, by any means, to commit any of the offences established in accordance with this article or to use narcotic drugs or psychotropic substances illicitly;[66]

vi. Participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.[67]

Subparagraph (a) of paragraph 1 (Article 3) of the Vienna Convention lists the following offences:

i. The production, manufacture, extraction; preparation, offering, offering for sale, distribution, sale, delivery on any terms whatsoever, brokerage, dispatch, dispatch in transit, transport, importation or exportation of any narcotic drug or any psychotropic substance contrary to the provisions of the 1961 Convention, the 1961 Convention as amended or the 1971 Convention;

[64] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (c) (i)
[65] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (c) (ii)
[66] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (c) (iii)
[67] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988, Article 3 (1) (c) (iv)

ii. The cultivation of opium poppy, coca bush or cannabis plant for the purpose of the production of narcotic drugs contrary to the provisions of the 1961 Convention and the 1961 Convention as amended;

iii. The possession or purchase of any narcotic drug or psychotropic substance for the purpose of any of the activities enumerated in (i) above;

iv. The manufacture, transport or distribution of equipment, materials or of substances listed in Table I and Table II, knowing that they are to be used in or for the illicit cultivation, production or manufacture of narcotic drugs or psychotropic substances.

The Palermo Convention requires each State Party to adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

i. 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;[68]

ii. 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.[69]

Subject to the basic concepts of its legal system:

[68] United Nations Convention Against Transnational Organized Crime and the Protocol There to 2004, Article 6 (1) (a) (i)

[69] United Nations Convention Against Transnational Organized Crime and the Protocol There to 2004, Article 6 (1) (a) (ii)

iii. The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;[70]

iv. Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.[71]

Although countries have followed the advice of the FATF by criminalising money laundering on the basis of the Vienna Convention and the Palermo Convention, the approaches in these countries are different.

This section compares the approaches in Nigeria with those of the United States and the United Kingdom.

2.1.1 NIGERIA

The Nigerian Money Laundering (Prevention and Prohibition) Act, 2022 makes it a money laundering offence for any person or body corporate in or outside Nigeria, to directly or indirectly:

i. Conceals or disguises the origin of;[72]

ii. Converts or transfers;[73]

iii. Removes from the jurisdiction; or[74]

[70] United Nations Convention Against Transnational Organized Crime and the Protocol There to 2004, Article 6 (1) (b) (i)
[71] United Nations Convention Against Transnational Organized Crime and the Protocol There to 2004, Article 6 (1) (b) (ii)
[72] Money Laundering (Prevention and Prohibition) Act, 2022, s. 18 (2) (a)
[73] Money Laundering (Prevention and Prohibition) Act, 2022, s. 18 (2) (b)
[74] Money Laundering (Prevention and Prohibition) Act, 2022, s. 18 (2) (c)

iv. Acquires, uses, retains or take possession or control of any fund or property, intentionally, knowingly or reasonably ought to have known that such fund or property is, or forms part of the proceeds of an unlawful act;[75]

Commits an offence of money laundering under the Nigerian Money Laundering (Prevention and Prohibition) Act, 2022.

A person also commits the offence of money laundering if he or she:

i. Conspires with, aids, abets or counsels any other person to commit the offence of money laundering;[76]

ii. Attempts to commit or is an accessory to an act or offence of money laundering; or[77]

iii. Incites, procures or induces any other person by any means whatsoever to commit the offence of money laundering.[78]

2.1.2 UNITED STATES

The U.S. Bank Secrecy Act (Statute) (1970) (as amended) is to the effect that:

(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity[79]—

(A)

[75] Money Laundering (Prevention and Prohibition) Act, 2022, s. 18 (2) (d)
[76] Money Laundering (Prevention and Prohibition) Act, 2022, s. 21(a).
[77] Money Laundering (Prevention and Prohibition) Act, 2022, s. 21(b).
[78] Money Laundering (Prevention and Prohibition) Act, 2022, s. 21(c).
[79] Bank Secrecy Act (Statute), s. 1956 (a) (1)

i. With the intent to promote the carrying on of specified unlawful activity; or[80]

ii. With intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or[81]

(B) Knowing that the transaction is designed in whole or in part—

i. To conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or[82]

ii. To avoid a transaction reporting requirement under State or Federal law,[83]

Shall be guilty of the offence of money laundering

A financial transaction shall be considered to be one involving the proceeds of specified unlawful activity if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.[84]

(2) Also, whoever transports, transmits or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States.[85]—

(A) With the intent to promote the carrying on of specified unlawful activity; or[86]

[80] Bank Secrecy Act (Statute), s. 1956 (a) (1) (A) (i)
[81] Bank Secrecy Act (Statute), s. 1956 (a) (1) (A) (ii)
[82] Bank Secrecy Act (Statute), s. 1956 (a) (1) (B) (i)
[83] Bank Secrecy Act (Statute), s. 1956 (a) (1) (B) (ii)
[84] Bank Secrecy Act (Statute), s. 1956 (a) (1) (B)
[85] Bank Secrecy Act (Statute), s. 1956 (a) (2)
[86] Bank Secrecy Act (Statute), s. 1956 (a) (2) (A)

(B) Knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part[87]—

i. To conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or[88]

ii. To avoid a transaction reporting requirement under State or Federal law,[89]

Shall be guilty of the offence of money laundering

(3) Whoever, with the intent—

i. To promote the carrying on of specified unlawful activity;[90]

ii. To conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity; or[91]

iii. To avoid a transaction reporting requirement under State or Federal law,[92]

Conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, or property used to conduct or facilitate specified unlawful activity, shall be guilty of the offence of money laundering.

The term “represented” means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a Federal official authorized to investigate or prosecute violations of this section.[93]

[87] Bank Secrecy Act (Statute), s. 1956 (a) (2) (B)
[88] Bank Secrecy Act (Statute), s. 1956 (a) (2) (B) (i)
[89] Bank Secrecy Act (Statute), s. 1956 (a) (2) (B) (ii)
[90] Bank Secrecy Act (Statute), s. 1956 (a) (3) (A)
[91] Bank Secrecy Act (Statute), s. 1956 (a) (3) (B)
[92] Bank Secrecy Act (Statute), s. 1956 (a) (3) (C)

2.1.3 UNITED KINGDOM

The UK Proceeds of Crime Act 2002 (as amended) makes it a money laundering offence[94] for a person to:

i. Conceal criminal property;[95]

ii. Disguise criminal property;[96]

iii. Convert criminal property;[97]

iv. Transfer criminal property;[98]

v. Remove criminal property from England and Wales or from Scotland or from Northern Ireland;[99]

vi. Enter into or become concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person;[100]

vii. Acquire criminal property;[101]

viii. Use criminal property;[102]

ix. Have possession of criminal property;[103]

x. Attempt, conspire or incite another to commit the above offences;[104]

---

[93] Bank Secrecy Act (Statute), s. 1956 (a) (3)
[94] Proceeds of Crime Act 2002 (as amended), s. 340 (11) (a)
[95] Proceeds of Crime Act 2002 (as amended), s. 327 (1) (a)
[96] Proceeds of Crime Act 2002 (as amended), s. 327 (1) (b)
[97] Proceeds of Crime Act 2002 (as amended), s. 327 (1) (c)
[98] Proceeds of Crime Act 2002 (as amended), s. 327 (1) (d)
[99] Proceeds of Crime Act 2002 (as amended), s. 327 (1) (e)
[100] Proceeds of Crime Act 2002 (as amended), s. 328 (1)
[101] Proceeds of Crime Act 2002 (as amended), s. 329 (1) (a)
[102] Proceeds of Crime Act 2002 (as amended), s. 329 (1) (b)
[103] Proceeds of Crime Act 2002 (as amended), s. 329 (1) (c)
[104] Proceeds of Crime Act 2002 (as amended), s. 340 (11) (b)

xi. Aid, abet, counsel or procure the commission of the above offences.[105]

The act of 'Entering into or becoming concerned in an arrangement which a person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person' is not a money laundering offence in Nigeria and United States but it is a money laundering offence in the United Kingdom as stated above.

2.2 PREDICATE OFFENCES FOR MONEY LAUNDERING (DOMESTIC CRIMES)

The FATF has advised countries to apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.

According to the FATF, Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences, or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.[106]

This section compares the approaches in Nigeria with those of the United States and the United Kingdom.

[105] Proceeds of Crime Act 2002 (as amended), s. 340 (11) (c)

[106] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 3

2.2.1 NIGERIA

The Nigerian Money Laundering (Prevention and Prohibition) Act, 2022 applies the crime of money laundering to a list of predicate offences and also to any other criminal act specified in the Nigerian Money Laundering Law or any other law in Nigeria.[107]

The predicate offences listed in the Nigerian Money Laundering Law includes: participation in an organized criminal group, racketeering, terrorism, terrorist financing, trafficking in persons, smuggling of migrants, sexual exploitation, sexual exploitation of children, illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking, illicit trafficking in stolen goods, corruption, bribery, fraud, currency, counterfeiting, counterfeiting and piracy of products, environmental crimes, murder, grievous bodily injury, kidnapping, hostage taking, robbery or theft, smuggling (including in relation to customs and excise duties and taxes), extortion, forgery, piracy, insider trading and market manipulation.[108]

2.2.2 UNITED STATES

The U.S. Bank Secrecy Act (Statute) applies the crime of money laundering to a list of predicate offences.[109]

The predicate offences listed in the **U.S. Bank Secrecy Act (Statute)** include: an offence under section 32 (relating to the destruction of aircraft), section 37 (relating to violence at international airports), section 115 (relating to influencing, impeding, or retaliating against a Federal official by threatening or injuring a family member), section

[107] Nigerian Money Laundering (Prevention and Prohibition) Act, 2022, s. 18(6).
[108] Nigerian Money Laundering (Prevention and Prohibition) Act, 2022, s. 18(6).
[109] Bank Secrecy Act (Statute), s. 1956 (c) (7) (A), (C), (D), (E) and (F)

152 (relating to concealment of assets; false oaths and claims; bribery), section 175c (relating to the variola virus), section 215 (relating to commissions or gifts for procuring loans), section 351 (relating to congressional or Cabinet officer assassination), any of sections 500 through 503 (relating to certain counterfeiting offenses), section 513 (relating to securities of States and private entities), section 541 (relating to goods falsely classified), section 542 (relating to entry of goods by means of false statements), section 545 (relating to smuggling goods into the United States.), section 549 (relating to removing goods from Customs custody), section 554 (relating to smuggling goods from the United States.), section 555 (relating to border tunnels), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), section 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds), section 793, 794, or 798 (relating to espionage), section 831 (relating to prohibited transactions involving nuclear materials), section 844 (f) or (i) (relating to destruction by explosives or fire of Government property or property affecting interstate or foreign commerce), section 875 (relating to interstate communications), section 922 (l) (relating to the unlawful importation of firearms), section 924 (n) (relating to firearms trafficking), section 956 (relating to conspiracy to kill, kidnap, maim, or injure certain property in a foreign country), section 1005 (relating to fraudulent bank entries), 1006 [2] (relating to fraudulent Federal credit institution entries), 1007 [2] (relating to Federal Deposit Insurance transactions), 1014 [2] (relating to fraudulent loan or credit applications), section 1030 (relating to computer fraud and abuse), 1032 [2] (relating to concealment of assets from conservator, receiver, or liquidating agent of financial institution), section 1111 (relating to murder), section 1114 (relating to murder of United States law enforcement officials), section 1116 (relating to murder of foreign officials,

official guests, or internationally protected persons), section 1201 (relating to kidnaping), section 1203 (relating to hostage taking), section 1361 (relating to wilful injury of Government property), section 1363 (relating to destruction of property within the special maritime and territorial jurisdiction), section 1708 (theft from the mail), section 1751 (relating to Presidential assassination), section 2113 or 2114 (relating to bank and postal robbery and theft), section 2252A (relating to child pornography) where the child pornography contains a visual depiction of an actual minor engaging in sexually explicit conduct, section 2260 (production of certain child pornography for importation into the United States), section 2280 (relating to violence against maritime navigation), section 2281 (relating to violence against maritime fixed platforms), section 2319 (relating to copyright infringement), section 2320 (relating to trafficking in counterfeit goods and services), section 2332 (relating to terrorist acts abroad against U.S. nationals), section 2332a (relating to use of weapons of mass destruction), section 2332b (relating to international terrorist acts transcending national boundaries), section 2332g (relating to missile systems designed to destroy aircraft), section 2332h (relating to radiological dispersal devices), section 2339A or 2339B (relating to providing material support to terrorists), section 2339C (relating to financing of terrorism), or section 2339D (relating to receiving military-type training from a foreign terrorist organization) of this title, section 46502 of title 49, U.S. Code, a felony violation of the Chemical Diversion and Trafficking Act of 1988 (relating to precursor and essential chemicals), section 590 of the Tariff Act of 1930 (19 U.S.C. 1590) (relating to aviation smuggling), section 422 of the Controlled Substances Act (relating to transportation of drug paraphernalia), section 38 (c) (relating to criminal violations) of the Arms Export Control Act, section 11 (relating to violations) of the Export Administration Act of 1979, section 206 (relating to penalties) of the International Emergency Economic Powers Act, section 16 (relating to offenses and punishment) of the Trading with the Enemy Act, any felony violation of section 15 of the

Food and Nutrition Act of 2008 (relating to supplemental nutrition assistance program benefits fraud) involving a quantity of benefits having a value of not less than five thousand dollars, any violation of section 543(a)(1) of the Housing Act of 1949 (relating to equity skimming), any felony violation of the Foreign Agents Registration Act of 1938, any felony violation of the Foreign Corrupt Practices Act, or section 92 of the Atomic Energy Act of 1954 (42 U.S.C. 2122) (relating to prohibitions governing atomic weapons), environmental crimes,[110] a felony violation of the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), the Ocean Dumping Act (33 U.S.C. 1401 et seq.), the Act to Prevent Pollution from Ships (33 U.S.C. 1901 et seq.), the Safe Drinking Water Act (42 U.S.C. 300f et seq.), or the Resources Conservation and Recovery Act (42 U.S.C. 6901 et seq.); or[111] any act or activity constituting an offence involving a Federal health care offense.[112]

Predicate offences also include any act or activity constituting an offence listed in section 1961 (1) of title 18 except an act which is indictable under subchapter II of chapter 53 of title 31;[113] and also any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848);[114]

[110] Bank Secrecy Act (Statute), s. 1956 (c) (7) (D)
[111] Bank Secrecy Act (Statute), s. 1956 (c)(7) (E)
[112] Bank Secrecy Act (Statute), s. 1956 (c)(7) (F)
[113] Bank Secrecy Act (Statute), s. 1956 (c)(7) (A)
[114] Bank Secrecy Act (Statute), s. 1956 (c)(7) (C)

2.2.3 UNITED KINGDOM

The UK Proceeds of Crime Act 2002 (as amended) applies the crime of money laundering to all predicate offences.[115]

2.3 PREDICATE OFFENCES FOR MONEY LAUNDERING (FOREIGN CRIMES)

The FATF has advised countries to extend predicate offences for money laundering to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically (double criminality test).

According to the FATF, countries could also provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically (single criminality test).[116]

This section compares the approaches in Nigeria with those of the United States and the United Kingdom.

2.3.1 NIGERIA

The Nigerian Money Laundering (Prevention and Prohibition) Act, 2022 remains silent with regards to the application of the above tests.

---

[115] Proceeds of Crime Act 2002 (as amended), s. 340 (2) (a), See also The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2013 Revised Version, Guidance for the UK financial sector Part I, Amended November 2013, Appendix II, Paragraph 1.

[116] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 3

The reason for such silence could be as a result of the fact that the **Nigerian Criminal Code Act 2004** applies the single criminality test to offences partially committed in Nigeria.[117]

It could therefore be inferred from the above facts that the same test may be applied to 'predicate offences for money laundering' occurring outside Nigeria.

2.3.2 UNITED STATES

The United States extends predicate offences for money laundering to conduct that would have constituted a predicate offence, had it occurred domestically (single criminality test).

This test is therefore limited to a list of predicate offences and the value of funds involved in a transaction. The predicate offences include:

i. the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act);[118]
ii. murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence (as defined in section 16);[119]
iii. fraud, or any scheme or attempt to defraud, by or against a foreign bank (as defined in paragraph 7 of section 1(b) of the International Banking Act of 1978));[120]

[117] Criminal Code Act 2004, s 12, See also F Nwadialo S.A.N, *The Criminal Procedure of the Southern States of Nigeria* (2nd Edition MIJ Professional Publishers Limited 1987) 14 – 15.
[118] Bank Secrecy Act (Statute), s. 1956 (c) (7) (B) (i)
[119] Bank Secrecy Act (Statute), s. 1956 (c) (7) (B) (ii)
[120] Bank Secrecy Act (Statute), s. 1956 (c) (7)(B) (iii)

iv. bribery of a public official, or the misappropriation, theft, or embezzlement of public funds by or for the benefit of a public official;[121]

v. smuggling or export control violations involving—

   a. an item controlled on the United States Munitions List established under section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

   b. an item controlled under regulations under the Export Administration Regulations (15 C.F.R. Parts 730–774);[122]

vi. an offence with respect to which the US would be obligated by a multilateral treaty, either to extradite the alleged offender or to submit the case for prosecution, if the offender were found within the territory of the United States; or[123]

vii. trafficking in persons, selling or buying of children, sexual exploitation of children, or transporting, recruiting or harbouring a person, including a child, for commercial sex acts.[124]

The value involved in a transaction or series of related transactions includes funds or monetary instruments of a value exceeding ten thousand dollars.[125]

2.3.3 UNITED KINGDOM

The United Kingdom applies both the single criminality test and the double criminality test to conducts occurring abroad. The single criminality test is limited to predicate

[121] Bank Secrecy Act (Statute), s. 1956 (c) (7) (B)(iv)
[122] Bank Secrecy Act (Statute), s. 1956 (c) (7) (B) (v)
[123] Bank Secrecy Act (Statute), s. 1956 (c) (7) (B) (vi)
[124] Bank Secrecy Act (Statute), s. 1956 (c)(7) (B) (vii)
[125] Bank Secrecy Act (Statute), s. 1956 (f)(2)

offences punishable for more than one year while the double criminality test is limited to predicate offences punishable for less than a year.[126]

2.4 PENALTIES

The FATF has advised countries to apply effective, proportionate and dissuasive criminal sanctions to natural persons convicted of money laundering.

The FATF has also advised countries to apply criminal liability and sanctions to legal persons and where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions should apply.[127]

This section compares the approaches in Nigeria with those of the United States and the United Kingdom.

2.4.1 NIGERIA

A person who commits the offence of money laundering is liable on conviction to imprisonment for a term of not less than four years but not more than fourteen years or a fine not less than five times the value of the proceeds of crime or both.[128]

A body corporate who commits the offence of money laundering is liable on conviction to a fine of not less than five times the value of the funds or the properties acquired as a

[126] Proceeds of Crime Act 2002, s. 340 (2) (b), See also Serious Organised Crime and Police Act 2005, s. 102 (1-7), The Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006, Article 2

[127] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 3

[128] Money Laundering (Prevention and Prohibition) Act, 2022, s. 18(3).

result of the offence committed.[129] Where the body corporate persists in the commission of the offence for which it was convicted in the first instance, the regulators may withdraw or revoke the certificate or license of the body corporate.[130]

2.4.2 UNITED STATES

A person who commits the offence of money laundering shall be sentenced to a fine of not more than five hundred thousand dollars or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.[131]

2.4.3 UNITED KINGDOM

A person who commits the offence of money laundering is liable on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both,[132] or on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.[133]

2.5 DISCUSSION

The previous section compared the approaches in Nigeria with those of the United States and the United Kingdom. This section will analyse issues that arose from the comparison to determine if there is need for reform.

[129] Money Laundering (Prevention and Prohibition) Act, 2022. s. 18(4).
[130] Money Laundering (Prevention and Prohibition) Act, 2022. s. 18(5).
[131] Bank Secrecy Act (Statute), s. 1956 (a) (1) (2) (3)
[132] Proceeds of Crime Act 2002, s. 334 (1) (a)
[133] Proceeds of Crime Act 2002, s. 334 (1) (b)

2.5.1 PREDICATE OFFENCES FOR MONEY LAUNDERING (FOREIGN CRIMES)

The Nigerian Criminal Code Act 2004 applies the single criminality test to foreign crimes partially committed in Nigeria.

The United States, on the other hand, applies the single criminality test to serious crimes that are committed outside the United States. This test is, therefore, limited to the value of funds involved in a transaction.

The United Kingdom applies the single criminality test to serious crimes that are committed outside the United Kingdom. This test is not limited to any value of funds as it is in the United States.

The Nigerian approach appears to be in line with Article 2 (2) of the Vienna Convention, which mandates countries to carry out their obligations in a manner consistent with the principles of sovereign equality and territorial integrity of countries and that of nonintervention in the domestic affairs of other countries.

The US and UK approaches appear to be inconsistent with these principles. They both establish their jurisdictions over offences committed abroad, provided that the offence is a serious offence.

This approach is also inconsistent with Article 2 (3) of the Vienna Convention, which mandates that countries should not exercise jurisdiction and performance of functions in the territory of another country that are exclusively reserved for the authorities of that other country by its domestic law.

In view of the above arguments, the Nigerian approach is a good approach.

The United States and United Kingdom are advised to adopt the Nigerian approach by applying the single criminality test to foreign crimes partially committed within their jurisdictions.

2.5.2 WHISTLEBLOWER POLICY

The Federal Executive Council had on the 21st day of December 2016 approved the Ministry of Finance' Whistleblowing Programme that may see individuals, who voluntarily volunteers credible information on stolen or concealed funds, smiling home with between 2.5 per cent and five per cent of the funds when recovered.

The programme was designed to encourage anyone with information about a violation, misconduct or improper activity that impacted negatively on Nigerians and government, to report such.[134]

The policy has been very successful in achieving its main objectives.

On the 8th day of April 2017, the Economic and Financial Crimes Commission (EFCC) recovered four hundred and forty-nine million, eight hundred and sixty thousand naira hidden in an abandoned shop in Lagos following a tip-off.[135]

On the 10th day of April, 2017, the EFCC again recovered five hundred and forty seven thousand, seven hundred and thirty euros and twenty one thousand and ninety pounds

[134] Adetayo, O., *'FG okays 5% of recovered loot for whistleblowers'*, (https://punchng.com 22 December 2016) Available at: http://punchng.com/fg-okays-5-recovered-loot-whistleblowers/ (accessed 6 June 2017).
[135] Akinkuotu, E., *'EFCC recovers N449m in abandoned Lagos shop'*, (https://punchng.com 8 April 2017) Available at: http://punchng.com/efcc-recovers-n449m-in-abandoned-lagos-shop/ (accessed 6 June 2017).

as well as five million six hundred forty-eight thousand five hundred naira from a Bureau de Change operator in Balogun Market, Lagos. The figure sums up to two hundred fifty million five hundred fifty-eight thousand six hundred seventy naira when converted to naira, according to the EFCC.[136]

On the 12th day of April, 2017, the EFCC raided a house in Ikoyi, Lagos recovering about forty three million dollars, twenty three million naira and twenty seven thousand pounds in cash. The operation followed a whistle-blower confidential alert received by the EFCC office in Lagos in the early hours of April, 11 2017.[137]

In total, the EFCC has recovered at least seventeen billion naira since the Federal Government introduced the whistle-blower policy on December 21, 2016.[138]

Despite the benefits associated with the policy, there have been concerns about the increase in the number of blackmailers in the country.[139]

Financial incentives have led to more approaches from opportunists and uninformed parties passing on speculative rumours or public information. The reputations of innocent parties have been unfairly damaged as a result.

For example, at about 8 am on Friday, May 26, 2017, men of the Nigeria Police Force from the Inspector General of Police Special Squad raided the official guest house of the

---

[136] The Punch, *'EFCC intercepts N250m cash haul at Balogun market'*, (https://punchng.com 10 April 2017) Available at: http://punchng.com/efcc-intercepts-n250m-cash-haul-at-balogun-market/ (accessed 4 June 2017).
[137] Akinkuotu, E., *'How EFCC recovered $43m, £27,000, N23m during house raid'*, (https://punchng.com 13 April 2017), Available at: http://punchng.com/efcc-recovers-43m-27000-n23m-during-house-raid/ (accessed 5 June 2017).
[138] Akinkuotu, E., *'EFCC recovers N17bn in four months'*, (https://punchng.com 23 April 2017) Available at: http://punchng.com/efcc-recovers-n17bn-in-four-months/ (accessed 6 June 2017).
[139] Okpare, O., *'Whistle-blowing: Blackmailers on the increase, says Uduaghan'*, (https://punchng.com 22 February 2017), Available at: http://punchng.com/whistle-blowing-blackmailers-increase-says-uduaghan/ (accessed 5 March 2017).

Deputy President of the Senate, Senator Ike Ekweremadu, located at No. 10 Ganges Street, Maitama, Abuja following a tip-off from a whistleblower. The raid was done without a search warrant. The police, however, stated at the end of the search that nothing incriminating was found.[140] Although the whistleblower was later arraigned before an Upper Area Court sitting at the Gudu District of Abuja on a one-count charge of criminal conspiracy and giving false information to mislead the police, contrary to **section 97(1) and 140 of the Penal Code Law**,[141] the search that was conducted on the premises of the Deputy President of the Senate, Senator Ike Ekweremadu without a warrant is unlawful and unconstitutional because the said act amounts to an infraction of the Constitutional right to privacy of Senator Ike Ekweremadu as provided by **Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).**[142]

Also, on the 16th of May, 2017, the Economic and Financial Crimes Commission arraigned two self-acclaimed whistleblowers, Buhari Fannami and Ba-Kura Abdullahi on two separate charges before Justice M. T Salihu of the Federal High Court Maiduguri, for allegedly giving false information to the agency.

The EFCC said in a statement by its spokesman, Mr. Wilson Uwujaren, that Fannamit had misled the commission with the information about illegally acquired monies

[140] UMORU, H. and KUMOLU, C., *'My house was raided by Police, nothing was found – Ekweremadu'*, (https://www.vanguardngr.com/ 27 May 2017) Available at: http://www.vanguardngr.com/2017/05/house-raided-police-nothing-found-ekweremadu/ (accessed 4 June 2017).
[141] Umoru, H. and Nnochiri, I., *'Ekweremadu: Police dock whistleblower over false information'*, (https://www.vanguardngr.com/ 31 May 2017) Available at: http://www.vanguardngr.com/2017/05/ekweremadu-police-dock-whistleblower-false-information/ (accessed 10 June 2017).
[142] Hassan v. E.F.C.C. (2014) I NWLR (Pt. 1389) 607 at 625

purportedly buried at the residence of one Ba'a Lawan but the information turned out to be false after the execution of a search warrant.[143]

The actions taken by the Police and the EFCC are bound to discourage opportunists from giving out false information to the relevant authorities.

The whistleblower policy is likely to be more effective when the **Public Interest Disclosure and Witness Protection Bill, 2017 becomes law**. The Bill expressly prohibits retaliation by employers against whistleblowers and provides them with a private cause of action in the event that they are discharged or discriminated against by their employers in violation of the Act.[144] The Bill also protects whistleblowers from any criminal or civil action.[145] The Bill makes it unlawful for employers to retaliate against any employee who makes or intends to make a public interest disclosure on fraud, corruption and theft in relation to public funds or any Government property whatsoever.[146] Criminal penalties apply, with fines up to five hundred thousand naira or imprisonment for a term of not less than two years or to both.[147] This measure is in line with the **Hawaii Whistleblowers Protection Act.**

[143] The Daily Times, *'EFCC arraigns 2 whistleblowers over false information'*, (https://dailytimesng.com 17 May 2017) Available at: https://dailytimes.ng/news/efcc-arraigns-2-whistleblowers-false-information/ (accessed 10 June 2017).
[144] Public Interest Disclosure and Witness Protection Bill, 2017, s. 44, s. 45
[145] Public Interest Disclosure and Witness Protection Bill, 2017, s. 42
[146] Public Interest Disclosure and Witness Protection Bill, 2017, s. 43 s. 52 (1)
[147] Public Interest Disclosure and Witness Protection Bill, 2017, s. 43

2.5.3 DEPLOYMENT OF THE LIE DETECTOR TECHNOLOGY (POLYGRAPH) FOR CRIMINAL INVESTIGATIONS AND CORROBORATION OF EVIDENCES IN COURT.

The lie detector technology (polygraph) has been deployed by the Economic and Financial Crimes Commission for criminal investigations and corroboration of evidences in court. This was accomplished with the establishment of a Polygraph Unit in the Economic and Financial Crimes Commission. The Economic and Financial Crimes Commission's Polygraph Unit was the first in Nigeria and the Economic and Financial Crimes Commission, the first organisation in Africa to get a conviction using the polygraph technology.[148]

The lie detector technology (polygraph) has also been deployed by the Economic and Financial Crimes Commission in the prosecution of cases involving financial crimes by calling a prosecution witness living in another jurisdiction via Skype. This method was adopted by the Economic and Financial Crimes Commission in a case of Conspiracy, Obtaining Under False Pretences and Impersonation to the tune of N12,800,200 (Twelve Million, Eight Hundred Thousand Two Hundred Naira) against Amobi Alukwu and his wife, Helen Alukwu which was brought before Justice N.I. Buba of the Federal High Court Enugu. In that case, the EFCC deployed technology in the prosecution of its case

[148] Economic and Financial Crimes Commission, *'A Gender-based Foundation Seeks EFCC's Technology Assistance in Prosecution of Sex Offenders',* (Available at: https://www.efccnigeria.org/ 2020) Available at: https://www.efccnigeria.org/efcc/news/6308-a-gender-based-foundation-seeks-efcc-s-technology-assistance-in-prosecution-of-sex-offenders (accessed 12 November 2021).

by calling a prosecution witness living in the United States of America, Obu Nnamdi Patrick via Skype.[149]

2.6 CONCLUSION

This chapter compared the approaches in Nigeria with those of the United States and United Kingdom on the basis of the 'criminalization of money laundering' and other related subtopics. It has also analysed issues that arose from the comparison to determine if there is need for reform. This section focuses on those areas that need reform.

Based on the arguments canvassed in Section 2.5, the following reforms are recommended:

I. The Nigerian Money Laundering (Prevention and Prohibition) Act, 2022 should be amended to include the single criminality test, even if it is already included in the Nigerian Criminal Code Act.

II. A Police Officer who receives information from a whistleblower about money hidden in an apartment should apply to a Court or Justice of the Peace within the local limits of whose jurisdiction he is for the issue of a search warrant before conducting a search on the said premises. This procedure is in line with **Section 143 of the Administration of Criminal Justice Act 2015 and the Court of Appeal decision in Hassan v. E.F.C.C. (2014) I NWLR (Pt. 1389) 607 at 625.**

III. The **Public Interest Disclosure and Witness Protection Bill, 2017** should be given accelerated consideration in the House of Representatives based on its

[149] Economic and Financial Crimes Commission, *'N12.8 Million Fraud: EFCC Deploys Technology In Court'*, (https://www.efccnigeria.org 2019), Available at: https://www.efccnigeria.org/efcc/news/3981-n12-8-million-fraud-efcc-deploys-technology-in-court (accessed 12 November 2021).

urgency and significance for the Federal Executive Council's whistleblowers Policy.

CHAPTER 3

CUSTOMER DUE DILIGENCE

'Customer due diligence/know your customer' is intended to enable a financial institution to form a reasonable belief that it knows the true identity of each of its customers and, with an appropriate degree of confidence, knows the types of business and transactions the customer is likely to undertake.

The financial institution should have procedures in place to: (i) identify and verify the identity of each customer on a timely basis, (ii) take reasonable risk-based measures to identify and verify the identity of any beneficial owner and (iii) obtain appropriate additional information to understand the customer's circumstances and business, including the expected nature and level of transactions.[150]

Financial institutions are required to undertake customer due-diligence (CDD) measures when: (i) establishing business relations, (ii) carrying out occasional transactions above the applicable designated threshold (fifteen thousand US dollars or Euros) or that are wire transfers, (iii) there is a suspicion of money laundering or terrorist financing or (iv) the financial institution has doubts about the veracity of adequacy of previously obtained customer identification data.

[150] FATF Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing, (High Level Principles and Procedures) (2007), paragraph 3.10.

The principle that financial institutions should conduct CDD should be set out in law. Each country may determine how it imposes specific CDD obligations, either through law or enforceable means.[151]

This chapter compares the approaches adopted in Nigeria, the United Kingdom and the United States as they relate to the application of CDD measures to determine what the best approach is.

The comparison falls under the following subheadings: 'Customer Information Required', 'Verification through Documents' and 'Verification through Nondocumentary Methods'.

3.1 CUSTOMER INFORMATION REQUIRED

3.1.1 NIGERIA

Financial institutions are required to obtain the following information in relation to natural persons:

i. Legal name and any other names used (such as maiden name);
ii. Permanent address (full address shall be obtained and the use of a post office box number only, is not sufficient);
iii. Telephone number, fax number and email address;
iv. Date and place of birth;
v. Nationality;
vi. Occupation, public position held and name of employer;

[151] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 10

vii. An official personal identification number or other unique identifier contained in an unexpired official document such as passport, identification card, residence permit, social security records or drivers' licence that bears a photograph of the customer;

viii. Type of account and nature of the banking relationship; and

ix. Signature.[152]

A financial institution shall make an initial assessment of a customer's risk profile from the information provided and particular attention shall be focused on those customers identified as having a higher risk profile and any additional inquiries made or information obtained in respect of those customers shall include:

i. Evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits;

ii. Personal reference by an existing customer of the same institution;

iii. Prior bank reference and contact with the bank regarding the customer;

iv. Source of wealth; and

v. Verification of employment and public position held where appropriate.[153]

3.1.2 UNITED STATES

Financial institutions are required to obtain the following information in relation to natural persons:

i. Name;

[152] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Schedule II Paragraph 1 (1).

[153] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Schedule II Paragraph 1 (5).

ii. Date of birth;

iii. Address;

iv. Identification number.[154]

Customers that pose higher money laundering or terrorist financing risks present increased exposure to banks; due diligence policies, procedures, and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious activity monitoring system that reduces the bank's reputation, compliance, and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank.

The bank may determine that a customer poses a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of[155] transactions, including those transactions involving higher-risk jurisdictions. If so, the bank should consider obtaining, both at account opening and throughout the relationship, the following information on the customer:

i. Purpose of the account;

ii. Source of funds and wealth;

iii. Individuals with ownership or control over the account, such as beneficial owners, signatories or guarantors;

[154] Federal Financial Institutions Examination Council: Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010, 54.

[155] Federal Financial Institutions Examination Council: Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010, 64.

iv. Occupation or type of business (of customer or other individuals with ownership or control over the account);

v. Financial statements;

vi. Banking references;

vii. Domicile (where the business is organized);

viii. Proximity of the customer's residence, place of employment, or place of business to the bank;

ix. Description of the customer's primary trade area and whether international transactions are expected to be routine;

x. Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers;

xi. Explanations for changes in account activity.[156]

3.1.3 UNITED KINGDOM

Firms are required to obtain the following information in relation to natural persons:

i. Full name;

ii. Residential address;

iii. Date of birth.[157]

When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship

[156] Federal Financial Institutions Examination Council: Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010, 65.

[157] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing 2020* Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.71.

might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to:

i. The customers residential status;
ii. Employment and salary details;
iii. Other sources of income or wealth (e.g., inheritance, divorce settlement, property sale).[158]

3.2 VERIFICATION THROUGH DOCUMENTS

3.2.1 NIGERIA

Financial institutions shall verify the information referred to in subsection 3.1.1 by at least one of the following methods:

i. Confirming the date of birth from an official document (such as birth certificate, passport, identity card, social security records);
ii. Confirming the permanent address (such as utility bill, tax assessment, bank statement, a letter from a public authority).[159]

3.2.2 UNITED STATES

A bank using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation.

[158] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing 2020* Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.5.6
[159] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Schedule II Paragraph 1 (2) (a) (b)

Banks shall verify the information referred to in subsection 3.1.2 by at least one of the following methods:

i. A Driver's licence;

ii. Passport.[160]

3.2.3 UNITED KINGDOM

If identity is to be verified from documents, this should be based on: Either a government-issued document which incorporates:

i. The customer's full name and photograph, and;

ii. Either his residential address;

iii. Or his date of birth

or a government, court or local authority-issued document (without a photograph) which incorporates the customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the UK financial services sector, which incorporates: The customer's full name and;

i. Either his residential address;

ii. Or his date of birth.

Government-issued documents with a photograph include:

i. Valid passport;

[160] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 55.

ii. Valid photo card driving licence (full or provisional);

iii. National identity card;

iv. Firearms certificate or shotgun licence;

v. Identity card issued by the Electoral Office for Northern Ireland.

Government-issued documents without a photograph include:

i. Valid (old style) full UK driving licence;

ii. Recent evidence of entitlement to a state or local authority-funded benefit (including housing benefit and council tax benefit), tax credit, pension, educational or other grants.

iii. Instrument of a Court appointment (such as liquidator, or grant of probate);

iv. Current council tax demand letter, or statement.[161]

Examples of other documents to support a customer's identity include current bank statements, or credit/debit card statements, issued by a regulated financial sector firm in the UK or EU, or utility bills. If the document is from the internet, a pdf version may be more reliable.[162]

[161] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.75.

[162] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.76.

3.3 VERIFICATION THROUGH NON-DOCUMENTARY METHODS

3.3.1 NIGERIA

Financial institutions may verify the information referred to in subsection 3.1.1 by at least one of the following methods:

i. Contacting the customer by telephone, by letter or by email to confirm the information supplied after an account has been opened (such as a disconnected phone, returned mail, or incorrect e-mail address shall warrant further investigation);

ii. Confirming the validity of the official documentation provided through certification by an authorized person such as embassy official, notary public.[163]

3.3.2 UNITED STATES

Banks are not required to use non-documentary methods to verify a customer's identity. However, a bank using non-documentary methods to verify a customer's identity must have procedures that set forth the methods the bank will use.

Non-documentary methods may include:

i. Contacting a customer;

[163] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Schedule II Paragraph 1 (2) (c) (d)

ii. Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a customer reporting agency, public data base, or other source;

iii. Checking references with other financial institutions; and

iv. Obtaining a financial statement.[164]

3.3.3 UNITED KINGDOM

If identity is verified electronically, this should be by the firm, using as its basis the customer's full name, address and date of birth, carrying out electronic checks either direct, or through a supplier.[165]

A number of commercial agencies which access many data sources are accessible online by firms, and may provide firms with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list. Some of these sources are, however, only available to closed user groups.[166]

Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources - where an individual has to

[164] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 2010, 55.

[165] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.80.

[166] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended November 2013, Paragraph 5.3.46.

prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.[167]

Negative information includes lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information may be necessary to mitigate against impersonation fraud.[168]

For an electronic check to provide satisfactory evidence of identity on its own, it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (e.g., a single check against the Electoral Roll) is not normally enough on its own to verify identity.[169]

Before using a commercial agency for electronic verification, firms should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

i. it is recognised, through registration with the Information Commissioner's Office, to store personal data;
ii. it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;

[167] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.47.
[168] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.49.
[169] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.50.

iii. it accesses negative information sources, such as databases relating to identity fraud and deceased persons;

iv. it accesses a wide range of alert data sources; and

v. it has transparent processes that enable the firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.[170]

In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify an identity.[171]

3.4 DISCUSSION

The previous sections compared the approaches adopted in Nigeria, the United Kingdom and the United States as they relate to the application of CDD measures.

This section will determine issues that arise from such a comparison.

3.4.1 MEANING OF 'CUSTOMER'

As stated above, financial institutions are required to apply the necessary CDD measures to their customers.

The term 'customer' is not expressly defined in the Nigerian or UK Money Laundering Regulations as it is defined in the US Bank Secrecy Act/Anti–Money Laundering Examination Manual 2010. Its meaning must be inferred from the definitions of 'business

[170] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.52.

[171] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.53.

relationship' and 'occasional transaction', the context in which it is used in the United Kingdom and Nigerian Money Laundering Regulations and its everyday dictionary meaning.[172]

In general, the customer is the party, or parties, with whom the business relationship is established, or for whom the transaction is carried out. Where, however, there are several parties to a transaction, not all will necessarily be customers.[173]

A 'business relationship' is defined as a business, professional or commercial relationship between a firm and a customer that, when contact is established, the firm expects to have an element of duration. A relationship need not involve the firm in an actual transaction; giving advice may often constitute establishing a business relationship.[174]

An 'occasional transaction' means a transaction carried out other than in the course of a business relationship (e.g., a single foreign-currency transaction or an isolated instruction to purchase shares), amounting to fifteen thousand Euros or more, whether

[172] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.3.

[173] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.4

[174] For United Kingdom laws, see the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 4. See also the Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.5. For Nigerian laws, see Money Laundering (Prevention and Prohibition) Act, 2022, s. 30. See also CBN (Anti–Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 132.

the transaction is carried out in a single operation or in several operations that appear to be linked.[175]

The United States, on the other hand, defines a customer as a person (an individual, a corporation, partnership, a trust, an estate or any other entity recognized as a legal person) who opens a new account; an individual who opens a new account for another individual who lacks legal capacity; or an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied. The definition of customer also does not include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity. Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities and publicly traded companies (as described in 31 CFR 103.22 (d) (2) (ii) through (iv).[176]

In view of the above facts, the US approach is far better than the United Kingdom and the Nigerian approach, because it leaves no room for ambiguity.

[175] For United Kingdom laws, see the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 3(1), 27(1), (2); See also the Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.3.6. For Nigerian laws, see Money Laundering (Prevention and Prohibition) Act, 2022, s. 30.
[176] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti–Money Laundering Examination Manual* (2010), 53.

3.4.2 THE THREE-TIERED KYC REGIME

The three-tiered KYC requirements was introduced by the Central Bank of Nigeria for compliance by banks and other financial institutions under its regulatory purview.[177]

The three-tiered KYC regime seeks to implement flexible account opening requirements for low-value and medium-value account holders subject to caps and transaction restrictions as the amount on the transactions increase. This means that account opening requirements will increase progressively with less restrictions on operations. However, the main objective of the approach is to promote and deepen financial inclusion.[178]

The structure ensures that the accounts remain attractive to customers of different socio-economic levels while close watch is kept on the risk involved.[179]

Low-value accounts, for example, are limited to a maximum single deposit of fifty thousand naira and maximum cumulative balance of three hundred thousand naira at any point in time.[180] Basic customer information required to be provided are:

---

[177] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 45 (1); Central Bank of Nigeria, '*Circular to all Banks and other Financial Institutions: Introduction of Three-Tiered Know Your Customer (KYC) Requirements'*, (https://www.cbn.gov.ng 18 January 2013) Available at: https://www.cbn.gov.ng/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf (accessed 10 April 2018).

[178] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 45 (1); Central Bank of Nigeria, *'Circular to all Banks and other Financial Institutions: Introduction of Three-Tiered Know Your Customer (KYC) Requirements'*, (https://www.cbn.gov.ng 18 January 2013) Available at: https://www.cbn.gov.ng/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf (accessed 10 April 2018).

[179] Central Bank of Nigeria, *'Circular to all Banks and other Financial Institutions: Introduction of Three-Tiered Know Your Customer (KYC) Requirements'*, (https://www.cbn.gov.ng 18 January 2013) Available at: https://www.cbn.gov.ng/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf (accessed 10 April 2018).

a. Passport photograph;

b. Name, place and date of birth;

c. Gender, address, telephone number, e.t.c.[181]

The information may be sent electronically or submitted onsite in the institution's branches or agent's office.[182]

Evidence of information provided by a customer or verification of same is not required.[183]

Though Nigeria has a Centralized Biometric Identification system which requires every customer to undertake biometric capturing and generate a Bank Verification Number which they must provide to any Bank they intend to also bank with, Mobile Money wallet holders on Tiered KYC Level 1 are not required to provide Bank Verification Number as part of the KYC documentation.[184] This is very different from the United Kingdom's approach which makes it mandatory for a bank to verify the identity and address of an applicant even when it is a low risk account or a basic bank account.[185]

Non-verification of customer information at the account opening stage may negatively impact on information sharing mechanisms. For example, a customer who successfully

---

[180] Central Bank of Nigeria, *'Circular to Banks and Other Financial Institutions: Review of Restrictions and Limits on Levels I and II of the Tiered KYC Accounts'*, (https://www.cbn.gov.ng 1st July, 2016) Available at: https://www.cbn.gov.ng/out/2016/fprd/july%202016%20circular%20tkyc%20review.pdf (accessed 6 May 2019).

[181] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 45 (2).

[182] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 45 (2).

[183] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 45 (2).

[184] Central Bank of Nigeria, *'Review of Daily Mobile Money Wallet Transaction and Balance Limit and Bank Verification Numbers (BVN) Requirement for Mobile Money Wallet Holders'*, (https://www.cbn.gov.ng 7 September 2017) Available at: https://www.cbn.gov.ng/out/2017/bpsd/review%20of%20daily%20mm%20wallet%20transaction%20&%20bvn%20requirement%20for%20mobile%20money%20wallet%20holders.pdf (accessed 6 May 2019).

[185] United Kingdom Payment Accounts Regulations 2015, Regulation 23 (3).

opened a low value account at Bank A may decide to open another low value account at Bank B, Bank C, Bank D and Bank E for the purpose of circumventing the threshold mechanism. The customer could use different names and different addresses to open these new accounts. Since his information at Bank A was not verified the customer can afford to open different accounts with different names in different Banks without being detected. With an account opened at 5 different Banks, the customer would have attained a cumulative balance of one million five hundred thousand naira.

It is worth noting that the Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013 did not make it mandatory for a bank to verify whether a customer already holds an account with another bank before opening a low value account. This is different from the United Kingdom's approach where the United Kingdom's Payment Accounts Regulations 2015 mandates designated credit institutions to verify whether a consumer does not hold a payment account with any United Kingdom credit institution, and in a situation where the bank determines that a customer does hold a payment account with another credit institution, the bank must not open a basic account for that customer.[186] This is not the case for Nigeria.

[186] United Kingdom Payment Accounts Regulations 2015, Regulation 23 (3). See also Santander, *'Customer identification requirements for UK residents'* (https://www.santander.co.uk/ 2018) Available at https://www.santander.co.uk/csdlvlr/BlobServer?blobtable=MungoBlobs&blobkey=id&blobcol=urldata&blobheader=application%2Fpdf&blobheadervalue1=inline%3Bfilename%3DCustomer+Identification+Requirements+do-ec-368.pdf&blobwhere=1314024309911&blobheadername1=Content-Disposition (accessed 3 April 2018); Barclays, *'Identification for bank accounts: What ID do I need to open a bank account?'* (https://www.barclays.co.uk 2018), Available at: https://www.barclays.co.uk/current-accounts/what-do-i-need-to-open-a-bank-account/ (accessed 2 April 2018).

3.4.3 TRANSPARENCY AND BENEFICIAL OWNERSHIP

Although inadequate, most financial institutions in Nigeria depend on the Corporate Affairs Commission (CAC) to confirm the identity of the beneficial owners (BOs) of their customers. Large banks, capital markets operators (CMOs), insurance brokers usually identify the BO using the shareholding structure as stated in the company registration documents. However, company registration documents kept by the CAC are not dependable and current. Contrary to the requirements of the Companies and Allied Matters Act (CAMA), entities that failed to file yearly returns for as long as thirteen years are still on the register with no sanctions applied.

The United Kingdom's situation is no different here. Media reports suggest that the UK's Companies House is a mere repository of information, with no statutory powers to verify information provided to it. It lacks the resources to police even the minimal laws that do exist.[187]

3.5 CONCLUSION

In view of the arguments in the previous section, the following are recommended:

I. Nigeria and the United Kingdom should amend their money laundering laws by defining who a customer is.

II. The Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013 should be amended to prohibit financial institutions from opening more than one low value account for Mobile Money wallet holders. In

[187] Financial Times, *'Overhaul of Companies House is long overdue'*, (https://www.ft.com 2021) Available at: https://www.ft.com/content/6fd92a72-e457-4d32-a5a5-c44ec2b76e20 (accessed 8 December 2021).

other words, financial institutions should be mandated to verify whether a customer already holds an account with another bank before opening a low value account, and in a situation where the bank determines that a customer does hold a payment account with another credit institution, the bank should not open a basic account for that customer. Verification can be done by mandating all bank customers to provide their Bank Verification Number before an account can be opened. This is the approach being adopted by the United Kingdom's Payment Accounts Regulations 2015. This approach will positively impact on account monitoring procedures; customer identification and verification will reduce the risk of impersonation fraud and identity theft while still promoting financial inclusion.

III. The Corporate Affairs Commission should maintain timely, adequate, accurate and up-to-date BO information. The Corporate Affairs Commission should have a policy of inquiring/prohibiting or otherwise becoming aware of foreign companies that are shareholders in local companies and that have issued bearer shares. This policy is particularly relevant for identifying the ultimate beneficial ownership of local companies which can impede effective law enforcement investigations involving foreign companies.

IV. The Corporate Affairs Commission should have a strong monitoring and sanctioning regime. According to GIABA's Second Mutual Evaluation Report on Nigeria, Existing monetary sanctions are not dissuasive enough to guarantee compliance to make disclosures, including the beneficial ownership of foreign partners and shareholders.

CHAPTER 4

POLITICALLY EXPOSED PERSONS

Individuals who have, or have had, a high political profile and those who hold, or have held, public office can pose a higher money laundering risk, as their positions may make them vulnerable to corruption. These people are collectively known as politically exposed persons (PEPs).[188]

The risk associated with such individuals extends to members of their immediate families and to other known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher-risk category[189] that requires financial institutions to apply additional measures in order to reduce the risk.[190]

A PEP is defined as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.[191]

The Financial Action Task Force (FATF) requires that countries apply the PEP definition to only those holding such a position *outside* their jurisdictions.[192]

---

[188] The Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing* June 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 5.5.13.

[189] Ibid.

[190] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12

[191] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(12)(a). See the Joint Money Laundering Steering Group (JMLSG), *Prevention of Money Laundering*, Guidance for the United Kingdom Financial Sector Part I, Amended July 2020, Paragraph 5.5.15. See also Money Laundering (Prevention and Prohibition) Act, 2022, s. 30 and the U.S. Patriot Act Final Regulation and Notice of Proposed Rule Making 2005, s. 312.

The United Nations Office on Drugs and Crime (UNODC), on the other hand, requires that countries apply the PEP definition to those holding such positions both inside and outside their jurisdictions.[193]

While some countries have adopted the approach of the FATF, others have adopted that of UNODC. For example, Nigeria and the United Kingdom apply the PEP definition to those holding such positions both inside and outside the country,[194] while the United States applies the PEP definition to those holding such positions outside their respective countries.[195]

The best approach is one that protects the financial system against corrupt PEPs and reduces the money laundering and terrorist financing risks to the barest minimum.

4.1 APPLICATION OF THE PEPs DEFINITION

A PEP is defined as 'an **individual who is or has, at any time in the preceding year, been entrusted with prominent public functions** and **an immediate family member**, or a **known close associate**, of such a person'.[196]

Individuals who are or have been entrusted with prominent public functions include: heads of state, heads of government, ministers and deputy, or assistant ministers, members of the Supreme Court, members of Courts of auditors or of the boards of

[192] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12
[193] United Nations Convention against Corruption (2004), Article 52 (1)
[194] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(12)(a). See the Joint Money Laundering Steering Group (JMLSG), *Prevention of Money Laundering*, Guidance for the United Kingdom Financial Sector Part I, Amended July 2020, Paragraph 5.5.15. See also Money Laundering (Prevention and Prohibition) Act, 2022, s. 30.
[195] USA Patriot Act of 2001: Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism, s. 312 (a) (3) (B).
[196] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 12.

central banks, ambassadors, charges d affairs and high-ranking officers in the armed forces, and members of the administrative, management or supervisory bodies of state owned enterprises. The categories above do not include middle-ranking or more junior officials.[197]

Immediate family members include: a spouse, a partner, children and their spouses or partners and parents.[198]

Persons known to be close associates include: any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations with a person referred to as a PEP or any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person referred to as a PEP.[199]

Financial institutions are required to verify the identity of customers, to take reasonable steps to determine the identity of beneficial owners of funds deposited into high –value accounts and to conduct enhanced scrutiny of accounts sought or maintained by or on behalf of individuals who are, or have been, entrusted with prominent public functions and their family members and close associates. Such enhanced scrutiny shall be reasonably designed to detect suspicious transactions for the purpose of reporting to competent authorities and should not be so construed as to discourage or prohibit financial institutions from doing business with any legitimate customer.[200]

---

[197] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(14).

[198] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(12)(b).

[199] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(12)(c).

[200] United Nations Convention Against Corruption 2004, Article 52 (1)

This section will determine the approach that is being adopted by Nigeria, the United States and the United Kingdom with regards to the application of the definition of PEPs.

4.1.1 NIGERIA

Nigeria applies the PEP definition to those holding such a position inside and outside the country.[201]

4.1.2 UNITED STATES

The United States apply the PEP definition to those holding such positions outside the country.[202] The United States refers to PEPs as Senior Foreign Political Figures and limits the application of the definition to Senior Foreign Political Figures who maintain a private banking account with a U.S. financial institution.[203]

4.1.3 UNITED KINGDOM

The United Kingdom applies the PEP definition to those holding such a position inside and outside the country.[204]

4.2 DISCUSSION

The previous section compared the approaches adopted in Nigeria, the United States and the United Kingdom with regard to the application of the PEP definition. The best

[201] Money Laundering (Prevention and Prohibition) Act, 2022, s. 30.
[202] Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT ACT) ACT of 2001, s. 312 (a) (3) (B)
[203] Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT ACT) ACT of 2001, s. 312 (a) (3) (B), See also Section 312 of the US Patriot Act Final Regulation and Notice of Proposed Rule Making 2005
[204] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 35(12)(a).

approach is one that protects the financial system against corrupt PEPs and reduces the risks of money laundering and terrorist financing to the barest minimum.[205]

4.2.1 PROTECTING THE FINANCIAL SYSTEM AGAINST CORRUPT PEPS

As stated earlier, Nigeria and the United Kingdom apply the PEP definition to those holding such positions inside and outside the country, while the United States applies the definition only to those holding such positions outside the country. This section will determine which of the above approaches is more likely to protect the financial system against corrupt PEPs.

The Nigerian and the United Kingdom approaches protect the financial system against individuals who are, or have been, entrusted with prominent public functions both inside and outside the country.

The US approach, on the other hand, protects the financial system against individuals who are or have been entrusted with prominent public functions outside their respective countries.

There appears to be no protection against individuals who are, or who have been, entrusted with prominent public functions within the United States. However, such

[205] Transparency International, *'The Global Coalition against Corruption'* (http://www.transparency.org/cpi2013) http://www.transparency.org/cpi2013/results Accessed 26th June 2014.

protection may not be needed since cases of corruption have been rare in these countries.[206]

4.2.2 ENHANCED DUE DILIGENCE FOR POLITICALLY EXPOSED PERSONS

Financial institutions are required by law to take adequate meaningful measures to establish the source of funds and source of wealth for high-risk customers like politically exposed persons. Financial institutions may wish to refer to information sources such as asset and income declarations, which some jurisdictions expect certain senior public officials to file and which often include information about an official's source of wealth and current business interests.[207] Financial institutions in the United Kingdom normally do not encounter any difficulties in gaining access to the asset details of officers holding public office in the United Kingdom.

Financial institutions in Nigeria may encounter challenges gaining access to the asset details of public officers. In January 3, 2020, the freedom of information (FoI) request, Socio-Economic Rights and Accountability Project (SERAP) urged President Muhammadu Buhari, Vice-President Yemi Osinbajo (SAN), the 36 state governors, and deputy governors to "make public details of their assets, specific properties, and incomes, contained in their asset declaration forms submitted to the Code of Conduct Bureau (CCB) since assuming office." But Buhari, Osinbajo, the 36 state governors, and their deputies rebuffed the request. Niger and Lagos states, which acknowledged the receipt of SERAP's FoI request, declined to release the requested information but

[206] Transparency International, *'Corruption Perceptions Index'* (https://www.transparency.org 2021) https://www.transparency.org/en/cpi/2021 Accessed 6 July 2022.
[207] See the Joint Money Laundering Steering Group (JMLSG), *Prevention of Money Laundering, Guidance for the United Kingdom Financial Sector* Part I, Amended July 2020, Paragraph 5.5.30.

contended that "the FoI Act is inapplicable to state governments, their agencies, and officials." Then the struggle shifted to the Federal High Court in Lagos where SERAP filed a lawsuit marked FHC/ABJ/CS/65/2020, seeking "an order for leave to apply for judicial review and an order of mandamus to direct and/or compel President Buhari, Vice President Osinbajo, 36 state governors and their deputies to make public their summary of assets." SERAP went further to seek a mandamus order to compel the CCB "to make available to the public, specific details of asset declarations submitted to it by successive Presidents, Vice-Presidents, Senate Presidents, Speakers of House of Representatives, state governors and their deputies since 1999." SERAP argued that asset declaration forms submitted to the CCB by public officers were public documents and public officers could not hide under the fundamental right to privacy to keep their assets secret, having been entrusted with the duty of managing public funds. The CCB, which contended that no law empowered it to release to the public the assets declaration forms submitted by public officers, vehemently opposed the suit. The CCB said it needed clear legislation by the National Assembly to release to the public details of declared assets by public officers. The court, in a May 11, 2020 judgment by Justice Muslim Hassan, agreed with the CCB and dismissed SERAP's suit. "I agree with the CCB that the duty to make the asset declaration form of public officers available depends on the terms and conditions to be prescribed by the National Assembly.[208]

[208] The Guardian, *'Transparency in asset declaration regime still a long way ahead'*, (https://guardian.ng/ 15 September 2020), Available at: https://guardian.ng/features/transparency-in-asset-declaration-regime-still-a-long-way-ahead/ (accessed 8 December 2021).

4.3 CONCLUSION

This chapter compared the approaches in Nigeria, the United States and United Kingdom with regard to the application of the PEP definition. It has analysed issues that arose from the comparison to determine if there is a need for reform.

Based on the outlined arguments, the following reforms are recommended:

I. The United States is recommended to extend the application of the PEP definition to individuals who hold prominent public functions within the country.
II. The Nigerian National Assembly should enact a law empowering the CCB to release to the public details of declared assets by public officers.

These recommended approaches will strengthen the anti-money laundering measures of United States and Nigeria.

CHAPTER 5

CASH COURIERS

The Financial Action Task Force (FATF)—an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and financing the proliferation of weapons of mass destruction—has advised countries to enact laws that require all persons who physically transport currency or bearer negotiable instruments (BNIs) in excess of fifteen thousand US dollars or Euros to submit a truthful declaration to the designated competent authorities.

Countries may opt from among the following three types of declaration systems: (i) a written declaration system for all travellers, (ii) a written declaration system for those travellers carrying an amount of currency or BNIs above the threshold and (iii) an oral declaration system. These systems are described below in their pure forms. However, it is not uncommon for countries to opt for a mixed system.[209]

(a) Written declaration system for all travellers: In this system, all travellers are required to complete a written declaration before entering the country. This would include questions on a common or customs declaration form. In practice, travellers must declare whether or not they are carrying currency or BNIs (e.g., by ticking a yes or no box).[210]

(b) Written declaration system for travellers carrying amounts above a threshold: In this system, all travellers carrying an amount of currency or BNIs above a preset designated

[209] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 32
[210] Ibid.

threshold are required to complete a written declaration form. In practice, travellers who are not carrying currency or BNIs over the designated threshold are not required to fill out any forms.[211]

(c) Oral declaration system for all travellers: In this system, all travellers are required to orally declare if they carry an amount of currency or BNIs above a prescribed threshold. This is usually done at customs entry points where travellers are required to choose between the 'red channel' (goods to declare) and the 'green channel' (nothing to declare). The traveller's choice of channel is considered the oral declaration. In practice, travellers do not declare in writing but are required to actively report to a customs official.[212]

While countries have followed the advice of the FATF, the laws in these countries are not identical. For example, Nigeria and the United Kingdom require all travellers to orally declare if they carry an amount of currency above the prescribed threshold, while the United States requires travellers who carry an amount of currency above a preset designated threshold to complete a written declaration form.

This chapter compares the approach adopted by Nigeria and United Kingdom with that of the United States to determine the best approach. This is likely the one that protects the integrity of the financial system against and terrorist financiers and reduces the risk of money laundering and terrorist financing to the barest minimum.

[211] Ibid.
[212] Ibid.

5.1 DECLARATION SYSTEM

5.1.1 NIGERIA

The dual channel system of passenger clearance is operated at Lagos/Abuja International Airports. By choosing a specifically designated exit, the traveller declares either that he is carrying with him an amount less than ten thousand dollars or an amount equivalent to ten thousand dollars or more than ten thousand dollars.

There are two designated exits and a passenger goes through one of the exits with all his baggage loaded on a trolley:

5.1.1.1 GREEN EXIT

A passenger who is satisfied that he does not have ten thousand dollars or more is to pass through the green exit indicated by a green regular octagon with the words “NOTHING TO DECLARE” in English or “RIEN A DECLARER” in French.

5.1.1.2 RED EXIT

A passenger who has ten thousand dollars or more is to pass through the Red channel indicated by a read square with the words “GOODS TO DECLARE” in English or “MERCHANDISES A DECLARER” IN French and to declare such goods to the Customs officer by the Examination bench.

By choosing a channel, a passenger is, by implication, declaring the contents of his baggage.[213]

Any person who falsely declares or fails to make a declaration to the Nigerian Custom Service is guilty of an offence and shall be liable on conviction to forfeit the undeclared funds or negotiable instrument or to imprisonment for a term of at least two years or both.[214]

5.1.2 UNITED STATES

When entering the United States in-transit to a foreign destination, you will be required to clear U.S. Customs Border Protection (CBP) and Immigration and Customs Enforcement. If you have "negotiable monetary instruments" (i.e. currency, personal checks (endorsed), travellers checks, gold coins, securities or stocks in bearer form) valued at ten thousand dollars or more in your possession a "Report of International Transportation of Currency or Monetary Instruments" form FinCEN 105 must be submitted to a CBP Officer upon your entry into the United States.

Monetary instruments that are made payable to a named person but are not endorsed or which bear restrictive endorsements are not subject to reporting requirements, nor are credit cards with credit lines of over ten thousand dollars. Gold bullion is not a monetary instrument for purposes of this requirement. The requirement to report monetary instruments on a FinCEN 105 does not apply to imports of gold bullion.

[213] Nigeria Customs Service, *'Passenger's Concessions'* (https://www.customs.gov.ng) https://www.customs.gov.ng/Stakeholders/passengers_concessions.php Accessed 7th September 2014.
[214] Money Laundering (Prevention and Prohibition) Act, 2022, s. 3 (5).

Failure to declare monetary instruments in amounts of or over ten thousand dollars can result in its seizure.[215]

5.1.3 UNITED KINGDOM

When you arrive in the United Kingdom, you'll have to go through customs. Most UK ports and airports have three customs exits or 'channels', while some have only one exit, with a red-point phone for declaring goods.

5.1.3.1 WHEN TO USE THE BLUE CHANNEL

You should use the blue channel if you are travelling from a country within the European Union (EU) and you have no banned or restricted goods.

This exit is not seen present in the Nigerian airports. The reason could be that Nigeria does not differentiate between European citizens and other citizens.

5.1.3.2 WHEN TO USE THE GREEN CHANNEL

You should use the green channel if you are travelling from outside the EU and have with you less than ten thousand euros (or equivalent) in cash.

Customs officials from the UK Border Agency (UKBA) carry out checks on travellers in the green channel and **there are penalties for failing to declare goods. This can include seizure of: duty free allowance goods, any goods in excess of your duty-free allowance, any vehicle used to transport the goods.**

[215] U.S Department of Homeland Security, *'Declaring currency when entering the U.S in-transit to a foreign destination'* (https://help.cbp.gov) https://help.cbp.gov/app/answers/detail/a_id/778/~/declaring-currency-when-entering-the-u.s.-in-transit-to-a-foreign-destination Accessed 7th September 2014.

5.1.3.3 WHEN TO USE THE RED CHANNEL OR RED-POINT PHONE

You should use the red channel or the red-point phone if you have ten thousand euros or more (or equivalent) in cash.

You'll be able to speak to a UKBA officer either in person or by using the red-point phone. You should tell them everything that you are bringing into the country. The UKBA officer may ask to look inside your luggage.[216]

5.2 DISCUSSION

As stated earlier, Nigeria and the United Kingdom require travellers to orally declare whether they carry an amount of currency above the prescribed threshold, while the United States requires all travellers who carry an amount above a preset designated threshold to complete a written declaration form.

This section determines what the best approach is. The best approach is likely the one that protects the integrity of the financial system against money launderers and terrorist financiers and reduces the risk of money laundering and terrorist financing to the barest minimum.[217]

[216] HM Revenue and Customs, *'Going through customs'* (http://www.hmrc.gov.uk) http://www.hmrc.gov.uk/customs/arriving/customs-channels.htm Accessed 7th September 2014.
[217] The Financial Action Task Force (FATF): International Standards On Combating Money Laundering and the financing of terrorism and proliferation,(The FATF Recommendations) 2012, Page 9.

5.2.1 PROTECTING THE FINANCIAL SYSTEM AGAINST MONEY LAUNDERERS AND TERRORISTS

The oral declaration system adopted in Nigeria does not appear to be working as effectively as it is in the United Kingdom. This could be because the so-called system has not curtailed the movement of criminal property by the deadly terrorist group Boko Haram.

Boko Haram primarily uses a system of couriers to move cash around Nigeria and across the porous borders from neighbouring African states. This cash is said to be derived from lucrative criminal activities that involve kidnappings.[218] An investigation published in February 2020 by Premium Times showed that smugglers are still able to engage in their illicit transborder trade relying on compromised customs and immigration officers who take bribes.[219]

Nigeria's use of higher denomination bank notes than those of the United Kingdom could be one of the reasons why the oral declaration system does not work as effectively. People are able to move large sums of money around without being detected.

The problem could be solved if the federal government directed the Central Bank of Nigeria (CBN) to stop the production of higher denomination bank notes. This would enable law enforcement agents to identify persons carrying large sums of money.

---

[218] P. Stewart and L. Wroughton, *'How Boko Haram Is Beating US Efforts to Choke Its Financing'* (http://www.reuters.com, July 1, 2014) http://www.reuters.com/article/2014/07/01/us-usa-nigeria-bokoharam-insight-idUSKBN0F636920140701, accessed August 5, 2014.

[219] Premium Times, *'INVESTIGATION: Smuggling still rampant in Nigeria's northwestern boundaries despite border closure'*, (https://www.premiumtimesng.com/ 6 February 2020) Available at: https://www.premiumtimesng.com/investigationspecial-reports/375994-investigation-smuggling-still-rampant-in-nigerias-northwestern-boundaries-despite-border-closure.html (accessed 5 July 2022).

The written declaration system appears to be working effectively in the United States. So far, there has been little or no record of any terrorist threat from within the United States, apart from the Boston bombings.

5.3 CONCLUSION

In view of these arguments, the following are recommended:

I. The Central Bank of Nigeria should permanently stop producing the one thousand naira and five-hundred-naira banknotes and exclude it from circulation, taking into account concerns that these banknotes could facilitate illicit activities. This is in line with the decision and approach of the European Central Bank to permanently stop producing the €500 banknote and to exclude it from the Europa series, taking into account concerns that this banknote could facilitate illicit activities.[220]

II. The Economic and Financial Crimes Commission should direct banks in Nigeria to monitor the bank accounts of customs and immigration officers who are stationed at the land borders for potential signs of corruption and money laundering.[221] Due diligence and account monitoring procedures should be performed on these accounts under the supervision of the AML/CFT Chief Compliance Officer.[222]

III. The Nigeria Custom Service and Immigration Service should have a policy that mandates that the lie detector test should be taken once in 5 years by all staff of

[220] European Central Bank, *'ECB ends production and issuance of €500 banknote'*, (https://www.ecb.europa.eu May 4, 2016) Available at: https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html (accessed 5 July 2022).
[221] Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 38(1).
[222] Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 38(3).

the organization. For Staff who are positioned at the land borders, the lie detector test should be taken every three years. This will enable the lie detector policy to be more effective. Let us take for example, a person passes the lie detector test genuinely without any influence of corruption; there is still a possibility that the person may change over time. The temptation to follow current employees to collect bribes is very high. But if the organization put a policy in place that mandates every Personnel to take the lie detector test every five years starting from the first five years after recruitment, the cankerworm called corruption may be curbed effectively. Imagine if every employee knew that they were going to be asked by an examiner, 5 years after working, to confirm if they ever collected bribe during the time they worked in the institution, most employees will desist from taking bribes or engaging in corrupt acts. The above measure will ensure that current employees who are chosen as examiners for the lie detector tests are fit and proper persons for the job.

CHAPTER 6

RECORD KEEPING

The Financial Action Task Force (FATF) has advised countries to enact laws that mandate financial institutions to keep all records obtained through CDD measures (e.g., copies or records of official identification documents like passports, identity cards, driving licences or similar documents); account files and business correspondence, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, unusual large transactions) for at least five years after the business relationship ends or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures. The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.[223]

Although there is no material difference in the approaches adopted by Nigeria, the United States and the United Kingdom in relation to record-keeping requirements, it is still necessary to discuss this topic.

This chapter critically analyses the rule-based approach that is applied to record-keeping requirements under the subheading 'The Risk-Based Approach to Record-Keeping Requirements'.

[223] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 11

6.1 THE RISK-BASED APPROACH TO RECORD-KEEPING REQUIREMENTS

The FATF requires financial institutions to apply a rule-based approach to record-keeping requirements. In other words, financial institutions are required by law to maintain records on transactions and information obtained through the CDD measures for a minimum period of five years.

A risk-based approach may be a preferable option to a rule-based approach.

A risk-based approach is designed to make it more difficult for money launderers and terrorist organizations to make use of financial institutions due to the increased focus on the identified higher-risk activities that are undertaken by these criminal elements.[224]

Countries should not be allowed to stipulate a minimum time frame for financial institutions to maintain records. Rather, the period should depend on whether or not the customer is high risk.

For customers who have been designated as higher risk by a firm, financial institutions should be allowed to keep records of information obtained through CDD measures for ten years or more. For customers designated as lower risk, financial institutions should be allowed to keep records of information obtained through CDD measures for as little as two years.

Keeping information for five years may lead to an unnecessary interference with a person's right to a private life, and such interference cannot be justified.

[224] FATF Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing, (High Level Principles and Procedures) (2007), paragraph 1.17.

6.2 CONCLUSION

In view of the arguments canvassed in section 10.1 of this chapter, a risk-based approach to record-keeping requirements is the preferable approach.

CHAPTER 7

REPORTING REQUIREMENTS

The Financial Action Task Force (FATF), the independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and financing the proliferation of weapons of mass destruction, advised countries to enact laws that mandate financial institutions and designated nonfinancial businesses and professions (DNFBPs) to file certain reports. These reports are to be filed when a financial institution or DNFBP suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing.[225]

Although countries have followed the advice of the FATF, the reporting requirements in different countries are not the same. For example, Nigeria and the United States require financial institutions to file suspicious transaction reports (STRs) and currency transaction reports (CTRs),[226] while countries like the United Kingdom require financial institutions to file only a suspicious activity report (SAR).[227]

[225] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation (The FATF Recommendations) (2012), Recommendation 20, 23.

[226] Money Laundering (Prevention and Prohibition) Act, 2022, sections 6, 2 and 10. See also the Codified Bank Secrecy Act Regulations 2010, s 1020.320 (b) (1), s 1022.320 (b) (1) and s 1010.311.

[227] The Joint Money Laundering Steering Group JMLSG, *Prevention of Money Laundering/Combating Terrorist Financing* (2013) revised version, Guidance for the United Kingdom Financial Sector Part I, Amended November 2013, Paragraph 6.33. Please note that STR and SAR are the same even if the names are different. For more information, see E.P Ellinger, *Modern Banking Law,* 5th edition (Oxford University Press, 2011), 97.

This chapter, therefore, compares the reporting requirements in Nigeria with those of the United States and the United Kingdom. The aim of such comparison is to determine if Nigeria needs to adopt the approach in these countries or if there is no need for reform.

This chapter briefly highlights the relevant money laundering laws/regulations in Nigeria, the United States and the United Kingdom. It will then compare the reporting requirements in Nigeria with those of the United States and the United Kingdom under five subheadings: 'What to File', 'Where to File', 'When to File', 'Confidentiality of SARs' and 'Penalties'. The chapter will later analyse issues that arise from the earlier comparison, with the aim of determining if there is need for reform.

7.1 RELEVANT MONEY LAUNDERING LAWS/REGULATIONS

7.1.1 NIGERIA

The laws enacted to combat money laundering in Nigeria include: the **Money Laundering (Prevention and Prohibition) Act, 2022, Central Bank of Nigeria (CBN) (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria) Regulations 2013** and the **Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Reporting Guidelines 2012**.

7.1.2 UNITED STATES

The laws enacted to combat money laundering in the United States include: the **Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the 'Bank Secrecy Act' or 'BSA') as**

amended, Codified Bank Secrecy Act (BSA) Regulations 2010, the **Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010** and the **Bank Secrecy Act/ Anti-Money Laundering Examination Manual for Money Service Businesses 2008.**

7.1.3 UNITED KINGDOM

The laws enacted to combat money laundering in the United Kingdom include: **Proceeds of Crime Act 2002 (as amended), Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017,** the **Financial Conduct Authority Handbook, Senior Management Arrangements, Systems and Controls (SYSC)** and the **Joint Money Laundering Steering Group JMLSG, Prevention of money laundering/combating terrorist financing, 2020 Revised Version, Guidance for the UK financial sector Part I Amended July 2020.**

7.2 REPORTING REQUIREMENTS

7.2.1 NIGERIA

7.2.1.1 WHAT TO FILE

A financial institution or designated non-financial institution is required to report any suspicious transaction.[228] A transaction is deemed to be suspicious if it involves a frequency which is unjustifiable or unreasonable[229] or is surrounded by conditions of unusual or unjustified complexity.[230] It is also deemed suspicious if it appears to have no

[228] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (2)
[229] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (1) (a)
[230] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (1) (b)

economic justification or lawful objective[231] or in the opinion of the financial institution or designated non-financial institution involves terrorist financing or is inconsistent with the known transaction pattern of the account or business relationship.[232] The report required to be filed is called a Suspicious Transaction Report (STR).[233]

In addition to reporting any suspicious transaction, a financial institution or designated non-financial institution is also required to report a transfer to or from a foreign country of funds or securities by a person or body corporate including a money service business of a sum exceeding ten thousand US dollars or its equivalent.[234] The law also requires a financial institution or designated non-financial institution to report in writing any single transaction, lodgement or transfer of funds in excess of five million naira or its equivalent in the case of an individual or ten million naira or its equivalent in the case of a body corporate.[235] The reports required to be filed is called a Currency Transaction Report (CTR).[236]

7.2.1.2 WHERE TO FILE

A financial institution or a designated non-financial institution is required to file a STR with the Nigerian Financial Intelligence Unit.[237]

[231] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (1) (c)
[232] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (1) (d), See also the CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 31 (1) for the definition of a Suspicious Transaction.
[233] Nigerian Financial Intelligence Unit: Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Reporting Guidelines 2012, Paragraph 2.
[234] Money Laundering (Prevention and Prohibition) Act, 2022, s. 3 (1)
[235] Money Laundering (Prevention and Prohibition) Act, 2022, s. 11 (1)
[236] Nigerian Financial Intelligence Unit: Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Reporting Guidelines 2012, Paragraph 2.
[237] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (2) (c)

A financial institution or a designated non-financial institution is also required to file a CTR for transfers to or from a foreign country of funds or securities by a person or body corporate including a money service business of a sum exceeding US$10,000 or its equivalent with the Nigerian Financial Intelligence Unit, Central Bank of Nigeria and Securities and Exchange Commission in writing.[238]

A financial institution or designated non-financial business and profession shall report to the Nigerian Financial Intelligence Unit in the case of a financial institution and to Special Control Unit Against Money Laundering in the case of a designated non-financial business and profession in writing, any single transaction, lodgment or transfer of funds in excess of —

(a) N5,000,000 or its equivalent, in the case of an individual; or

(b) N10,000,000 or its equivalent, in the case of a body corporate.[239]

7.2.1.3 WHEN TO FILE

A financial institution that suspects or has reason to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, is required to report its suspicions **immediately and without delay.**[240] The report must be filed within 24 hours.[241]

[238] Money Laundering (Prevention and Prohibition) Act, 2022, s. 3 (1).
[239] Money Laundering (Prevention and Prohibition) Act, 2022, s. 11 (1).
[240] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (1)
[241] Money Laundering (Prevention and Prohibition) Act, 2022, s. 7 (2). See CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 31 (3)

All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved.[242]

A transfer to or from a foreign country of funds or securities by a person or body corporate including a money service business of a sum exceeding US$10,000 or its equivalent must be reported in writing within one day from the date of the transaction.[243]

A financial institution or designated non-financial business and profession is required to report in writing within seven days, any single transaction, lodgment or transfer of funds in excess of —

(a) N5,000,000 or its equivalent, in the case of an individual ; or

(b) N10,000,000 or its equivalent, in the case of a body corporate.[244]

7.2.1.4 CONFIDENTIALITY OF STRs/TIPPING OFF (GENERAL RULE)

Financial institutions, their directors, officers and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed with the competent authorities.[245]

7.2.1.5 CONFIDENTIALITY OF STRs/TIPPING OFF (EXCEPTION)

There are no exceptions to the general rule.[246]

[242] CBN (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 32 (7)
[243] Money Laundering (Prevention and Prohibition) Act, 2022, s. 3 (1).
[244] Money Laundering (Prevention and Prohibition) Act, 2022, s. 11 (1)
[245] Money Laundering (Prevention and Prohibition) Act, 2022, s. 19 (1) (a)

7.2.1.6 PENALTIES

A person who discloses the fact that a report is required to be filed is liable on conviction to a fine of not less than ten million naira or imprisonment for a term of at least two years.[247]

A person who fails to file a STR or CTR would be liable to a fine of ten million naira or imprisonment for a term of at least three years or both, in the case of an individual and twenty-five million naira in the case of a body corporate.[248]

7.2.2 UNITED STATES

7.2.2.1 WHAT TO FILE

7.2.2.1.1 BANKS

Every bank is required to file a report of any suspicious transaction relevant to a possible violation of law or regulation.[249] A transaction requires reporting if it is conducted or attempted by, at, or through the bank, it involves or aggregates at least five thousand dollars in funds or other assets, and the bank knows, suspects or has reason to suspect that:

i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location,

[246] Money Laundering (Prevention and Prohibition) Act, 2022, s. 19 (1) which provides for no exception to the General Rule
[247] Money Laundering (Prevention and Prohibition) Act, 2022, s. 19 (2) (a)
[248] Money Laundering (Prevention and Prohibition) Act, 2022, s. 19 (2) (b)
[249] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (a) (1)

or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation,

ii. The transaction is designed to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act, or

iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[250]

A suspicious transaction shall be reported by completing a Suspicious Activity Report (SAR).[251]

In addition to filing of a SAR, Banks are required to file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to such financial institution which involves a transaction in currency of more than ten thousand US dollars. This report is referred to as a Currency Transaction Report.[252]

7.2.2.1.2 MONEY SERVICE BUSINESSES

Every money service business is required to file a report of any suspicious transaction relevant to a possible violation of law or regulation.[253] A transaction requires reporting if it is conducted or attempted by, at or through a money service business, involves or aggregates funds or other assets of at least two thousand dollars and the money service

[250] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (a) (2)
[251] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (b) (1)
[252] Codified Bank Secrecy Act Regulations 2010, s. 1010.311
[253] Codified Bank Secrecy Act Regulations 2010, s. 1022.320 (a) (1)

business knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

i. Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation.

ii. Is designed, whether through structuring or other means, to evade any requirements of this chapter or of any other regulations promulgated under the Bank Secrecy Act, as amended.

iii. Serves no business or apparent lawful purpose, and the reporting money service business knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

iv. Involves use of the money service business to facilitate criminal activity.[254]

A suspicious transaction shall be reported by completing a Suspicious Activity Report – MSB ('SAR-MSB')[255]

In addition to filing a SAR, a money service business is also required to file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by,

[254] Codified Bank Secrecy Act Regulations 2010, s. 1022.320 (a) (2)
[255] Codified Bank Secrecy Act Regulations 2010, s. 1022.320 (b) (1)

through or to such financial institution which involves a transaction in currency of more than ten thousand dollars.[256]

7.2.2.2 WHERE TO FILE

7.2.2.2.1 BANKS

The SAR is to be filed with the Financial Crimes Enforcement Network (FinCEN) in a central location, to be determined by FinCEN, as indicated in the instructions to the SAR.[257]

The CTR is to be filed with the Commissioner of Internal Revenue, unless otherwise specified.[258]

7.2.2.2.2 MONEY SERVICE BUSINESSES

The SAR-MSB is to be filed in a central location to be determined by FinCEN, as indicated in the instructions to the SAR-MSB.[259]

The CTR is to be filed with the Commissioner of Internal Revenue, unless otherwise specified.[260]

[256] Codified Bank Secrecy Act Regulations 2010, s. 1010.311
[257] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (b) (2)
[258] Codified Bank Secrecy Act Regulations 2010, s. 1010.306 (a) (3)
[259] Codified Bank Secrecy Act Regulations 2010, s. 1022.320 (b) (2)
[260] Codified Bank Secrecy Act Regulations 2010, s. 1010.306 (a) (3)

7.2.2.3 WHEN TO FILE

7.2.2.3.1 BANKS

A bank is required to file a SAR no later than 30 calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, a bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case is reporting to be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. In situations involving violations that require immediate attention, such as, for example, on-going money laundering schemes, the bank shall notify by telephone, an appropriate law enforcement authority in addition to filing timely a SAR.[261]

A CTR is also required to be filed by the bank within 15 days following the day on which the reportable transaction occurred.[262]

7.2.2.3.2 MONEY SERVICE BUSINESSES

A money service business is required to file each SAR-MSB no later than 30 calendar days after the date of the initial detection by the money service business of facts that may constitute a basis for filing a SAR-MSB.[263]

A CTR is also required to be filed by the money service business within 15 days following the day on which the reportable transaction occurred.[264]

[261] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (b) (3)
[262] Codified Bank Secrecy Act Regulations 2010, s. 1010.306 (a) (1)
[263] Codified Bank Secrecy Act Regulations 2010, s. 1022.320 (b) (3)
[264] Codified Bank Secrecy Act Regulations 2010, s. 1010.306 (a) (1)

7.2.2.4 CONFIDENTIALITY OF SARs/TIPPING OFF (GENERAL RULE)

7.2.2.4.1 BANKS AND MONEY SERVICE BUSINESSES

No bank/money service business and no director, officer, employee, or agent of any bank/money service business is to disclose a SAR or any information that would reveal the existence of a SAR. Any bank, and any director, officer, employee, or agent of any bank/money service business that is subpoenaed or otherwise requested to disclose a SAR or any information that would reveal the existence of a SAR, shall decline to produce the SAR or such information. The bank/money service business is also to notify FinCEN of any such request and the response thereto.[265]

7.2.2.5 CONFIDENTIALITY OF SARs/TIPPING OFF (EXCEPTIONS)

7.2.2.5.1 BANKS AND MONEY SERVICE BUSINESSES

The disclosure by a bank/money service business, or any director, officer, employee, or agent of a bank/money service business of:

i. A SAR, or any information that would reveal the existence of a SAR, to FinCEN or any Federal, State, or Local Law enforcement agency, or any Federal regulatory authority that examines the bank/money service business for compliance with the Bank Secrecy Act, or any State regulatory authority administering a State law that requires the bank/money service business to

[265] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (e) (1), s 1022.320 (d) (1)

comply with the Bank Secrecy Act or otherwise authorizes the State authority to ensure that the bank/money service business complies with the Bank Secrecy Act;[266] or

ii. The underlying facts, transactions and documents upon which a SAR is based, including but not limited to, disclosures to another financial institution, or any director, officer, employee, or agent of a financial institution, for the preparation of a Joint SAR;[267] or

iii. The sharing by a bank/money service business, or any director, officer, employee, or agent of the bank/money service business, of a SAR, or any information that would reveal the existence of a SAR, within the bank's/money service business's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act as determined by regulation or in guidance is not prohibited.[268]

7.2.2.6 PENALTIES

7.2.2.6.1 CIVIL PENALTY

i. For any wilful violation, committed on or before October 12, 1984, of any reporting requirement for financial institutions, the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who wilfully participates in the violation, a civil penalty not to exceed one thousand dollars.[269]

[266] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (e) (1) (A) (1), s 1022.320 (d) (1) (A) (1)
[267] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (e) (1) (A) (2), s 1022.320 (d) (1) (A) (2)
[268] Codified Bank Secrecy Act Regulations 2010, s. 1020.320 (e) (1) (B), s 1022.320 (d) (1) (B)
[269] Codified Bank Secrecy Act Regulations 2010, s. 1010.820 (a)

ii. For any wilful violation committed after October 12, 1984 and before October 28, 1986, of any reporting requirement for financial institutions, the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who wilfully participates in the violation, a civil penalty not to exceed ten thousand dollars.[270]

iii. For any wilful violation committed after October 27, 1986, of any reporting requirement for financial institutions under this part (except §103.24, §103.25 or §103.32), the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who wilfully participates in the violation, a civil penalty not to exceed the greater of the amount (not to exceed $100,000) involved in the transaction or twenty five thousand dollars.[271]

7.2.2.6.2 CRIMINAL PENALTY

Any person who violates any provision, may, upon conviction thereof, be fined not more than two hundred and fifty thousand dollars or be imprisoned not more than 5 years, or both.[272]

7.2.3 UNITED KINGDOM

7.2.3.1 WHAT TO FILE

A firm's nominated officer must report any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may

[270] Codified Bank Secrecy Act Regulations 2010, s. 1010.820 (b)
[271] Codified Bank Secrecy Act Regulations 2010, s. 1010.820 (f)
[272] Codified Bank Secrecy Act Regulations 2010, s. 1010.840 (b)

be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing.[273] Such report is called a Suspicious Activity Report.[274]

7.2.3.2 WHERE TO FILE

To avoid committing a failure to report offence, nominated officers must make their disclosures to the National Crime Agency (NCA). The national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UK Financial Intelligence Unit (FIU) within the NCA.[275]

7.2.3.3 WHEN TO FILE

Such reports must be made as soon as is reasonably practicable after the information comes to him.[276]

7.2.3.4 CONFIDENTIALITY OF SARs/TIPPING OFF (GENERAL RULE)

A person is not to disclose a SAR if such disclosure is likely to prejudice any investigation that might be conducted following the disclosure and the information on

[273] Proceeds of Crime Act 2002 (as amended), s. 331, The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 19 (4) (d) and the Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing,* 2020 Revised Version, Guidance for the UK financial sector Part I Amended July 2020, Paragraph 6.33.
[274] Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing,* 2020 Revised Version, Guidance for the UK financial sector Part I Amended July 2020, Chapter 6, See also P Lilley, *Dirty Dealing: The Untold Truth About Global Money Laundering, International Crime and Terrorism* (3rd Edition, Kogan Page Limited, 2006) 209.
[275] Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing,* 2020 Revised Version, Guidance for the UK financial sector Part I Amended July 2020, Paragraph 6.40
[276] Joint Money Laundering Steering Group JMLSG, *Prevention of money laundering/combating terrorist financing,* 2020 Revised Version, Guidance for the UK financial sector Part I Amended July 2020, Paragraph 6.33

which the disclosure is based came to the person in the course of a business in the regulated sector.[277]

7.2.3.5 CONFIDENTIALITY OF SARs/TIPPING OFF (EXCEPTION)

i. An employee, officer or partner of an undertaking does not commit an offence if the disclosure is to an employee, officer or partner of the same undertaking.[278]

ii. A person does not commit an offence in respect of a disclosure by a credit institution or a financial institution if—

   a. The disclosure is to a credit institution or a financial institution,

   b. The institution to whom the disclosure is made is situated in an EEA State or in a country or territory imposing equivalent money laundering requirements, and

   c. Both the institution making the disclosure and the institution to which it is made belong to the same group.[279]

iii. A professional legal adviser or a relevant professional adviser does not commit an offence under section 333A if—

   (a) The disclosure is to professional legal adviser or a relevant professional adviser,

   (b) both the person making the disclosure and the person to whom it is made carry on business in an EEA State or in a country or territory imposing equivalent money laundering requirements, and

[277] Proceeds of Crime Act 2002 (as amended), s. 333A (1)
[278] Proceeds of Crime Act 2002 (as amended), s. 333B (1)
[279] Proceeds of Crime Act 2002 (as amended), s. 333B (2)

(c) Those persons perform their professional activities within different undertakings that share common ownership, management or control.[280]

7.2.3.6 PENALTIES

7.2.3.6.1 TIPPING OFF

A person guilty of the offence of tipping off is liable on summary conviction to imprisonment for a term not exceeding 3 months or to a fine not exceeding level 5 on the standard scale or to both[281] and on conviction on indictment, to imprisonment for a term not exceeding two years, or to a fine, or to both.[282]

7.2.3.6.2 FAILURE TO FILE A SAR

A person guilty of not filing a SAR is liable on summary conviction for a term not exceeding 6 months or to a fine not exceeding the statutory maximum or to both,[283] and on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.[284]

[280] Proceeds of Crime Act 2002 (as amended), s. 333B (4), See also Proceeds of Crime Act 2002 (as amended), s 333C and D for more exceptions.
[281] Proceeds of Crime Act 2002 (as amended), s. 333A (4) (a)
[282] Proceeds of Crime Act 2002 (as amended), s. 333A (4) (b)
[283] Proceeds of Crime Act 2002 (as amended), s. 334 (2) (a)
[284] Proceeds of Crime Act 2002 (as amended), s. 334 (2) (b)

7.3 DISCUSSION

The previous section compared the reporting requirements in Nigeria with those of the United States and the United Kingdom. This section analyses the issues that arose from the comparison, with the aim of determining if there is need for reform.

7.3.1 WHAT TO FILE

As stated earlier, Nigerian and US money laundering laws require financial institutions to file currency transaction reports (CTRs) and suspicious transaction reports (STRs), while the United Kingdom's law requires that financial institutions file only suspicious activity reports (SARs). Is it necessary for Nigerian and US money laundering laws to mandate financial institutions to file CTRs since they are not required by the United Kingdom?

The question can be answered by looking briefly into the history behind the US Bank Secrecy Act. In 1970, Congress passed the Currency and Foreign Transactions Reporting Act, commonly known as the Bank Secrecy Act, which established requirements for record keeping and reporting by private individuals, banks and other financial institutions. The Bank Secrecy Act was designed to help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions. The statute requires individuals, banks and other financial institutions to file currency reports with the US Department of the Treasury, properly identify persons conducting transactions and maintain a paper trail by keeping appropriate records of financial transactions. These records enable law enforcement and regulatory agencies to pursue investigations of criminal tax and regulatory violations, if warranted, and provide evidence that is useful in prosecuting money laundering and other financial crimes.

In April 1996, a suspicious activity report (SAR) was developed to be used by all banking organizations in the United States. A banking organization is required to file a SAR whenever it detects a known or suspected criminal violation of federal law, a suspicious transaction related to money laundering activity or a violation of the Bank Secrecy Act.[285]

Legislators did not remove the CTR requirement, even though the SAR seeks to achieve the same objective, which is identifying the source, volume and movement of currency and preventing money laundering.

The international law the United States based its 1996 development on required financial institutions to file both a CTR and a STR.[286] This international law has been updated several times, with the most recent version requiring only an STR to be filed.[287]

Since the CTR requirement seeks to achieve a similar objective as the SAR requirement, it's no surprise that the UK money laundering law does not include the CTR requirement. This strengthens the argument that it may not be necessary for a financial institution to be required by law to file a CTR.

7.3.2 WHEN A TRANSACTION REQUIRES REPORTING

As stated earlier, the Nigerian and United Kingdom money laundering laws require all suspicious transactions, including attempted transactions, to be reported, regardless of the amount involved. This position is different from that of the US Bank Secrecy Act,

[285] Federal Financial Institutions Examination Council: *Bank Secrecy Act/Anti–Money Laundering Examination Manual* (2010), 7–8.
[286] The Forty Recommendations of the Financial Action Task Force on Money Laundering (1990), Recommendations 16, 24; The Financial Action Task Force on Money Laundering, The Forty Recommendations (1996), Recommendations 15, 23.
[287] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 20.

which sets a particular threshold for reporting. This section of the chapter seeks to determine which of these requirements is preferable.

A threshold requirement appears to allow businesses to flourish because bank customers who engage in transactions below five thousand dollars will not have their transactions stalled by ongoing investigations. However, the threshold mechanism can be circumvented with techniques like smurfing.[288]

Therefore, the 'no threshold rule' is preferable.

7.3.3 CONFIDENTIALITY OF SARS

The Money Laundering (Prevention and Prohibition) Act, 2022 (MLPA 2022) provides no exceptions to the general rule of tipping off, which is contrary to the positions of the United Kingdom and the United States. This section of the chapter seeks to determine if the tipping-off provision in MLPA 2022 needs to be amended to include detailed exceptions.

The tipping-off provision, as currently drafted, could cause serious problems for financial institutions and designated nonfinancial institutions. First, it is not clear if a disclosure by a financial institution to law enforcement agents is permitted. Second, it is not clear if a disclosure by a financial institution to another financial institution is permitted. Third, it is not clear if a disclosure by a professional legal adviser to another professional legal adviser is permitted. All these disclosures are stated in both the UK and US laws as clear exceptions to the general rule of tipping off.

[288] Smurfing is the act of breaking down a transaction into smaller transactions to avoid regulatory requirements or an investigation by the authorities. http://financial-dictionary.thefreedictionary.com/Smurfing

In view of the above arguments, the tipping-off provision in MLPA 2022 needs to be amended to contain detailed exceptions like those of the United Kingdom and the United States.

7.4 CONCLUSION

This chapter compared the reporting requirements in Nigeria with those of the United States and the United Kingdom. It has also analysed issues that arose from the comparison to determine the need for reform. This section focuses on those areas that need reform.

Based on the arguments in Section 7.3 of this chapter, the following reforms to MLPA 2022 are recommended:

I. Sections three and eleven of MLPA 2022 should be deleted, and section seven should remain intact. In other words, firms should be required to file only STRs and should no longer be required to file CTRs.

II. Section 19 (1) (a) of MLPA 2022 and Regulation 31 (6) of CBN (Anti–Money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria) Regulations 2013 should be amended to include exceptions to the general rule of tipping off, as stated in the US Codified Bank Secrecy Act Regulations 2010.[289] Alternatively, the exceptions could be added to Section 333B, 333D (1) and (2) and 333D (3) of the United Kingdom's Proceeds of Crime Act 2002 (as amended).

[289] Codified Bank Secrecy Act Regulations (2010), s. 1020.320 (e) (1) (A) (1), s. 1022.320 (d) (1) (A) (1), s. 1020.320 (e) (1) (A) (2), s. 1022.320 (d) (1) (A) (2), s. 1020.320 (e) (1) (B), s. 1022.320 (d) (1) (B).

CHAPTER 8

COMPLIANCE OFFICERS

The Financial Action Task Force (FATF) has advised countries to enact laws that require financial institutions to implement programmes against money laundering and terrorist financing. These programmes should include the appointment of a compliance officer at the management level.[290]

A compliance officer is responsible for the oversight of the firm's anti–money laundering (AML) systems and controls, which include appropriate training for the firm's employees in relation to money laundering and considering each report received from staff to determine whether it gives rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering.[291]

Although countries have followed the advice of the FATF, the enacted laws are not identical. For example, Nigeria and the United States require financial institutions to appoint compliance officers who receive disclosures from staff and who train staff.[292] The United Kingdom requires financial institutions to appoint compliance officers with the

[290] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the financing of terrorism and proliferation, (The FATF Recommendations) 2012, Recommendation 18
[291] Money Laundering (Prevention and Prohibition) Act, 2022, s. 10 (1); Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti–Money Laundering Examination Manual (2010)*, 36; Senior Management Arrangements, Systems and Controls (SYSC), 6.3.9 (1) R, see also SYSC, 6.3.7 G.
[292] Money Laundering (Prevention and Prohibition) Act, 2022, s. 10 (1); Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti–Money Laundering Examination Manual* (2010), 36.

responsibility of training staff,[293] but the duty of receiving disclosures from staff rests on the nominated officer.[294]

This chapter compares the approach adopted in Nigeria and the United States with that of the United Kingdom, with the aim of determining if Nigeria and the United States should adopt the approach of the United Kingdom or if there is no need for reform.

The comparison will be made under two subheadings: 'The Title of the Individual Responsible for Anti–Money Laundering Compliance' and 'Duties and Responsibilities'. The chapter will later analyse issues that arise from the comparison to determine if there is need for reform.

8.1 THE TITLE OF THE INDIVIDUAL RESPONSIBLE FOR ANTI MONEY LAUNDERING COMPLIANCE

8.1.1 NIGERIA

The individual responsible for coordinating and monitoring day-to-day Anti Money Laundering compliance is known as the compliance officer.[295]

8.1.2 UNITED STATES

The individual responsible for coordinating and monitoring day-to-day Anti Money Laundering compliance is known as the compliance officer.[296]

[293] Senior Management Arrangements, Systems and Controls (SYSC), 6.3.9 (1) R, see also SYSC, 6.3.7 G.
[294] Proceeds of Crime Act 2002 (as amended), ss. 337, 338; Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 19 (4) (d).
[295] Money Laundering (Prevention and Prohibition) Act, 2022, s. 10 (1) (a)

8.1.3 UNITED KINGDOM

The individual responsible for coordinating and monitoring day-to-day Anti Money Laundering compliance is known as the money laundering reporting officer.[297]

The title given to such individual appears to be different from that of the FATF.

8.2 DUTIES AND RESPONSIBLITIES

8.2.1 NIGERIA

Compliance officers are under a duty: to receive disclosures from staffs in the firm and to train staffs in the firm.[298]

8.2.2 UNITED STATES

Compliance officers are under a duty: to receive disclosures from staffs in the firm and to train staffs in the firm.[299]

8.2.3 UNITED KINGDOM

Compliance officers are under a duty to train staffs in the firm.[300] The duty to receive disclosures from staffs in the firm rests on the Nominated Officer.[301]

---

[296] Federal Financial Institutions Examination Council: Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010, Page 36
[297] Senior Management Arrangements, Systems and Controls (SYSC), 6.3.9 (1) R, see also SYSC, 6.3.7 G
[298] Money Laundering (Prevention and Prohibition) Act, 2022, s. 10 (1)
[299] Federal Financial Institutions Examination Council: Bank Secrecy Act/Anti-Money Laundering Examination Manual 2010, Page 36
[300] Senior Management Arrangements, Systems and Controls (SYSC), 6.3.9 (1) R, see also SYSC, 6.3.7 G

In practice, the compliance officer and nominated officer will be one and the same person.[302]

8.3 DISCUSSION

The previous section compared the approach in Nigeria with that in the United States and the United Kingdom as it relates to compliance officers. This section will analyse issues that arose to determine if there is a need for reform.

8.3.1 MINIMUM REQUIREMENTS OF COMPLIANCE OFFICERS

In its attempt to ensure strict compliance with all extant regulations; particularly those relating to foreign exchange transactions, Financial Action Task Force (FATF) and Anti-Money Laundering/ Combating the Financing of Terrorism (AML/CFT), the CBN via a circular dated September 28, 2016, decided to enhance the minimum qualifications for the position of the Chief Compliance Officers (CCOs) of Deposit Money Banks (DMBs).

Going forward, DMBs are required to appoint not only a CCO who must not be below the rank of a General Manager regardless of the category of institution but also an Executive Compliance Officer (ECO) who should not be below the rank of an Executive Director. The CCO will report to the ECO while the ECO will in turn report directly to the Board of Directors.

The CBN will hold the Executive Compliance Officer responsible and accountable for any breach of any extant regulation in the DMBs. For avoidance of doubt, the CBN shall

---

[301] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulation 19 (4) (d).

[302] The Joint Money Laundering Steering Group JMLSG, Prevention of money laundering/combating terrorist financing 2020 Revised Version, Guidance for the UK financial sector Part I, Amended July 2020, Paragraph 3.4.

suspend/dismiss any ECO and CCO found wanting in the discharge of his/her responsibility.

DMBs are required to forward the names of their ECO and CCO together with their curriculum vitae to the CBN for approval. The ECOs are however allowed to combine the responsibility with other functions while CCOs will focus ONLY on compliance matters in the bank.[303]

The fitness requirements for appointment to the office of Chief Compliance Officer and Executive Compliance Officer is as provided in the Fit and Proper (Approved Persons) Framework for General Managers and Executive Directors.

The Recommended Additional Certification for the office of Chief Compliance Officer and Executive Compliance Officer is the International Compliance Association Certificate (ICA). or Certified Anti Money Laundering Specialists (CAMS), or Certified Fraud Examiner (CFE).[304]

The CBN, via a circular to Banks, Discount Houses and other Financial Institutions dated the 17th of November, 2014, had noted the onerous challenge of having dedicated Compliance Officers (CO) at each branch of a bank and has given dispensation that banks may elect to operate a *cluster structure, whereby a designated CO would be responsible for a cluster of branches instead of having a CO at each branch, as earlier advised in the circular under reference.* Consequently, the CBN has approved the

[303] Central Bank of Nigeria, *'Circular to All Deposit Money Banks (DMBs)'*, (https://www.cbn.gov.ng/ 28 September 2016) Available at: https://www.cbn.gov.ng/out/2016/fprd/aml%20september%202016%20circular%20to%20banks%20on%20ccos%20(2).pdf (accessed 15 April, 2019).

[304] Central Bank of Nigeria, *'Circular to Banks, Discount Houses and Other Financial Institutions: Status and Reporting Line of Chief Compliance Officers'*, (https://www.cbn.gov.ng/ 17 November 2014) Available at: https://www.cbn.gov.ng/out/2014/fprd/status%20and%20reporting%20line%20of%20chief%20compliance%20officers.pdf (accessed 15 April, 2019).

establishment of Zonal Compliance Officers for banks, who must at a minimum, be on the same level with the management of the Zones where they work. Branch /Cash Centres, therefore, need not have Compliance Officers, provided the Compliance Officer at the Zone that controls the Branch/Cash Centre, effectively performs compliance functions at the Branch/Cash Centre. **Where a bank or a financial institution decides to operate the cluster arrangement, details of such arrangement must be sent to the Director, Banking Supervision Department, or Director, Other Financial Institutions Department CBN, as the case may be, for prior approval.**

The cluster structure must however take into cognisance, the size, number and proximity to each branch as well as the level of automation of the compliance function, without compromising compliance. **It is important to note that the function of Compliance Office(r) must be clearly separated from that of internal Control/Audit.** Compliance Officers of Banks, Discount Houses and Other Financial Institutions should meet the criteria specified for the category of their institutions.

All banks and other financial institutions are hereby enjoined to comply strictly with the requirements of this circular.[305]

Despite the advantages of the fit and proper test, there have been damning reports that some politicians are using fraudsters working in banks to launder public funds. According to the **Economic and Financial Crimes Commission**, fraudsters have been aiding politically exposed and other persons to commit various financial crimes.[306] This

[305] Central Bank of Nigeria, *'Circular to Banks, Discount Houses and Other Financial Institutions: Status and Reporting Line of Chief Compliance Officers'*, (https://www.cbn.gov.ng/ 17 November 2014) Available at: https://www.cbn.gov.ng/out/2014/fprd/status%20and%20reporting%20line%20of%20chief%20compliance%20officers.pdf (accessed 15 April, 2019).

[306] The Punch, *'Fraudsters working in banks, aiding corrupt politicians –EFCC'*, (https://punchng.com/ 6 April 2019) Available at: https://punchng.com/fraudsters-working-in-banks-aiding-corrupt-politicians-efcc/ (accessed 6 April, 2019).

revelation epitomises systemic failure aggravated by the Central Bank of Nigeria's weak regulation.

The **Financial Conduct Authority** (the conduct regulator for 56,000 financial services firms and financial markets in the United Kingdom and the prudential regulator for over 18,000 of those firms), on the other hand, has taken action against firms for violating anti-money laundering laws. On the **31st of January, 2017**, the **Financial Conduct Authority** (FCA) fined Deutsche Bank AG (Deutsche Bank) £163,076,224 for failing to maintain an adequate anti-money laundering (AML) control framework during the period between 1 January 2012 and 31 December 2015. This is the largest financial penalty for AML controls failings ever imposed by the FCA, or its predecessor the Financial Services Authority (FSA).

According to the **Financial Conduct Authority**, Deutsche Bank exposed the UK financial system to the risks of financial crime by failing to properly oversee the formation of new customer relationships and the booking of global business in the UK. As a consequence of its inadequate AML control framework, Deutsche Bank was used by unidentified customers to transfer approximately $10 billion, of unknown origin, from Russia to offshore bank accounts in a manner that is highly suggestive of financial crime.

Mark Steward, Director of Enforcement and Market Oversight at the FCA, said:

"Financial crime is a risk to the UK financial system. Deutsche Bank was obliged to establish and maintain an effective AML control framework. By failing to do so, Deutsche Bank put itself at risk of being used to facilitate financial crime and exposed the UK to the risk of financial crime."

"The size of the fine reflects the seriousness of Deutsche Bank's failings. We have repeatedly told firms how to comply with our AML requirements and the failings of Deutsche Bank are simply unacceptable. Other firms should take notice of today's fine and look again at their own AML procedures to ensure they do not face similar action."

The FCA found significant deficiencies throughout Deutsche Bank's AML control framework. The FCA specifically found that, during the relevant period, Deutsche Bank's Corporate Banking and Securities division (CB&S) in the UK:

- performed inadequate customer due diligence
- failed to ensure that its front office took responsibility for the CB&S division's Know Your Customer obligations
- used flawed customer and country risk rating methodologies
- had deficient AML policies and procedures
- had an inadequate AML IT infrastructure
- lacked automated AML systems for detecting suspicious trades
- failed to provide adequate oversight of trades booked in the UK by traders in non-UK jurisdictions

As a result of these failings Deutsche Bank failed to obtain sufficient information about its customers to inform the risk assessment process and to provide a basis for transaction monitoring. The failings allowed the front office of Deutsche Bank's Russia-based subsidiary (DB Moscow) to execute more than 2,400 pairs of trades that mirrored each other (mirror trades) between April 2012 and October 2014.

The mirror trades were used by customers of Deutsche Bank and DB Moscow to transfer more than $6 billion from Russia, through Deutsche Bank in the UK, to overseas

bank accounts, including in Cyprus, Estonia, and Latvia. The orders for both sides of the mirror trades were received by DB Moscow, which executed both sides at the same time.

The customers on the Moscow and London sides of the mirror trades were connected to each other and the volume and value of the securities was the same on both sides. The purpose of the mirror trades was the conversion of Roubles into US Dollars and the covert transfer of those funds out of Russia, which is highly suggestive of financial crime.

A further $3.8 billion in suspicious “one-sided trades” also occurred. The FCA believes that some, if not all, of an additional 3,400 trades formed one side of mirror trades and were often conducted by the same customers involved in the mirror trading.

As a result, Deutsche Bank breached Principle 3 (taking reasonable steps to organise its affairs responsibly and effectively, with adequate risk management systems) of the FCA’s Principles for Businesses. In addition, Deutsche Bank also breached Senior Management Arrangements, Systems and Controls (SYSC) rules 6.1.1 R and 6.3.1 R.

The FCA emphasises the importance of having a strong AML control framework through its proactive supervisory programmes on AML. Firms are regularly reminded of the importance of safeguarding the UK financial system from financial crime and how to comply with AML requirements.

Deutsche Bank agreed to settle at an early stage of the FCA’s investigation and therefore qualified for a 30% (stage 1) discount. This discount does not apply to the £9.1 million in commission that Deutsche Bank generated from the suspicious trading, which has been disgorged as part of the overall penalty meaning that the firm has received no

financial benefit from the breach. Were it not for the 30% discount the financial penalty would have been £229,076,224.[307]

On the **6th day of June, 2018**, the Financial Conduct Authority fined Canara Bank £896,100 for anti-money laundering systems failings and imposed a restriction, preventing it from accepting deposits from new customers for 147 days. According to the Financial Conduct Authority, Between 26 November 2012 and 29 January 2016, Canara failed to maintain adequate anti-money laundering systems and failed to take sufficient steps to remedy identified weaknesses, despite having been notified of shortcomings in its anti-money laundering systems and controls. Mark Steward, Executive Director of Enforcement and Market Oversight at the Financial Conduct Authority, said:

"Financial crime and money–laundering failures are areas of focused priority for us. Canara was warned its money laundering controls were inadequate and so its failure to remediate them properly is at the more serious end of the range of sanctions."

The Final Notice highlights the importance of branches of overseas banks and their senior management having sufficient understanding of their regulatory responsibilities and ensuring those obligations are met with appropriate resources. Specifically, the Financial Conduct Authority found that Canara failed to maintain adequate systems and controls to manage the risk of money laundering. These failures were systemic and affected almost all levels of its business and governance structure including: (1) Senior Management; (2) Governance/Oversight; (3) three Lines of Defence; (4) Money laundering reporting function; and (5) AML systems and controls. As a result, Canara

[307] Financial Conduct Authority, *'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings'*, (https://www.fca.org.uk 31 January 2017), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure (accessed 6 April 2019).

breached Principle 3 (taking reasonable steps to organise its affairs responsibly and effectively, with adequate risk management systems) of the FCA's Principles for Businesses.

Canara agreed to resolve the case and qualified for a 30% discount.[308]

On the **19th day of March, 2019**, UBS AG (UBS) was fined £27,599,400 by the Financial Conduct Authority (FCA) for failings relating to 135.8 million transaction reports between November 2007 and May 2017.

Mark Steward, FCA Executive Director of Enforcement and Market Oversight said:

'Firms must have proper systems and controls to identify what transactions they have carried out, on what markets, at what price, in what quantity and with whom. If firms cannot report their transactions accurately, fundamental risks arise, including the risk that market abuse may be hidden.'

Effective market oversight relies on the complete, accurate and timely reporting of transactions. This information helps the FCA to effectively supervise firms and markets. In particular, transaction reports help the FCA identify potential instances of market abuse and combat financial crime.

UBS failed to ensure it provided complete and accurate information in relation to approximately 86.67m reportable transactions. It also erroneously reported 49.1m transactions to the FCA, which were not, in fact, reportable. Altogether, over a period of

[308] Financial Conduct Authority, *'FCA fines and imposes a restriction on Canara Bank for anti-money laundering systems failings'*, (https://www.fca.org.uk 6 June 2018), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-and-imposes-restriction-canara-bank-anti-money-laundering-systems-failings (accessed 6 April 2019).

9 and a half years, UBS made 135.8m errors in its transaction reporting, breaching FCA rules.

The FCA also found that UBS failed to take reasonable care to organise and control its affairs responsibly and effectively in respect of its transaction reporting. These failings related to aspects of UBS's change management processes, its maintenance of the reference data used in its reporting and how it tested whether all the transactions it reported to the FCA were accurate and complete.

UBS agreed to resolve the case and so qualified for a 30% discount in the overall penalty. Without this discount, the FCA would have imposed a financial penalty of £39,427,795.[309]

On the **28th day of March, 2019,** Goldman Sachs International (GSI) was fined £34,344,700 by the Financial Conduct Authority (FCA) for failing to provide accurate and timely reporting relating to 220.2 million transaction reports between November 2007 and March 2017. Mark Steward, FCA Executive Director of Enforcement and Market Oversight said:

'The failings in this case demonstrate a failure over an extended period to manage and test controls that are vitally important to the integrity of our markets. These were serious and prolonged failures. We expect all firms will take this opportunity to ensure they can fully detail their activity and are regularly checking their systems so any problems are detected and remedied promptly, unlike in this case.'

[309] Financial Conduct Authority, *'FCA fines UBS AG £27.6 million for transaction reporting failures'*, (https://www.fca.org.uk 19 March 2019), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-ubs-ag-276-million-transaction-reporting-failures (accessed 6 April 2019).

Accurate and complete transaction reporting helps underwrite market integrity and supervise firms and markets. In particular, transaction reports help the FCA identify potential instances of market abuse and combat financial crime. GSI failed to ensure it provided complete, accurate and timely information in relation to approximately 213.6m reportable transactions. It also erroneously reported 6.6m transactions to the FCA, which were not, in fact, reportable. Altogether, over a period of 9 and a half years, GSI made 220.2m errors in its transaction reporting, breaching FCA rules.

The FCA also found that GSI failed to take reasonable care to organise and control its affairs responsibly and effectively in respect of its transaction reporting. These failings related to aspects of GSI's change management processes, its maintenance of the counterparty reference data used in its reporting and how it tested whether all the transactions it reported to the FCA were accurate and complete.

GSI agreed to resolve the case and so qualified for a 30% discount in the overall penalty. Without this discount, the FCA would have imposed a financial penalty of £49,063,900.[310]

The Financial Crimes Enforcement Network (a bureau within the U.S. Department of the Treasury and is the federal authority that enforces the Bank Secrecy Act (BSA) by investigating and imposing civil money penalties on financial institutions, nonfinancial trades or businesses, and individuals for willful and negligent violations of the BSA and regulations or orders issued thereunder) has brought a number of enforcement actions

[310] Financial Conduct Authority, *'FCA fines Goldman Sachs International £34.3 million for transaction reporting failures'*, (https://www.fca.org.uk/ 28 March 2019), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-goldman-sachs-international-transaction-reporting-failures (accessed 6 April 2019).

against financial institutions in the United States for violations of the reporting, recordkeeping, or other requirements of the Bank Secrecy Act (BSA), 31 U.S.C. 5311 et seq., and its implementing regulations at 31 C.F.R. In 2021, three enforcement actions were initiated against financial institutions and in 2022, two enforcement actions have been brought so far and published on their official website.[311]

8.3.2 DUTIES AND RESPONSIBILITIES

As stated earlier, the duties of compliance officers in Nigeria and the United States include receiving disclosures from staff and training staff, while compliance officers in the United Kingdom train staff, but receiving disclosures from staff is the responsibility of the nominated officer.

This section will determine if Nigeria and the United States need to adopt the approach used in the United Kingdom, or if there is no need for reform.

The United Kingdom's approach allows for the responsibilities conferred on compliance officers by the FATF to be shared between two people, thereby reducing the burden of work on the compliance officers. This is not the approach adopted by Nigeria and the United States.

However, compliance officers in Nigeria and the United States could delegate some of their duties to other competent individuals.[312]

[311] Financial Crimes Enforcement Network, *'Enforcement Actions'*, (https://www.fincen.gov 2022), Available at https://www.fincen.gov/news-room/enforcement-actions (accessed 5 July 2022).
[312] Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti–Money Laundering Examination Manual* (2010), 36.

8.4 CONCLUSION

This chapter compared the approach in Nigeria with that of the United States and the United Kingdom as it relates to compliance officers. It has also analysed issues that arose from the comparison to determine if there is need for reform. This section focuses on those areas that need reform.

Based on the arguments canvassed in Section 8.3, the Central Bank of Nigeria should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the **Financial Action Task Force (FATF) Recommendations**. Available evidence suggests that the Economic and Financial Crimes Commission has recovered more than two trillion dollars in 12 years, as of February 2016. The money passed through the banks; much of it ended up in safe havens in Europe and other parts of the world. But delinquent banks pay a heavy price abroad when caught in such a labyrinth.[313] For instance, the Financial Crimes Enforcement Network (FinCEN), in coordination with the Office of the Comptroller of the Currency, and the United States Department of Justice, had on February 15, 2018, assessed a one hundred and eighty five million dollars civil money penalty against U.S. Bank National Association for willful violations of several provisions of the Bank Secrecy Act (BSA).[314] The Central Bank of Nigeria is strongly advised to enforce its regulations and punish errant banks/telecommunications companies so as to discourage their serial abuse of guidelines for the financial sector. This approach will strengthen Know Your

[313] The Punch, *'Court BVN ruling: Saving genuine account owners'*, (http://punchng.com/ 3 November 2017), Available at: http://punchng.com/court-bvn-ruling-saving-genuine-account-owners/ (accessed 8 April 2018).

[314] Financial Crimes Enforcement Network, '*FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws'*, (https://www.fincen.gov/ 15 February 2018), Available at: https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering (accessed 9 April 2018).

Customer policies, aimed at reducing fraud and money laundering. **This measure is in line with the Financial Action Task Force Recommendations (Recommendation 26).**

CHAPTER 9

PLEA BARGAINING

The Financial Action Task Force (FATF) has advised countries to adopt measures that enable their competent authorities to freeze or seize and confiscate laundered property.[315] These measures include the introduction of the concept of plea bargaining into a country's criminal justice system. This measure ensures that all criminal proceeds are confiscated.

In a plea bargain deal, both sides gain something from the arrangement. The prosecution gains a conviction without the time and expense of a trial, while the defendant might get a reduced sentence or have some of the charges dropped. In some cases, for example, the prosecution will offer a plea deal so that the victim does not have to go through the drama and stress of testifying at a trial.[316]

While countries have adopted the concept of plea bargaining into their criminal justice system, the application of the concept in these countries is not identical.

This chapter seeks to compare the approach in Nigeria with those of the United States and the United Kingdom to determine the best approach. This is likely the one that

[315] The Financial Action Task Force (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, (The FATF Recommendations) 2012, Interpretive Note to Recommendation 4

[316] C. Montaldo, *'The plea bargain stage of a criminal case, stages of the criminal justice system'* (http://crime.about.com) http://crime.about.com/od/Crime_101/a/The-Plea-Bargain-Stage-Of-A-Criminal-Case.htm, accessed July 4, 2014.

achieves the highest number of convictions without necessarily interfering with a person's right to a jury trial.[317]

This chapter will start by defining what plea bargaining is and giving a brief introduction of the history and nature of plea bargaining. Then it will compare the approach adopted in Nigeria with those of the United States and the United Kingdom.

9.1 DEFINITION OF PLEA BARGAINING

To a layman on the street, plea bargaining in the Nigerian context is a system in which room is provided for unfettered looting of public treasury at all levels of governance in our country. This is done in such a way that billions of naira is stolen, and some paltry millions are returned to the coffers of the government, while a large chunk of the looted public funds at the end of the day is left for the looter and his/her unborn generations.[318]

But to an Advocate of Legal Practice, plea bargaining consists of the exchange of official concessions for a defendant's act of self-conviction. These concessions may relate to the sentence imposed by the Court or recommended by the prosecution, the offence charged, or a variety of other circumstances; they may be explicit or implicit; and they may proceed from any of a number of officials.[319] The benefit offered by the defendant, however is always the same: entry of[320] a plea of guilty. This definition excludes unilateral exercises of prosecutorial or judicial discretion, such as an unqualified dismissal or reduction of charges. It also excludes the exchange of official concessions for actions other than entry of a guilty plea, such as offering restitution to the victim of a

[317] Note that a judge can only make a confiscation order after a conviction has been secured.
[318] O Joseph, *'Why encourage plea bargaining?'* (http://www.punchng.com, 2nd September 2012) http://www.punchng.com/opinion/letters/why-encourage-plea-bargaining/ Accessed 3rd July 2014.
[319] A Alschuler, '*Plea Bargaining and its History*' 1979, 79 Columbia Law Review 1, 3.
[320] Ibid

crime, giving information or testimony concerning other alleged offenders, or resigning from public office following allegations of misconduct.[321]

Black's Law Dictionary defines plea bargain as follows:

A negotiated agreement between a prosecutor and a criminal defendant whereby the defendant pleads guilty to a lesser offence or to one of multiple charges in exchange for some concession by the prosecutor[322]

9.2 HISTORY OF PLEA BARGAINING

The plea bargain was a prosecutorial tool used only episodically before the 19th century. "In America," Fisher says, "it can be traced almost to the very emergence of public prosecution -- and public prosecution, although not exclusive to the United States., developed earlier and more broadly in the United States than in most places."

Below is a summary of the history of plea bargaining from the 16th century to the 19th century

1633: Galileo gets house arrest from the Inquisition in exchange for his reciting penitential psalms weekly and recanting Copernican heresies.

1931: Al Capone brags about his light sentence for pleading guilty to tax evasion and Prohibition violations. The judge then declares that he isn't bound by the bargain, and Capone does seven and a half years in Alcatraz.

[321] A Alschuler, '*Plea Bargaining and its History*' 1979, 79 Columbia Law Review 1, 4.
[322] B A. Garner, *Black's Law Dictionary* (8th Edition West, a Thomson business 2004) 1190.

1969: To avoid execution, James Earl Ray pleads guilty to assassinating Martin Luther King Jr. and gets 99 years.

1973: Spiro Agnew resigns the vice presidency and pleads no contest to the charge of failing to report income; he gets three years' probation and a ten thousand dollars fine (roughly one-third of the amount at issue).

1990: Facing serious federal charges of insider trading, Michael Milken pleads to lesser charges of securities fraud; soon after, his 10-year sentence is reduced to 2 years.[323]

9.3 THE NATURE OF PLEA BARGAINING

There are two basic types of plea bargaining: charge bargain and sentence bargain. In the case of charge bargain, it is arranged in a way that the prosecutor agrees to drop some of the counts or reduce the charge to a less serious offence in exchange for a plea of either guilty or no contest from the defendant.

In the case of sentence bargain, the prosecutor agrees to recommend a lighter sentence in exchange for a plea of either guilty or no contest from the defendant.[324]

9.4 DISCUSSION

The previous sections defined plea bargaining and discussed the history and nature of plea bargaining.

[323] D Olin, '*The Way We Live Now: 9-29-02: Crash Course; Plea Bargain'* (http://www.nytimes.com 29th September 2002) http://www.nytimes.com/2002/09/29/magazine/the-way-we-live-now-9-29-02-crash-course-plea-bargain.html Accessed 3rd July 2014.
[324] B A. Garner, *Black's Law Dictionary* (8th Edition West, a Thomson business 2004) 1190.

This section compares the approach to plea bargaining in Nigeria with those of the United States and the United Kingdom. The aim of this comparison is to determine what the best approach is, which is the one that achieves the highest number of convictions without necessarily interfering with a person's right to a jury trial.

9.4.1 NIGERIA

The practice of plea bargaining is obviously very embryonic in Nigeria. It was never part of any Nigerian law until 2002 when the **Economic and Financial Crimes Commission (the Commission)** was established. Looking at a plethora of statutory provisions in Nigeria, the author has no hesitation in asserting that the first federal enactment to experiment with a form of plea bargaining is the **Economic and Financial Crimes Commission (Establishment) Act (EFCC Act)**.[325]

The provision of **Section 14 (2) of the EFCC Act** indicates that when a defendant agrees to give up money stolen by him; the Commission may compound any offence for which such a person is charged under the Act. This provision has no universal application to all criminal trials in Nigeria as negotiations there under are expressly limited to offences punishable under the EFCC Act.

Sections 14-18 of the EFCC Act provides for crimes for which the Commission can exercise jurisdiction. These includes: offences relating to financial malpractices, offences in relation to terrorism, offences relating to public officers' retention of proceeds of criminal conduct and offences in relation to economic and financial crimes.

The statutory blessing given to plea bargaining in Nigeria is not limited to the EFCC Act. In fact, the most commendable step in giving statutory back up to plea bargain in Nigeria

[325] Economic and Financial Crimes Commission (Establishment) Act 2004, s. 1.

is the enactment of the **Administration of Criminal Justice Law 2011, Laws of Lagos State,** which institutionalized plea bargain in Lagos State. For the purpose of proper understanding and appreciation of the position in Lagos, this research will reproduce the relevant sections of the aforementioned law:

76(1) The prosecutor and a defendant or his legal practitioner may before the plea to the charge, enter into an agreement in respect of:

(a) a plea of guilty by the defendant to the offence charged or a lesser offence of which he may be convicted on the charge, and

(b) an appropriate sentence to be imposed by the Court if the defendant is convicted of the offence to which he intends to plead guilty.

(2) The prosecutor may only enter into an agreement contemplated in subsection (1) of this Section: (a) after consultation with the Police Officer responsible for the investigation of the case and if reasonably feasible, the victim, and

(b) with due regard to the nature of and circumstances relating to the offence, the defendant and the interest of the community.

(3) The prosecutor, if reasonably feasible shall afford the complainant or his representative the opportunity to make representations to the prosecutor regarding

(a) the contents of the agreement; and

(b) the inclusion in the agreement of a compensation or restitution order.

(4) An agreement between the parties contemplated in subsection (1) shall be reduced to writing and shall:

(a) state that, before conclusion of the agreement, the defendant has been informed (i) that he has a right to remain silent; (ii) of the consequences of not remaining silent; (iii) that he is not obliged to make any confession or admission that could be used in evidence against him.

(b) state fully the terms of the agreement and any admissions made and,

(c) be signed by the prosecutor, the defendant, the legal practitioner and the interpreter as the case may be.

(5) The Presiding Judge, or Magistrate before whom criminal proceedings are pending shall not participate in the discussions contemplated in subsection (1). Provided that he may be approached by Counsel regarding the contents of the discussions and he may inform them in general terms of the possible advantages of discussions, possible sentencing options or the acceptability of a proposed agreement.

(6) Where a plea agreement is reached by the prosecution and defence, the prosecutor shall inform the court that the parties have reached an agreement and the Presiding Judge or Magistrate shall then inquire from the defendant to confirm the correctness of the agreement.

(7) The Presiding Judge or Magistrate shall ascertain whether the defendant admits the allegations in the charge to which he has pleaded guilty and whether he entered into the agreement voluntarily and without undue influence and may:

(a) if satisfied that the defendant is guilty of the offence to which he has pleaded guilty, convict the defendant on his plea of guilty to that offence, or;

(b) if he is for any reason of the opinion that the defendant cannot be convicted of the offence in respect of which the agreement was reached and to which the defendant has pleaded guilty or that the agreement is in conflict with the defendant's rights referred to in subsection (4) of this Section, he shall record a plea of not guilty in respect of such charge and order that the trial proceed.

(8) Where a defendant has been convicted in terms of subsection (7) (a), the Presiding Judge or Magistrate shall consider the sentence agreed upon in the agreement and if he is:

(a) satisfied that such sentence is an appropriate sentence impose the sentence, or:

(b) of the view that he would have imposed a lesser sentence than the sentence agreed upon in the agreement impose the lesser sentence; or

(c) of the view that the offence requires a heavier sentence than the sentence agreed upon in the agreement, he shall inform the defendant of such heavier sentence he considers to be appropriate.

(9) Where the defendant has been informed of the heavier sentence as contemplated in subsection (8) above, the defendant may:

(a) abide by his plea of guilty as agreed upon in the agreement and agree that, subject to the defendant's right to lead evidence and to present argument relevant to sentencing, the Presiding Judge, or Magistrate proceed with the sentencing; or

(b) withdraw from his plea agreement, in which event the trial shall proceed de novo before another Presiding Judge, or Magistrate, as the case maybe.

(10) Where a trial proceeds as contemplated under subsection (9) (a) or de novo before another Presiding Judge, or Magistrate as contemplated in subsection (9) (b):

(a) no reference shall be made to the agreement;

(b) no admissions contained therein or statements relating thereto shall be admissible against the defendant; and

(c) the prosecutor and the defendant may not enter into a similar plea and sentence agreement.

Plea bargaining has secured convictions in high-profile cases, including Federal Republic of Nigeria v. Cecilia Ibru, Federal Republic of Nigeria v. Alamieyeseigha, Federal Republic of Nigeria v. Tafa Balogun and Federal Republic of Nigeria v. Lucky Igbinedion.

In the case of Federal Republic of Nigeria v. Cecilia Ibru, the commission had charged Mrs Cecilia Ibru with a twenty-five-count criminal information offence bordering on financial crimes before the court. However, she entered into a plea bargain with the prosecution and pleaded guilty to a lesser three-count charge. The court thereafter convicted Ibru on the three-count charge and ordered the forfeiture of her assets, which amounted to about one hundred and ninety-one billion naira. She was sentenced to six months in prison for each of the three counts, to be served concurrently. In effect, Ibru was expected to spend only six months in jail.[326]

[326] K. Oladele, *'Plea bargaining and the criminal justice system in Nigeria'* (http://www.vanguardngr.com October 14, 2010) http://www.vanguardngr.com/2010/10/plea-bargaining-and-the-criminal-justice-system-in-nigeria/, accessed July 4, 2014.

Another plea bargain under the EFCC Act was the former governor of Bayelsa State, Alamieyeseigha, who stood trial on a thirty-three-count charge of corruption, money laundering, illegal acquisition of property and false declaration of assets. He pleaded guilty to a six-count charge of money laundering brought by the commission and forfeited properties worth billions of naira in exchange for the lesser sentence. The former governor entered into a plea bargain with the commission, gave up his right to a trial and pleaded guilty to the charges. Rather than serving a prolonged prison term if convicted, he accepted the commission's offer for a guilty plea. However, because he had completed almost two years in jail before accepting the bargain, he was released a few days after his conviction.[327]

Other beneficiaries of plea bargains in Nigeria include Tafa Balogun, the former inspector general of police and Mr Lucky Igbinedion, the former governor of Edo State.[328]

As shown in the cases cited, plea bargaining has proven useful in Nigeria's criminal justice system by saving time and avoiding the necessity of public trials, thereby protecting innocent victims of crime from the ordeal of giving evidence during trials. The use of plea bargaining in these cases has yielded fruits, one of which was the reduction of public expenditure that would have been incurred during prolonged trials.

If the cases had gone to full trial, there would have been an unacceptable waste of state resources as trials are so costly. Lawyers are paid appearance fees each time they appear in court for a case. The commission usually hires the services of senior advocates of Nigeria, so one can imagine how much money would have been spent if

[327] Ibid.
[328] Ibid.

these cases had gone to full trial. So, we can appreciate Tafa Balogun and the rest who chose to accept the plea bargains.

This has also helped decongest prisons. Overcrowding in Nigeria's prisons is no longer news. The prisons have poor sanitary systems, and they rarely have facilities; where facilities do exist, they are dilapidated and unhygienic.

Despite the advantages noted above, the concept of plea bargaining has been criticized by a number of people. The most notable among them is the former chief justice of Nigeria (CJN), Justice Dahiru Musdapher, who was reported to have criticized the commission for smuggling the plea bargain concept into Nigerian criminal jurisprudence and also said that the concept had 'dubious' origins. The former CJN explained that he meant that the concept had a dubious origin in Nigeria.

> *When I described the concept of 'dubious origin', I was not referring to the original raison d'être or the juridical motive behind its conception way back, either in the United States or in England in the early nineteenth century; I was referring to the sneaky motive behind its introduction into our legal system, or its evident fraudulent application. You will learn that plea bargain is not only 'condemnation without adjudication', as John Langbien decried it; it is, as some other critics say, 'a triumph of administrative and organizational interests over justice'. At its very best, it penalizes the innocent who may be tempted to plead guilty to avoid being actuated by judicial default, and, at its most obnoxious extent, it grants 'undue leniency' as reward to criminals simply for pleading their guilt. You will see also that plea bargain is not only a flagrant subordination of the public's interest to the interest of 'criminal justice administration', but, worst of all, the concept*

generally promotes a cynical view of the entire legal system. I have said that our wavering disposition on the ethical standards set by your noble profession guarantees or jeopardizes our peace, security and progress. And it is the reason that I have chosen this occasion to speak—with all sense of solemnity—on a matter that has continued to eat away at even the modest gains that we seem to be making in reforming both the infrastructure and the overall judicial template of the Nigerian Judiciary.[329]

The commission did not smuggle the concept into Nigeria. The lawmakers carved laws around the concept of plea bargaining, and the commission capitalized on those provisions to the country's advantage by applying them to the cases they were dealing with for the benefit of Nigeria and Nigerians.

The concept of plea bargaining did not have a 'dubious' origin in the sense that there was not a sneaky motive behind its introduction into Nigeria's legal system, nor was its application fraudulent. This is a new age in which alternative dispute resolutions are taking the place of litigation. Plea bargaining is like the alternative dispute resolution that is used in a civil trial. It saves the court time and money.

Plea bargaining does, however, penalize the innocent who may be tempted to plead guilty. Prosecutors could try to intimidate defendants by drawing up countless numbers of charges, thus forcing innocent defendants to submit to the plea bargain offers, which is complete injustice. This can be avoided if the defendants become more enlightened about the bag of tricks the prosecutors could attempt to play on them.

---

[329]D. A. Akintimoye, *'Should plea bargaining be abolished or encouraged in Nigeria?'* (http://community.vanguardngr.com March 7, 2012) http://community.vanguardngr.com/profiles/blogs/should-plea-bargaining-be-abolished-or-encouraged-in-nigeria, accessed January 2, 2014.

9.4.2 UNITED STATES

The **Federal Rules of Criminal Procedure 2010,** and in specific, **Rule 11 (c),** recognizes and codifies the concept of plea agreements in the United States.

One recent estimate indicated that guilty pleas account for the disposition of as many as 95% of all criminal cases in United States. A substantial number of these are the result of plea discussions.[330]

While some scholars have interpreted the above statistics to mean that the process of plea bargaining is been abused in the American Criminal Justice System.[331] The statistics could be interpreted to mean that the concept of plea bargaining has been properly administered in the United States.

The basis for such interpretation lies in **subdivision (c) Rule 11** of the **U.S. Federal Rules of Criminal Procedure 2010.**

The procedure described in subdivision (c) is designed to prevent abuse of plea discussions and agreements by providing appropriate and adequate safeguards.

Subdivision (c) (1) specifies that the "attorney for the government and the attorney for the defendant or the defendant when acting pro se may" participate in plea discussions. The inclusion of "the defendant when acting pro se" is intended to reflect the fact that there are situations in which a defendant insists upon representing himself. It may be desirable that an attorney for the government not enter plea discussions with a

[330] G Fields and J R. Emshwiller, *'Federal Guilty Pleas, Soar As Bargains Trump Trials'* (http://online.wsj.com 23rd September 2012) http://online.wsj.com/news/articles/SB10000872396390443589304577637610097206808 Accessed 7th October 2014.

[331] T Lynch, '*The Case against Plea Bargaining*' (Regulation Fall 2003) 24

defendant personally. If necessary, counsel can be appointed for purposes of plea discussions. **Subdivision (b) (2)** makes it mandatory that the court inquire of the defendant whether his plea is the result of plea discussions between him and the attorney for the government. This is intended to enable the court to reject an agreement reached by an unrepresented defendant unless the court is satisfied that acceptance of the agreement adequately protects the rights of the defendant and the interests of justice.

Apparently, it is the practice of most prosecuting attorneys to enter plea discussions only with defendant's counsel. Discussions without benefit of counsel increase the likelihood that such discussions may be unfair. Some courts have indicated that plea discussions in the absence of defendant's attorney may be constitutionally prohibited.[332]

Subdivision (c) (2) provides that the judge shall require the disclosure of any plea agreement in open court.

Upon notice of the plea agreement, the court is given the option to accept or reject the agreement or defer its decision until receipt of the presentence report.

The judge may, and often should, defer his decision until he examines the presentence report. This is made possible by rule 32 which allows a judge, with the defendant's consent, to inspect a presentence report to determine whether a plea agreement should be accepted.

[332] See Anderson v. North Carolina, 221 F.Supp. 930, 935 (W.D.N.C.1963); Shape v. Sigler, 230 F.Supp. 601, 606 (D.Neb. 1964).

The plea agreement procedure does not attempt to define the criteria for the acceptance or rejection of a plea agreement. Such a decision is left to the discretion of the individual trial judge.

Subdivision (c)(4) makes is mandatory, if the court decides to accept the plea agreement, that it inform the defendant that it will embody in the judgment and sentence the disposition provided in the plea agreement, or one more favourable to the defendant. This serves the purpose of informing the defendant immediately that the agreement will be implemented.

Subdivision (c)(5) requires the court, if it rejects the plea agreement, to inform the defendant of this fact and to advise the defendant personally, in open court, that the court is not bound by the plea agreement. The defendant must be afforded an opportunity to withdraw his plea and must be advised that if he persists in his guilty plea or plea of nolo contendere, the disposition of the case may be less favourable to him than that contemplated by the plea agreement.

If the court rejects the plea agreement and affords the defendant the opportunity to withdraw the plea, the court is not precluded from accepting a guilty plea from the same defendant at a later time, when such plea conforms to the requirements of rule 11.

In addition to Rule 11 (c) of the Federal Rules of Criminal Procedure, there are a number of cases decided by the U.S. Supreme Court on 21st March 2012, which support the above interpretation.

In the first case, **Missouri v. Frye,** defendant Galin Frye was charged with felony driving without a licence after several repeated offences. The State offered to reduce the charge to a misdemeanour with maximum jail time of one year in exchange for a guilty plea.

Although prosecutors communicated this offer to Mr. Frye's attorney, the attorney made no effort to relay the offer to his client. As a result, the offer expired without Mr. Frye ever knowing of its existence. Mr. Frye later pled guilty without any agreement with the State, and he was sentenced to three years in prison.

The Supreme Court held that Mr. Frye was entitled to the effective assistance of counsel during plea negotiations and that **Strickland v. Washington** provides the appropriate standard for evaluating such a claim. Consequently, a prisoner pursuing such a claim must prove both deficient performance and prejudice. Citing to a number of sources, including the **ABA Criminal Justice Standards,** the Court found that an attorney's failure to communicate a plea offer to his client may constitute deficient performance. While evaluating deficient performance in Mr. Frye's case, the Court noted that there was no evidence that any effort was made to communicate the offer or that Mr. Frye interfered in any way with the communication of the offer.

Having found deficient performance, the Court then analysed whether Mr. Frye was prejudiced by his attorney's actions. In order to prove prejudice, the Court held that Mr. Frye must show a "reasonable probability" that 1) he would have accepted the offer had it been made known to him; 2) acceptance of the offer would have resulted in a less severe sentence; 3) the state would not have withdrawn or changed the offer; and 4) the trial court would have sentenced him according to the agreement. Although the Court found that Mr. Frye had likely satisfied the first two requirements, it expressed serious doubts that the State would not have withdrawn the offer or that the trial court would not have rejected it. Writing for the majority, Justice Kennedy pointed out a number of considerations, such as the fact that Mr. Frye was charged with another instance of the same offence while the case was pending and that Missouri law allows a trial judge to disregard a plea agreement during sentencing. Ultimately the Court found that the issue

of prejudice in Mr. Frye's case turned on questions of state law and remanded the case for further proceedings.

A companion case, **Lafler v. Cooper,** was decided the same day as **Frye.** Anthony Cooper was charged by the state of Michigan with attempted murder for shooting a woman in her buttocks and leg. The prosecution offered a reduced sentence in exchange for a guilty plea, but Mr. Cooper's attorney advised him not to take it, erroneously instructing him that he could not be convicted of attempted murder because the victim was shot below the waist. Consequently, Mr. Cooper's case went to trial, where he was convicted and sentenced to a term 3.5 times longer than the sentence offered in the plea bargain. During state post-conviction proceedings, the court rejected the claim of ineffective assistance of counsel, its analysis turning on whether Mr. Cooper's rejection of the offer was voluntary. Mr. Cooper then filed a habeas petition with the federal district court, which applied the **Strickland** standard and found that he had been denied his Sixth Amendment right to counsel. The Sixth Circuit affirmed the district court's decision and ordered that Mr. Cooper be sentenced to the terms of the original plea offer.

The Supreme Court affirmed the Sixth Circuit's decision in part, holding that if a plea bargain is offered, a criminal defendant has a constitutional right to effective assistance of counsel in considering whether to accept that offer. It rejected the State's argument that a fair trial and sentencing by jury could correct the earlier constitutional error, noting that "the constitutional rights of criminal defendants . . . are granted to the innocent and the guilty alike." Again writing for the majority, Justice Kennedy limited his analysis to the question of prejudice and the appropriate remedy, because both parties conceded deficient performance.

Examining the same factors discussed in **Frye,** the Court agreed with the Sixth Circuit, finding Mr. Cooper had satisfied the prejudice prong of **Strickland**. The Court found that the Sixth Circuit erred, however, in determining the appropriate remedy. It held that, in this instance, the State should re-offer the plea bargain, and if accepted by the defendant, the trial court could then exercise its discretion in issuing a sentence. Justice Kennedy suggested that this discretion is very broad, indicating that the court may issue a sentence ranging anywhere from the terms of the plea agreement to the original sentence being challenged by the defendant. He declined to discuss the "boundaries of proper discretion," finding that this would be best informed by state law. The Court vacated the Sixth Circuit's judgment and remanded for further proceedings.

Both cases were decided by a 5-4 majority of the court, with Justice Scalia writing dissents in each case joined by Justices Thomas and Roberts, and Justice Alito dissenting separately in **Lafler.**[333]

9.4.3 UNITED KINGDOM

The concept of 'plea bargaining' traditionally has no legal standing in the law of England and Wales. However, informal 'discussions' between Counsel on both sides will often lead to an 'offer' by the defence to enter a plea of guilty to either a lesser count or to an agreed basis of plea.

Normally, the first occasion at which a defendant is required to enter a plea is at the Plea and Case Management Hearing in the Crown Court. The defendant may enter a guilty

[333] E M Williams, *'U.S. Supreme Court Recognizes Right to Effective Counsel in Plea Bargains'* (http://www.americanbar.org) http://www.americanbar.org/publications/project_press/2012/spring/plea_bargains.html Accessed 1st October 2014.

plea at the hearing, and may subsequently change his plea to guilty at any time before a trial commences or even during the trial process.

A plea of guilty must be entered voluntarily. If the accused is deprived of a genuine choice as to plea and in consequence purports to plead guilty, the plea is a nullity and the conviction can be quashed on appeal.[334]

The above procedure ensures that plea discussions are not being abused in the United Kingdom's Criminal Justice System.

Some recent developments have sought to formalise the process of plea bargaining in the United Kingdom. A 'Goodyear application' enables the accused to seek, and the Judge, if he feels it appropriate, to provide an indication of sentence. The following guidelines are given in **R v. Goodyear [2005] 1 WLR 2532:**

i. A Court should not give an indication of sentence unless one has been sought by the accused.
ii. The Court remains entitled to exercise the power to indicate that the sentence, or type of sentence, on the accused would be the same whether the case proceeds as a plea of guilty or goes to trial with a resulting conviction. The Court is also entitled to remind the defence advocate that the accused is entitled to seek an advance indication of sentence.
iii. Where an indication is sought, the Court may refuse altogether to give an indication, or may postpone doing so, with or without giving reasons.
iv. Where the Court has it in mind to defer an indication, the probability is that the Judge would explain his reasons, and further indicate the circumstances in

[334] The SFO Operational Handbook 2012.

which, and when he would be prepared to respond to a request for a sentence indication.

v. If the Court refuses to give an indication it remains open to the defence to make a further request for an indication at a later stage. The Court should not normally initiate the process, except where appropriate to indicate that the circumstances have changed sufficiently to permit a renewed application for an indication.

vi. Once an indication has been given, it is binding.

vii. If the accused does not plead guilty, the indication will cease to have effect.

viii. Where appropriate, there must be an agreed, written basis of plea, otherwise the Judge should refuse to give an indication.[335]

The process laid down in R v. Goodyear [2005] 1 WLR 2532 is somewhat similar to plea bargaining, but it is not plea bargaining.

There is no actual agreement between the judge and the defendants to reduce the sentence if the defendants plead guilty. Also, there is no actual agreement between the prosecutors and the defendants to reduce the number of charges if the defendants plead guilty.

The only agreement is for the judge to reveal the details of judgment before the prescribed time.

9.5 CONCLUSION

The concept of plea bargaining has not been abused in Nigeria, the United States or the United Kingdom. Rather, it has been utilized in a coordinated way and, in the process, has made a positive impact on the criminal justice system of these countries. Plea

[335] The SFO Operational Handbook 2012.

bargaining has saved time and state resources, and although it has its disadvantages, the advantages completely outweigh them.

The United States has secured the highest number of convictions compared to Nigeria and the United Kingdom.

Therefore, Nigeria and the United Kingdom are recommended to adopt the US approach.

CONCLUSION

This research compared the approaches adopted in Nigeria, the United States and the United Kingdom in relation to money laundering offences, customer due-diligence measures, politically exposed persons, cash couriers, record keeping, reporting requirements, compliance officers and confiscation measures.

This concluding chapter presents a summary of the findings and recommendations of this research. It will also expound on the additional strategies and controls that can strengthen Nigeria's anti-money laundering and countering the financing of terrorism (AML/CFT) measures to make it more effective.

A. FINDINGS

I. Money Laundering Offence: Application of the Single Criminality Test

The Nigerian approach appears to be in line with Article 2 (2) of the Vienna Convention, which mandates countries to carry out their obligations in a manner consistent with the principles of sovereign equality and territorial integrity of countries and that of nonintervention in the domestic affairs of other countries.

The US and UK approaches appear to be inconsistent with these principles. They both establish their jurisdictions over offences committed abroad, provided that the offence is a serious offence.

This approach is also inconsistent with Article 2 (3) of the Vienna Convention, which mandates that countries should not exercise jurisdiction and performance of functions in

the territory of another country that are exclusively reserved for the authorities of that other country by its domestic law.

II. Money Laundering Offence: Whistleblower Policy

The policy has been very successful in achieving its main objectives in Nigeria. Despite the benefits associated with the policy, there have been concerns about the increase in the number of blackmailers in the country. Financial incentives have led to more approaches from opportunists and uninformed parties passing on speculative rumours or public information. The reputations of innocent parties have been unfairly damaged as a result.

III. Customer Due Diligence: Meaning of Customer

The term ‘customer’ is not expressly defined in the Nigerian or UK Money Laundering Regulations as it is defined in the US Bank Secrecy Act/Anti–Money Laundering Examination Manual 2010. In view of this, the US approach is far better than the United Kingdom and the Nigerian approach, because it leaves no room for ambiguity.

IV. Customer Due Diligence: The Three-Tiered KYC Regime

Non-verification of customer information at the account opening stage may negatively impact on information sharing mechanisms. For example, a customer who successfully opened a low value account at Bank A may decide to open another low value account at Bank B, Bank C, Bank D and Bank E for the purpose of circumventing the threshold mechanism.

V. Customer Due Diligence: Transparency and Beneficial Ownership

Company registration documents kept by the Corporate Affairs Commission (CAC) are not dependable and current.

VI. Politically Exposed Persons: Enhanced Due Diligence

Financial institutions in Nigeria may encounter challenges gaining access to the asset details of public officers due to a May 11, 2020 judgment by Justice Muslim Hassan, which agreed with the Code of Conduct Bureau (CCB) that the duty to make the asset declaration form of public officers available depends on the terms and conditions to be prescribed by the National Assembly.

VII. Cash Couriers

The oral declaration system adopted in Nigeria does not appear to be working as effectively as it is in the United Kingdom. This could be because the so-called system has not curtailed the movement of criminal property by the deadly terrorist group Boko Haram.

VIII Record Keeping

A risk-based approach to record-keeping requirements is the preferable approach. A risk-based approach is designed to make it more difficult for money launderers and terrorist organizations to make use of financial institutions due to the increased focus on the identified higher-risk activities that are undertaken by these criminal elements.

IX. Reporting Requirements

The ‘no threshold rule’ for reporting suspicious transactions is preferable.

The tipping-off provision, as currently drafted, could cause serious problems for financial institutions and designated nonfinancial institutions. First, it is not clear if a disclosure by a financial institution to law enforcement agents is permitted. Second, it is not clear if a disclosure by a financial institution to another financial institution is permitted. Third, it is not clear if a disclosure by a professional legal adviser to another professional legal adviser is permitted. All these disclosures are stated in both the UK and US laws as clear exceptions to the general rule of tipping off.

X. Compliance Officers

Despite the advantages of the fit and proper test for Compliance Officers, there have been damning reports that some politicians are using fraudsters working in banks to launder public funds. According to the Economic and Financial Crimes Commission, fraudsters have been aiding politically exposed and other persons to commit various financial crimes. This revelation epitomises systemic failure aggravated by the Central Bank of Nigeria's weak regulation.

The United Kingdom's approach allows for the responsibilities conferred on compliance officers by the Financial Action Task Force to be shared between two people, thereby reducing the burden of work on the compliance officers. This is not the approach adopted by Nigeria and the United States. However, compliance officers in Nigeria and the United States could delegate some of their duties to other competent individuals.

XI. Plea Bargaining

The concept of plea bargaining has not been abused in Nigeria, the United States or the United Kingdom. Rather, it has been utilized in a coordinated way and, in the process, has made a positive impact on the criminal justice system of these countries. Plea

bargaining has saved time and state resources, and although it has its disadvantages, the advantages completely outweigh them.

The United States has secured the highest number of convictions compared to Nigeria and the United Kingdom.

B. RECOMMENDATIONS

I. Money Laundering Offence

i. The Nigerian Money Laundering (Prevention and Prohibition) Act, 2022 should be amended to include the single criminality test, even if it is already included in the Nigerian Criminal Code Act.

ii. A Police Officer who receives information from a whistleblower about money hidden in an apartment should apply to a Court or Justice of the Peace within the local limits of whose jurisdiction he is for the issue of a search warrant before conducting a search on the said premises. This procedure is in line with **Section 143 of the Administration of Criminal Justice Act 2015 and the Court of Appeal decision in Hassan v. E.F.C.C. (2014) I NWLR (Pt. 1389) 607 at 625.**

iii. The **Public Interest Disclosure and Witness Protection Bill, 2017** should be given accelerated consideration in the House of Representatives based on its urgency and significance for the Federal Executive Council's whistleblowers Policy.

II. Customer Due Diligence

i. Nigeria and the United Kingdom should amend their money laundering laws by defining who a customer is.

ii. The Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013 should be amended to prohibit financial institutions from opening more than one low value account for Mobile Money wallet holders. In other words, financial institutions should be mandated to verify whether a customer already holds an account with another bank before opening a low value account, and in a situation where the bank determines that a customer does hold a payment account with another credit institution, the bank should not open a basic account for that customer. Verification can be done by mandating all bank customers to provide their Bank Verification Number before an account can be opened. This is the approach being adopted by the United Kingdom's Payment Accounts Regulations 2015. This approach will positively impact on account monitoring procedures; customer identification and verification will reduce the risk of impersonation fraud and identity theft while still promoting financial inclusion.

iii. The Corporate Affairs Commission should maintain timely, adequate, accurate and up-to-date Beneficial Ownership information. The Corporate Affairs Commission should have a policy of inquiring/prohibiting or otherwise becoming aware of foreign companies that are shareholders in local companies and that have issued bearer shares. This policy is particularly relevant for identifying the ultimate beneficial ownership of local companies which can impede effective law enforcement investigations involving foreign companies.

iv. The Corporate Affairs Commission should have a strong monitoring and sanctioning regime. According to GIABA's Second Mutual Evaluation Report on Nigeria, Existing monetary sanctions are not dissuasive enough to guarantee compliance to make disclosures, including the beneficial ownership of foreign partners and shareholders.

III. Politically Exposed Persons

i. The Nigerian National Assembly should enact a law empowering the Code of Conduct Bureau to release to the public details of declared assets by public officers.

IV. Cash Couriers

i. The Central Bank of Nigeria should permanently stop producing the one thousand naira and five-hundred-naira banknotes and exclude it from circulation, taking into account concerns that these banknotes could facilitate illicit activities. This is in line with the decision and approach of the European Central Bank to permanently stop producing the €500 banknote and to exclude it from the Europa series, taking into account concerns that this banknote could facilitate illicit activities.[336]

ii. The Economic and Financial Crimes Commission should direct banks in Nigeria to monitor the bank accounts of customs and immigration officers who are stationed at the land borders for potential signs of corruption and money laundering.[337] Due diligence and account monitoring procedures should be performed on these accounts under the supervision of the AML/CFT Chief Compliance Officer.[338]

iii. The Nigeria Custom Service and Immigration Service should have a policy that mandates that the lie detector test should be taken once in 5 years by all staff of

[336] European Central Bank, 'ECB ends production and issuance of €500 banknote', (https://www.ecb.europa.eu May 4, 2016) Available at: https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html (accessed 5 July 2022).
[337] Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 38(1).
[338] Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013, Regulation 38(3).

the organization. For Staff who are positioned at the land borders, the lie detector test should be taken every three years. This will enable the lie detector policy to be more effective. Let us take for example, a person passes the lie detector test genuinely without any influence of corruption; there is still a possibility that the person may change over time. The temptation to follow current employees to collect bribes is very high. But if the organization put a policy in place that mandates every Personnel to take the lie detector test every five years starting from the first five years after recruitment, the cankerworm called corruption may be curbed effectively. Imagine if every employee knew that they were going to be asked by an examiner, 5 years after working, to confirm if they ever collected bribe during the time they worked in the institution, most employees will desist from taking bribes or engaging in corrupt acts. The above measure will ensure that current employees who are chosen as examiners for the lie detector tests are fit and proper persons for the job.

V. Record Keeping

Countries should not be allowed to stipulate a minimum time frame for financial institutions to maintain records. Rather, the period should depend on whether or not the customer is high risk.

For customers who have been designated as higher risk by a firm, financial institutions should be allowed to keep records of information obtained through CDD measures for ten years or more. For customers designated as lower risk, financial institutions should be allowed to keep records of information obtained through CDD measures for as little as two years.

VI. Reporting Requirements

i. Sections three and eleven of MLPA 2022 should be deleted, and section seven should remain intact. In other words, firms should be required to file only STRs and should no longer be required to file CTRs.

ii. Section 19 (1) (a) of MLPA 2022 and Regulation 31 (6) of CBN (Anti–Money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria) Regulations 2013 should be amended to include exceptions to the general rule of tipping off, as stated in the US Codified Bank Secrecy Act Regulations 2010.[339] Alternatively, the exceptions could be added to Section 333B, 333D (1) and (2) and 333D (3) of the United Kingdom's Proceeds of Crime Act 2002 (as amended).

VII. Compliance Officers

The Central Bank of Nigeria should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the **Financial Action Task Force (FATF) Recommendations**. Available evidence suggests that the Economic and Financial Crimes Commission has recovered more than two trillion dollars in 12 years, as of February 2016. The money passed through the banks; much of it ended up in safe havens in Europe and other parts of the world. But delinquent banks pay a heavy price abroad when caught in such a labyrinth.[340] For instance, the Financial Crimes Enforcement Network (FinCEN), in coordination with the Office of the Comptroller of the Currency, and the United States Department of Justice, had on

[339] Codified Bank Secrecy Act Regulations (2010), s. 1020.320 (e) (1) (A) (1), s. 1022.320 (d) (1) (A) (1), s. 1020.320 (e) (1) (A) (2), s. 1022.320 (d) (1) (A) (2), s. 1020.320 (e) (1) (B), s. 1022.320 (d) (1) (B).
[340] The Punch, 'Court BVN ruling: Saving genuine account owners', (http://punchng.com/ 3 November 2017), Available at: http://punchng.com/court-bvn-ruling-saving-genuine-account-owners/ (accessed 8 April 2018).

February 15, 2018, assessed a one hundred and eighty five million dollars civil money penalty against U.S. Bank National Association for willful violations of several provisions of the Bank Secrecy Act (BSA).[341] The Central Bank of Nigeria is strongly advised to enforce its regulations and punish errant banks/telecommunications companies so as to discourage their serial abuse of guidelines for the financial sector. This approach will strengthen Know Your Customer policies, aimed at reducing fraud and money laundering. **This measure is in line with the Financial Action Task Force Recommendations (Recommendation 26).**

VIII. Plea Bargaining

i. The concept of plea bargaining has not been abused in Nigeria, the United States or the United Kingdom. Rather, it has been utilized in a coordinated way and, in the process, has made a positive impact on the criminal justice system of these countries. Plea bargaining has saved time and state resources, and although it has its disadvantages, the advantages completely outweigh them.

ii. The United States has secured the highest number of convictions compared to Nigeria and the United Kingdom.

iii. Therefore, Nigeria and the United Kingdom are recommended to adopt the US approach.

[341] Financial Crimes Enforcement Network, 'FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws', (https://www.fincen.gov/ 15 February 2018), Available at: https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering (accessed 9 April 2018).

C. ADDITIONAL MEASURES TO MITIGATE MONEY LAUNDERING AND TERRORIST FINANCING RISKS

While Chapters 2 to 9 were able to thoroughly address research questions 1 and 2 as stated in the introduction, the section will address research question 3.

I. ARTIFICIAL INTELLIGENCE

Financial institutions must ensure that their Know Your Customer (KYC)' application programming interfaces (APIs) are powered by machine learning algorithms. Machine learning refers to the ability for software to learn and to become more accurate in its outcomes. Machine learning technology can take in large amount of data from public sources and connect it to customer information.

Machine learning can be used to analyze API's dataflows. Once the information has been digested, the machine learning algorithms will match the information to each entity and look for any anomalies within the data that needs to be corrected. In using the KYC API and machine learning technology to verify a customer's identity, Banks should ensure that they are able to demonstrate that they have both verified that the customer (or beneficial owner) exists, and satisfied themselves that the applicant seeking the business relationship is, in fact, that customer (or beneficial owner).

Banks should ensure that they have strong automated monitoring systems powered by machine learning algorithms that can detect highly suspicious transaction patterns including possible layering schemes through shell companies, and transactions not commensurate with the business's purpose. Dealers in precious metals, precious stones, or jewels planning to launder illicit funds could use shell companies to mask the beneficial ownership of account assets and this can make the tracking of funds

movements more difficult for law enforcement and tax officials. Banks must develop sufficient policies and procedures to address the AML risks associated with providing financial services to shell companies, including the potential for straw ownership and risks related to the commingling of funds. Banks must have adequate procedures for detecting red flags relating to certain transfers of funds among accounts at the Bank. The Bank must have a mechanism to detect large money movements with little to no securities trading, a commonly known red flag for potential money laundering in brokerage accounts. The Bank must deal appropriately with this particular category of customers that are using securities-related accounts for the movement of funds.

II. INDEPENDENT TESTING

Banks are required to conduct an independent compliance testing commensurate with the AML risk profile of the Bank to monitor and maintain an adequate program.[342] By not conducting the required independent review, Banks will be unable to identify vulnerabilities in its compliance program and properly monitor the account activity of its customers to detect suspicious activity going through the Bank.

Independent testing of the Bank's AML program should be conducted annually, unless the Bank does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts, in which case, independent testing must be conducted biennially.

Where a Bank configures its automated transaction monitoring system to generate a certain number of alerts each month, the Bank should conduct "below-threshold" testing to evaluate the extent to which the limits placed on alerts for

[342] 31 U.S.C. § 5318(h)(1)(D); 31 C.F.R. § 1020.210; Nigerian Money Laundering (Prevention and Prohibition) Act 2022, s. 10 (1) (d).

Queries is making the Bank to fail to investigate and file SARs on suspicious activity. The below-threshold test involves selecting a sample of alerts that occurred immediately below the alert limits to determine whether the limits should be adjusted to capture suspicious activity that occurred below the threshold. Where the below-threshold" testing reveals that the Bank's suppression of a substantial number of alerts prevented the Bank from investigating and reporting suspicious activity, the Bank should address the numerical caps by adjusting the limits to capture suspicious activity that occurred below the threshold and hiring more employees and investigators in its AML department.

III. TRAINING

A bank's AML program must provide for education and training of personnel regarding its responsibilities under the program, including the detection of suspicious transactions.[343] A bank's training program must provide Compliance staff with adequate job-specific training. The Bank's training program should not only focus on general AML requirements but also include topics on risks specific to the Bank.

Banks should combine focused class room training with on-line learning systems to deliver training. A one size fits all approach may not be the best since there will be classes of employees for whom the on-line learning system is not suitable.

D. CONCLUSION

In conclusion, Nigeria should implement the proposed reforms based on an appropriate assessment of their money laundering and terrorist financing risks with artificial

[343] 31 U.S.C. § 5318(h)(1)(C); 31 C.F.R. § 1020.210; Nigerian Money Laundering (Prevention and Prohibition) Act 2022, s. 10 (1) (b).

intelligence enabled systems. These measures will protect the financial system against money launderers and terrorist financiers, and reduce the risk of money laundering and terrorist financing to the barest minimum. The mechanisms/measures which have been extensively discussed in this research thesis with the proposed reforms will help financial institutions to identify, assess and understand their money laundering and terrorist financing risks, and take commensurate measures in order to mitigate them.

APPENDIX 1

GLOSSARY OF TERMINOLOGY

Confiscation

The term *confiscation,* which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

Currency

Currency refers to banknotes and coins that are in circulation as a medium of exchange.

Designated nonfinancial businesses and professions

Designated non-financial businesses and professions means:

a) Casinos.

b) Real estate agents.

c) Dealers in precious metals.

d) Dealers in precious stones.

e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.

f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

Financial institutions

Financial institutions mean any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.

2. Lending.

3. Financial leasing.

4. Money or value transfer services.

5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).

6. Financial guarantees and commitments.

7. Trading in:

(a) money market instruments (cheques, bills, certificates of deposit, derivatives etc.);

(b) foreign exchange;

(c) exchange, interest rate and index instruments;

(d) transferable securities;

(e) commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.

9. Individual and collective portfolio management.

10. Safekeeping and administration of cash or liquid securities on behalf of other persons.

11. Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance.

13. Money and currency changing.

Money Service Business

Money Service Business includes currency dealers, money transmitters, cheque cashers, and issuers of travellers' cheques, money orders or stored value.

Smurfing

Smurfing is the act of breaking down a transaction into smaller transactions to avoid regulatory requirements or an investigation by the authorities.

Terrorist

The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts ; (iii) organises or directs others to commit terrorist acts ; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terrorist act

A *terrorist act* includes:

(a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

APPENDIX 2

BIBLIOGRAPHY

BOOKS

Akehurst M, A Modern Introduction to International Law (5th Edition, George Allen and Unwin (Publishers) Ltd 1984).

Alldridge P Money Laundering Law, Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the proceeds of crime. (Hart Publishing 2003).

Ellinger E.P, MODERN BANKING LAW (5TH Edition, Oxford University Press 2011).

Elliott C and Quinn F, Contract Law (7th Edition Pearson Education Limited 2009).

Esoimeme, E.E., A Comparative Study of the Money Laundering Laws/Regulations in Nigeria, the United States and the United Kingdom', (Eric Press 2014).

Esoimeme, E.E., 'Deterring and Detecting Money Laundering and Terrorist Financing: A Comparative Analysis of Anti–Money Laundering and Counterterrorism Financing Strategies, (DSC Publications Ltd 2018).

Esoimeme, E.E., 'The Risk-Based Approach to Combating Money Laundering and Terrorist Financing', (Eric Press 2015).

Evans M D, International Law (3rd Edition Oxford University Press 2010).

Gardiner R K, International Law (First Published Pearson Education Ltd 2003).

Garner B.A, Black's Law Dictionary (8th Edition West, a Thomson business 2004).

Hopton D, MONEY LAUNDERING, A CONCISE GUIDE FOR ALL BUSINESS (2nd Edition, Ashgate Publishing Ltd 2007).

Horsey K and Rackley E, Tort Law (2nd Edition Oxford University Press 2011).

Jones, M A, Textbook on Torts (8th Edition Oxford University Press 2002).

Kalin W, Kunzli J 'The Law of International Human Rights Protection' (First Published, Oxford University Press 2009).

Kidner R, Casebook on Torts (12th Edition Oxford University Press 2012).

Lilley P, DIRTY DEALING THE UNTOLD TRUTH ABOUT GLOBAL MONEY LAUNDERING.

INTERNATIONAL CRIME AND TERRORISM (3rd Edition, Kogan Page Limited, 2006).

Loughman B P, Sibery R A, Bribery and Corruption, Navigating the global risks (John Wiley and Sons 2012).

Mathers C, Crime School: Money Laundering, True Crime meets the world of Business and finance (Firefly Books U.S Inc 2004).

Nwadialo F, S.A.N, The Criminal Procedure of the Southern States of Nigeria (2nd Edition MIJ Professional Publishers Limited 1987).

Odibei F F, Cases and Materials on Human Rights Law (1st Edition Pearl Publishers 2011).

Rehman J ‘International Human Rights Law’ (2nd Edition Pearson Education Limited 2010).

Reid K, ‘A Practitioners Guide to the European Convention on Human Rights’ (3rd Edition Sweet and Maxwell Ltd 2008).

Rehman J, International Human Rights Law (2nd Edition Pearson Education Limited 2010).

Schutter O D, International Human Rights Law (First Published Cambridge University Press 2010).

Shaw M.N, International Law (5th Edition Cambridge University Press 2003).

Umozurike U.O, Introduction to International Law (3rd Edition, Spectrum Books Limited, 2005).

ARTICLES

Aigbovo O: Nigerian anti-corruption statutes: an impact assessment 2013 16 (1) JMLC 62 – 78.

Alschuler A, ‘Plea Bargaining and its History’ 1979, 79 Columbia Law Review

Alldridge P, The UK Bribery Act, ‘The Caffeinated Younger Sibling of the FCPA’ 2012, 73 (5) Ohio State Journal, 1181 - 1216

Aaronberg D, Higgins N, All hail the Bribery Act-the toothless wonder 2011,6, Arch Rev 5-6.

Breslin B: The Bribery Act 2010: raising the bar above the US Foreign Corrupt Practices Act 2010, 31 (11) Comp Law. 362 – 369

Butcher C: Bribery Act proves hot topic for legal advisers.2011.25(25) Lawyers 7

Choo KKR, 'Politically exposed persons (PEPs): risk and mitigation 2008, 11 (4) JMLC, 371 – 387'

De Wit J: A risked based approach to AML 2007 15 (2) JFR and C 156 – 165

Drinnan R Australia: Proposed reform to Australian Foreign Bribery Legislation 2012,2, IELR, 40 -42

Garner B A, Black's Law Dictionary (8th Edition West, a Thomson business 2004)

Geary J, PEPs – Lets get serious. 2010 13(2) JMLC 103 – 108

Greenberg TS: Stolen Asset Recovery, Politically Exposed Persons, A policy paper on strengthening preventive measures

Lordi J A, The Uk Bribery Act: Endless Jurisdictional Liability on Corporate Violators 2012 Vol 44 Case W Res J Int LL,955.

Lynch T, 'The Case against Plea Bargaining' (Regulation Fall 2003) 24

Marshall P, Part 7 of the Proceeds of Crime Act 2002: double criminality, Legal Certainty, Proportionality and trouble ahead. 2003 11 (2) JFC 111-126

Marshall P, 'Part 7 of the Proceeds of Crime Act 2002: double criminality, legal certainty, proportionality and trouble ahead' 2003, 11 (2) JFC 111, 115 - 116.

Marshall P, 'Criminal Conduct Under Part 7 of the Proceeds of Crime Act 2002: A Requirement For Double Criminality'? (2003) 6 JIBFL 233

Marchini R: The new UK Bribery Act and data protection issues involving associated persons including suppliers and employees. 2011, 11 (8), WDPR 9 – 11

Nweze C, 'CBN laments skills gap of Compliance Officers' (http://thenationonlineng.net 29th May 2014) http://thenationonlineng.net/new/cbn-laments-skills-gap-compliance-officers/ Accessed 1st of October 2014

Otusanya OJ: 'The Role of offshore financial centres in elite money laundering practices: evidence from Nigeria. 2012,15(3) JMLC, 336 – 361'

Wells C: Bribery: Corporate Liability under the draft bill 2009.2009 7, Crim LR 479 – 487

Williams E M, 'U.S. Supreme Court Recognizes Right to Effective Counsel in Plea Bargains' (http://www.americanbar.org) http://www.americanbar.org/publications/project_press/2012/spring/plea_bargains.html Accessed 1st October 2014

Yeoh P: Bribery Act 2010: Implications for regulated firms (Legislative Comment) 2012 20 (3), JFR and C, 264 – 277

ELECTRONIC SOURCES

Adetayo, O., 'FG okays 5% of recovered loot for whistleblowers', (https://punchng.com 22 December 2016) Available at: http://punchng.com/fg-okays-5-recovered-loot-whistleblowers/ (accessed 6 June 2017).

Akinkuotu, E., 'EFCC recovers N17bn in four months', (https://punchng.com 23 April 2017) Available at: http://punchng.com/efcc-recovers-n17bn-in-four-months/ (accessed 6 June 2017).

Akinkuotu, E., 'EFCC recovers N449m in abandoned Lagos shop', (https://punchng.com 8 April 2017) Available at: http://punchng.com/efcc-recovers-n449m-in-abandoned-lagos-shop/ (accessed 6 June 2017).

Akinkuotu, E., 'How EFCC recovered $43m, £27,000, N23m during house raid', (https://punchng.com 13 April 2017), Available at: http://punchng.com/efcc-recovers-43m-27000-n23m-during-house-raid/ (accessed 5 June 2017).

Akintimoye D A, 'Should plea bargaining be abolished or encouraged in Nigeria?' (http://community.vanguardngr.com 7th March 2012) http://community.vanguardngr.com/profiles/blogs/should-plea-bargaining-be-abolished-or-encouraged-in-nigeria Accessed 2nd January 2014

Aon Plc (2013): http://www.aon.com/about-aon/about-aon.jsp Accessed on 20th May 2013

Barclays, 'Identification for bank accounts: What ID do I need to open a bank account?' (https://www.barclays.co.uk 2018), Available at: https://www.barclays.co.uk/current-accounts/what-do-i-need-to-open-a-bank-account/ (accessed 2 April 2018).

Basel Committee on Banking Supervision, 'About the Basel Committee' (http://www.bis.org 20th June 2014) http://www.bis.org/bcbs/about.htm Accessed 10th September 2014

Basel Institute on Governance, 'Basel AML Index 2021', (https://baselgovernance.org 2021), Available at: https://baselgovernance.org/publications/basel-aml-index-2021 (accessed 4 July 2022).

Central Bank of Nigeria, 'Circular to all Banks and other Financial Institutions: Introduction of Three-Tiered Know Your Customer (KYC) Requirements', (https://www.cbn.gov.ng 18 January 2013) Available at: https://www.cbn.gov.ng/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf (accessed 10 April 2018).

Central Bank of Nigeria, 'Circular to All Deposit Money Banks (DMBs)', (https://www.cbn.gov.ng/ 28 September 2016) Available at: https://www.cbn.gov.ng/out/2016/fprd/aml%20september%202016%20circular%20to%20banks%20on%20ccos%20(2).pdf (accessed 15 April, 2019).

Central Bank of Nigeria, 'Circular to Banks and Other Financial Institutions: Review of Restrictions and Limits on Levels I and II of the Tiered KYC Accounts', (https://www.cbn.gov.ng 1st July, 2016) Available at: https://www.cbn.gov.ng/out/2016/fprd/july%202016%20circular%20tkyc%20review.pdf (accessed 6 May 2019).

Central Bank of Nigeria, 'Circular to Banks, Discount Houses and Other Financial Institutions: Status and Reporting Line of Chief Compliance Officers', (https://www.cbn.gov.ng/ 17 November 2014) Available at: https://www.cbn.gov.ng/out/2014/fprd/status%20and%20reporting%20line%20of%20chief%20compliance%20officers.pdf (accessed 15 April, 2019).

Central Bank of Nigeria, 'Review of Daily Mobile Money Wallet Transaction and Balance Limit and Bank Verification Numbers (BVN) Requirement for Mobile Money Wallet Holders', (https://www.cbn.gov.ng 7 September 2017) Available at: https://www.cbn.gov.ng/out/2017/bpsd/review%20of%20daily%20mm%20wallet%20transaction%20&%20bvn%20requirement%20for%20mobile%20money%20wallet%20holders.pdf (accessed 6 May 2019).

Daily Lives and Corruption: Public Opinion in Southern Africa by Transparency International 2011: http://corruptionwatch.org.za/sites/default/files/ti_public_opinion_corruption_sa_111122.pdf Accessed 15th May 2013

Economic and Financial Crimes Commission, 'A Gender-based Foundation Seeks EFCC's Technology Assistance in Prosecution of Sex Offenders', (Available at: https://www.efccnigeria.org/ 2020) Available at: https://www.efccnigeria.org/efcc/news/6308-a-gender-based-foundation-seeks-efcc-s-technology-assistance-in-prosecution-of-sex-offenders (accessed 12 November 2021).

Economic and Financial Crimes Commission, 'N12.8 Million Fraud: EFCC Deploys Technology In Court', (https://www.efccnigeria.org 2019), Available at: https://www.efccnigeria.org/efcc/news/3981-n12-8-million-fraud-efcc-deploys-technology-in-court (accessed 12 November 2021).

European Central Bank, 'ECB ends production and issuance of €500 banknote', (https://www.ecb.europa.eu May 4, 2016) Available at: https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html (accessed 5 July 2022).

Financial Action Task Force, 'About us' (http://www.fatf-gafi.org) http://www.fatf-gafi.org/pages/aboutus/ Accessed 10th September 2014

Financial Conduct Authority, 'FCA fines and imposes a restriction on Canara Bank for anti-money laundering systems failings', (https://www.fca.org.uk 6 June 2018), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-and-imposes-restriction-canara-bank-anti-money-laundering-systems-failings (accessed 6 April 2019).

Financial Conduct Authority, 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings', (https://www.fca.org.uk 31 January 2017), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure (accessed 6 April 2019).

Financial Conduct Authority, 'FCA fines Goldman Sachs International £34.3 million for transaction reporting failures', (https://www.fca.org.uk/ 28 March 2019), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-goldman-sachs-international-transaction-reporting-failures (accessed 6 April 2019).

Financial Conduct Authority, 'FCA fines UBS AG £27.6 million for transaction reporting failures', (https://www.fca.org.uk 19 March 2019), Available at: https://www.fca.org.uk/news/press-releases/fca-fines-ubs-ag-276-million-transaction-reporting-failures (accessed 6 April 2019).

Financial Crimes Enforcement Network, 'FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws', (https://www.fincen.gov/ 15 February 2018), Available at: https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-national-association-violations-anti-money-laundering (accessed 9 April 2018).

Financial Crimes Enforcement Network, 'Enforcement Actions', (https://www.fincen.gov 2022), Available at https://www.fincen.gov/news-room/enforcement-actions (accessed 5 July 2022).

Financial Times, 'Overhaul of Companies House is long overdue', (https://www.ft.com 2021) Available at: https://www.ft.com/content/6fd92a72-e457-4d32-a5a5-c44ec2b76e20 (accessed 8 December 2021).

Growing Beyond: a place for integrity 12th Global Survey by Ernst and Young 2012: http://www.ey.com/Publication/vwLUAssets/Global-Fraud-Survey-a-place-for-integrity-12th-Global-Fraud-Survey/$FILE/EY-12th-GLOBAL-FRAUD-SURVEY.pdf Accessed 15th May 2013

Hebert Smith Asia's anti-corruption report issue 1 Summer 2012: https://www.icsaglobal.com/assets/files/AsiaanticorruptionreportIssue1.pdf Accessed 15th May 2013

HM Revenue and Customs, 'Going through customs' (http://www.hmrc.gov.uk) http://www.hmrc.gov.uk/customs/arriving/customs-channels.htm Accessed 7th September 2014

International Association of Insurance Supervisors, 'About the IAIS' (http://www.iaisweb.org) http://www.iaisweb.org/About-the-IAIS-28 Accessed 10th September 2014

International Monetary Fund, 'About the IMF' (http://www.imf.org) http://www.imf.org/external/about/ourwork.htm Accessed 10th September 2014

International Monetary Fund, 'Anti-Money Laundering/Combating the Financing of Terrorism' (https://www.imf.org) https://www.imf.org/external/np/leg/amlcft/eng/ Accessed 28th September 2014

International Monetary Fund, 'The IMF and the Fight Against Money Laundering and the Financing of Terrorism' (https://www.imf.org 5th September 2014) https://www.imf.org/external/np/exr/facts/aml.htm Accessed 28th September 2014

Joseph O, 'Why encourage plea bargaining?' (http://www.punchng.com, 2nd September 2012) http://www.punchng.com/opinion/letters/why-encourage-plea-bargaining/ Accessed 3rd July 2014

Montaldo C, 'The plea bargain stage of a criminal case, stages of the criminal justice system' (http://crime.about.com) http://crime.about.com/od/Crime_101/a/The-Plea-Bargain-Stage-Of-A-Criminal-Case.htm Accessed 4th July 2014

Nigeria Customs Service, 'Passenger's Concessions' (https://www.customs.gov.ng) https://www.customs.gov.ng/Stakeholders/passengers_concessions.php Accessed 7th September 2014

Okpare, O., 'Whistle-blowing: Blackmailers on the increase, says Uduaghan', (https://punchng.com 22 February 2017), Available at: http://punchng.com/whistle-blowing-blackmailers-increase-says-uduaghan/ (accessed 5 March 2017).

Oladele K, 'Plea bargaining and the criminal justice system in Nigeria' (http://www.vanguardngr.com 14th October 2010) http://www.vanguardngr.com/2010/10/plea-bargaining-and-the-criminal-justice-system-in-nigeria/ Accessed 4th July 2014

Olin D, 'The Way We Live Now: 9-29-02: Crash Course; Plea Bargain' (http://www.nytimes.com 29th September 2002) http://www.nytimes.com/2002/09/29/magazine/the-way-we-live-now-9-29-02-crash-course-plea-bargain.html Accessed 3rd July 2014

Premium Times, 'INVESTIGATION: Smuggling still rampant in Nigeria's northwestern boundaries despite border closure', (https://www.premiumtimesng.com/ 6 February 2020) Available at: https://www.premiumtimesng.com/investigationspecial-reports/375994-investigation-smuggling-still-rampant-in-nigerias-northwestern-boundaries-despite-border-closure.html (accessed 5 July 2022).

R L Cassin: Understanding the KBR Halliburton Charges (The FCPA Blog, 24th February 2009) http://fcpablog.squarespace.com/blog/2009/2/24/understanding-the-kbr-halliburton-charges.html Accessed 16th May 2013

Santander, 'Customer identification requirements for UK residents' (https://www.santander.co.uk/ 2018) Available at https://www.santander.co.uk/csdlvlr/BlobServer?blobtable=MungoBlobs&blobkey=id&blobcol=urldata&blobheader=application%2Fpdf&blobheadervalue1=inline%3Bfilename%3DCustomer+Identification+Requirements+do-ec-368.pdf&blobwhere=1314024309911&blobheadername1=Content-Disposition (accessed 3 April 2018).

Stewart P and Wroughton L 'How Boko Haram is beating U.S efforts to choke its financing' (http://www.reuters.com 1st July 2014) http://www.reuters.com/article/2014/07/01/us-usa-nigeria-bokoharam-insight-idUSKBN0F636920140701 Accessed 5th of August 2014

The Criminalisation of Bribery in Asia and the Pacific: Frameworks and Practices in 28 Asian and Pacific Jurisdictions. Thematic Review – Final Report by ADB/OECD Anti-Corruption initiative for Asia and the Pacific 2010: http://www.oecd.org/site/adboecdanti-corruptioninitiative/46485272.pdf Accessed 15th May 2013

The Daily Times, 'EFCC arraigns 2 whistleblowers over false information', (https://dailytimesng.com 17 May 2017) Available at: https://dailytimes.ng/news/efcc-arraigns-2-whistleblowers-false-information/ (accessed 10 June 2017).

The Guardian, 'Transparency in asset declaration regime still a long way ahead', (https://guardian.ng/ 15 September 2020), Available at: https://guardian.ng/features/transparency-in-asset-declaration-regime-still-a-long-way-ahead/ (accessed 8 December 2021).

The International Organization of Securities Commissions, 'General Information' (http://www.iosco.org) http://www.iosco.org/about/ Accessed 10th of September 2014

The Law Commission (LAW Com No 313) Reforming Bribery 2008: ***lawcommission****.justice.gov.uk/docs/cp185_****Reforming_Bribery****_report.pdf Accessed 15th May 2013*

The Punch, 'Court BVN ruling: Saving genuine account owners', (http://punchng.com/ 3 November 2017), Available at: http://punchng.com/court-bvn-ruling-saving-genuine-account-owners/ (accessed 8 April 2018).

The Punch, 'EFCC intercepts N250m cash haul at Balogun market', (https://punchng.com 10 April 2017) Available at: http://punchng.com/efcc-intercepts-n250m-cash-haul-at-balogun-market/ (accessed 4 June 2017).

The Punch, 'Fraudsters working in banks, aiding corrupt politicians –EFCC', (https://punchng.com/ 6 April 2019) Available at: https://punchng.com/fraudsters-working-in-banks-aiding-corrupt-politicians-efcc/ (accessed 6 April, 2019).

The World Bank, 'Comprehensive Reference Guide to AML/CFT' (http://web.worldbank.org) http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAML/0,,contentMDK:20746893~menuPK:2495265~pagePK:210058~piPK:210062~theSitePK:396512,00.html Accessed 10th September 2014

The World Bank, 'What we do' (http://www.worldbank.org) http://www.worldbank.org/en/about/what-we-do Accessed 10th September 2014

Transparency International, *'Corruption Perceptions Index'* (https://www.transparency.org 2021) https://www.transparency.org/en/cpi/2021 Accessed 6 July 2022.

Transparency International, Óverview' (http://www.transparency.org) http://www.transparency.org/whoweare/organisation Accessed 10th September 2014

U.S Department of Homeland Security, 'Declaring currency when entering the U.S in-transit to a foreign destination' (https://help.cbp.gov) https://help.cbp.gov/app/answers/detail/a_id/778/~/declaring-currency-when-entering-the-u.s.-in-transit-to-a-foreign-destination Accessed 7th September 2014

UMORU, H. and KUMOLU, C., 'My house was raided by Police, nothing was found – Ekweremadu', (https://www.vanguardngr.com/ 27 May 2017) Available at:

http://www.vanguardngr.com/2017/05/house-raided-police-nothing-found-ekweremadu/ (accessed 4 June 2017).

Umoru, H. and Nnochiri, I., 'Ekweremadu: Police dock whistleblower over false information', (https://www.vanguardngr.com/ 31 May 2017) Available at: http://www.vanguardngr.com/2017/05/ekweremadu-police-dock-whistleblower-false-information/ (accessed 10 June 2017).

Willis Limited (2013) http://www.willis.com/Regulation/ accessed 15th May 2013

Wolfsberg Group, 'Global Banks: Global Standards' (http://www.wolfsberg-principles.com/) http://www.wolfsberg-principles.com/ Accessed 28th September 2014