MONEY LAUNDERING TYPOLOGIES THROUGH FRAUD IN NIGERIA

DECEMBER 2023

A publication of the Nigerian Financial Intelligence Unit

The Nigerian Financial Intelligence Unit (NFIU) is the central national agency responsible for the receipt of disclosures from reporting organisations, the analysis of these disclosures and the production of intelligence for dissemination to competent authorities. The NFIU is an autonomous unit, domiciled within the Central Bank of Nigeria and the central coordinating body for the country's Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML/CFT/CPF) framework.

The Director/Chief Executive Officer, Nigerian Financial Intelligence Unit
12, Ibrahim Taiwo Street, Aso Villa Abuja, Nigeria
1, Monrovia Street, Block 3, Wuse II, Abuja, Nigeria
(e-mail: info@nfiu.gov.ng)

Cover photo credits
© pngimg.com, pixabay.com, pngwing.com,
vecteezy.com, pinterest.com, toolxox.com, pngkey.com,
medium.com

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

We extend our profound gratitude to the following agencies and organizations for their unwavering support and commitment in facilitating the completion of this report on money laundering typologies from fraud in Nigeria:

1. Association of Chief Compliance Officers of Banks in Nigeria
2. Central Bank of Nigeria
3. Committee of e-Business Industry Heads
4. Economic and Financial Crimes Commission
5. Federal Ministry of Justice
6. INTERPOL– National Central Bureau
7. National Insurance Commission
8. Securities and Exchange Commission

This collaborative effort between the public and private sector exemplifies the essence of partnership in comprehending the intricate dynamics of money laundering through fraud, especially in the context of emerging technologies. The recognition of the high threat posed by money laundering through fraud, as identified in Nigeria's National Risk Assessment, underscores the urgency and importance of this study.

The outcomes of this research are poised to elevate our collective understanding and response to the ever-evolving challenges posed by fraudulent activities. This report will serve as a vital resource for reporting entities and competent authorities, equipping them with the knowledge required to detect and combat fraud effectively.

Finally, we would like to express our gratitude to all of the Nigerian Financial Intelligence Unit (NFIU) team members whose persistent work and commitment made this study possible. We appreciate their efforts to this project and their excellent dedication to professionalism and quality.

Thank you all for your support and contributions to this report on money laundering typologies through fraud in Nigeria.

Modibbo R. HammanTukur
Director/CEO
Nigerian Financial Intelligence Unit

LIST OF ACRONYMS

ACAMS	Association of Certified Anti-Money Laundering Specialist
ACCOBIN	Association of Chief Compliance Officers of Banks in Nigeria
ACFE	Association of Certified Fraud Examiner
AI	Artificial Intelligence
AML	Anti Money Laundering
API	Application Programme Interface
ATM	Automated Teller Machine
BDC	Bureau de Change
BEC	Business Email Compromise
BINs	Bank Identification Numbers
BTC	Bitcoin
BVN	Bank Verification Number
CAC	Corporate Affairs Commission
CBI	Citizenship By Investment
CBN	Central Bank of Nigeria
CBTRs	Cash Based Transaction Reports
CDD	Customer Due Diligence
CeBIH	Committee of e-Business Industry Heads
CFE	Certified Fraud Examiner
CFT	Combating the Financing of Terrorism
CMOs	Capital Market Operators
COO	Chief Operating Officer
CPF	Combating Proliferation Financing
CRIMS	Crime Record Information Management System
CTRs	Currency Transaction Reports
DMBs	Deposit Money Banks
DNFBPs	Designated Non-Financial Business and Professions
EDD	Enhanced Due Diligence
EFCC	Economic and Financial Crimes Commission
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FGN	Federal Government of Nigeria
FIs	Financial Institutions
FinTech	Financial Technology
FITC	Financial Institute Training Centre
FMoJ	Federal Ministry of Justice
FTRs	Foreign Transaction Reports
GDP	Gross Domestic Product
GoAML	Government Office Anti-Money Laundering
ICO	Initial Coin Offerings
IMTOs	International Money Transfer Operators
INTERPOL	International Criminal Police Organization
IOSCO	International Organization of Securities Commissions
KYC	Know Your Customer
LEAs	Law Enforcement Agencies

LPO	Local Purchasing Order
ML	Money Laundering
MLPPA	Money Laundering (Prevention and Prohibition) Act
NAICOM	National Insurance Commission
NCB	National Central Bureau
NDLEA	National Drug Law Enforcement Agency
NeFF	Nigerian Electronic Fraud Forum
NFIU	Nigerian Financial Intelligence Unit
NIBSS	Nigeria Inter-Bank Settlement System
NIMC	National Identity Management Commission
NIN	National Identification Number
NPF	Nigerian Police Force
PEPs	Political Exposed Persons
PIA	Public Internet Access
PSFU	Police Special Fraud Unit
PSPs	Payment Service Providers
REs	Reporting Entities
ROI	Return On Investment
SARs	Suspicious Activity Reports
SCUML	Special Control Unit against Money Laundering
SEC	Securities and Exchange Commission
SRBs	Self-Regulatory Bodies
STRs	Suspicious Transaction Reports
UK	United Kingdom
UN	United Nations
USA	United State of America
US-CIS	United States Center for Immigration Studies
USD	United States Dollar
USSD	Unstructured Supplementary Service Data

CHAPTER 1 INTRODUCTION

Background

Fraud arises from the exposure of illegal financial activities, in both public and private sectors of the economy, and can be perpetrated by individuals and corporate institutions, and can be simplistic or complex in nature. This dishonest behaviour presents itself in a variety of ways, including, but not limited to, deceit, bribery, fraud, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealing of material facts, and collusion.

Fraud has been in existence over several centuries and its diverse nature has resulted in several studies producing several definitions addressing each facet of this crime.

The Nigerian Police Force defines fraud as "dishonest activity causing actual or potential financial loss to any person or entity, including theft of money or other property, by employees or persons external to the entity; and where deception is used at the time, immediately before or immediately following the activity"[1]. In another context, the Association of Certified Fraud Examiners (ACFE,1999) defined fraud as "the wilful misuse or misappropriation of an organization's assets or resources for personal gain".

A central theme in the numerous definitions of fraud is the deceptive attempt to acquire monetary or intangible advantages inflicting harm or disadvantage to the misled individual or institution, is central to these classifications. Alongside associated crimes such as market abuse and counterfeiting, fraud can have a catastrophic, from the excessive personal losses incurred by the most vulnerable victims to the ability of organizations to remain in operation.

To make matters worse, the expansion of global financial markets has provided many more chances for transborder criminals, resulting in an increase in the number of recorded cases of fraud globally[2]. Given its transnational nature, the Financial Action Task Force[3] listed fraud as a money laundering offence requiring jurisdictions to implement adequate measure to

[1] https://www.specialfraudunit.org.ng/en/?page_id=93
[2] ibid
[3] The Financial Action Task Force (FAF) is the global standard setter for combatting money laundering, terrorist financing and other predicate crimes (www.fatf.org)

identify fraud types, conduct risk assessment and ensure appropriate measures are enforced to mitigate the identified risks.

Nigeria, as Africa's most populous country and one of its largest economies, is not immune to this menace. In recent years, the country has faced a growing concern over the occurrence of money laundering activities, particularly through fraud schemes. While public concern expands by the day and management vigilance improves, with the aid of computerization, millions of naira are still lost to fraud, which results in huge financial losses to business organizations and their customers, depletion of shareholders' funds and capital base, and loss of confidence in businesses[4].

A report from Financial Institute Training Centre (FITC) on fraud and forgeries on Nigerian banks and industries for the 3rd quarter 2022 indicates that a total number of Nineteen Thousand, Three Hundred and Fourteen (19,314) cases of Frauds and Forgeries were recorded with approximately N9.63 billion loss. The figures showed that the highest number of occurrences was recorded under computer/ web fraud followed by mobile fraud which includes fraud committed through USSD transaction and other related fraud[5]. In another source, the Sun (2023) has referenced the statement made by Nigeria Inter-Bank Settlement System (NIBSS) stating that Nigerian banks have lost N9.7 billion to e-fraud in the first seven months of 2023.

Fraud has gained prominence in transnational organized crime emanating from Nigeria, in which investigations have revealed a structure in which criminals are trained on credit card, bank, and insurance scams to raise funds to finance nefarious activities. In a sweeping international effort, INTERPOL's Operation Jackal conducted between May 15 and May 29 2023 successfully targeted West African organized crime groups, specifically Black Axe, prominent in Nigeria, and renowned for their cyber-enabled financial fraud activities. This operation involved 21 countries and led to the freezing of over 200 illicit bank accounts, EUR 2.15 million in seized or frozen assets, 103 arrests, the identification of 1,110 suspects, and notable recoveries in multiple countries.

[4]Dimensions of Fraud in Quoted Firms in Nigeria article in American Journal of Social and Management Sciences · September 2012

[5] https://fitc-ng.com/wp-content/uploads/2023/07/FITC-Frauds-Forgeries-Report-2022-3rd-quarter.pdf

The 2022 National Inherent Risk Assessment of money laundering in Nigeria report revealed the threat of fraud to be very high. The report states that fraudsters in Nigeria display a high degree of sophistication, operating across complex sectors while skilfully adapting to and manipulating rules and regulations. The banking sector was reported to have witnessed the highest number of fraudulent activities occasioned by Advance Fee Fraud (419/Yahoo Yahoo). Notably, the dominant form of internet crime identified from the report is Online Dating/Romance Scam, comprising 64% of arrests made.

The report also highlights the exploitation of both bank and non-bank products and services to commit fraud. These include the use of International Money Transfer Operators (IMTOs), web transactions, mobile wallets, gift cards, cryptocurrencies, use of Bureau De Change services, These findings underscore the evolving and complex nature of fraud-related money laundering in Nigeria.

Study Objectives

The objectives of the study are as follows;

a) To determine the level of fraud in Nigeria and highlight the common methods employed by criminals to launder the proceeds of fraudulent activities.

b) To review the legal and institutional frameworks to curb fraud across various sectors.

c) To identify the vulnerabilities in various sectors that enable fraud.

d) To identify the trends and patterns of fraud in various sectors through the analysis of case studies provided by competent authorities.

e) To recommend policies that will safeguard the Nigerian economy against fraud.

f) Highlight red flags or indicators that may assist in combatting fraud.

g) To recommend preventive measures for Supervisory Authorities, Law Enforcement Agencies (LEAs) and Reporting Entities (REs).

h) To sensitize the populace on precautionary measures to take against fraud.

Methodology

The project adopted both primary and secondary data sources by analyzing questionnaire responses and a desk review of reports, journals, reliable open-source information, and interviews with subject matter experts. The project team consisted of experts from the

Association of Chief Compliance Officers of Banks in Nigeria (ACCOBIN), Central Bank of Nigeria (CBN), Committee of e-Business Industry Heads (CeBIH), Economic and Financial Crimes Commission (EFCC), Federal Ministry of Justice (FMOJ), the International Criminal Police Organization – National Central Bureau (INTERPOL-NCB), the Securities and Exchange Commission (SEC), the National Insurance Commission (NAICOM) and the Nigerian Financial Intelligence Unit (NFIU).

In order to illustrate the money laundering dimension associated with the types of fraud, the study leveraged on sanitized case studies provided by agencies on the project team. The report was further reviewed and validated by the agencies and institutions on the project team.

CHAPTER TWO: UNDERSTANDING FRAUD: DEFINITION AND TYPES

Understanding Fraud

Fraud refers to alteration of facts either by deliberately withholding relevant information or providing false statements to another person/institution with the intention of obtaining something that cannot be secured without the deception[6]. The act is characterized by the intentional deprivation of a deceived individual or institution from the benefits rightfully due to them, achieved through a spectrum of deceptive means which encompass a variety of unlawful and unethical tactics.

There have been several studies and research to evaluate the nature and impact of fraud. A widely received study originates from the criminological research of Edwin Sutherland and Donald R. Cress and introduced into the lexicon of fraud risk analysis by Steve Albrecht. This study introduces the concept known as the "fraud triangle[7], an essential framework for assessing and predicting the conditions conducive to heightened fraud risk.

The fraud triangle, elucidates that individuals are propelled towards committing fraud when three pivotal elements converge: (1) the existence of perceived pressure, (2) the presence of perceived opportunity, and (3) the availability of a mechanism to rationalize the fraudulent act as consistent with one's ethical framework.

In contemporary anti-fraud practice, the fraud triangle serves as a fundamental tool employed by professionals to reveal the underlying conditions that may incentivize individuals or entities to engage in fraudulent activities. Furthermore, this model proves invaluable in shedding light on broader economic or industry-specific circumstances that could contribute to an elevated overall risk of fraud. To identify and assess such risks, anti-fraud experts systematically scrutinize the presence and interplay of the following three critical factors:

Motivation: The presence of external or internal pressures that prompt individuals or entities to contemplate fraudulent actions, such as financial distress or personal incentives.

[6] What Is Fraud? Definition, Types, and Consequences (investopedia.com)
[7] https://www.whistleblowers.org/fraud-triangle/

Opportunity: The existence of vulnerabilities within an environment that enable fraud to occur, including weak internal controls or insufficient oversight.

Rationalization: The capacity of individuals to psychologically justify their fraudulent behaviour, often by convincing themselves that their actions are consistent with their personal values or situational ethics.

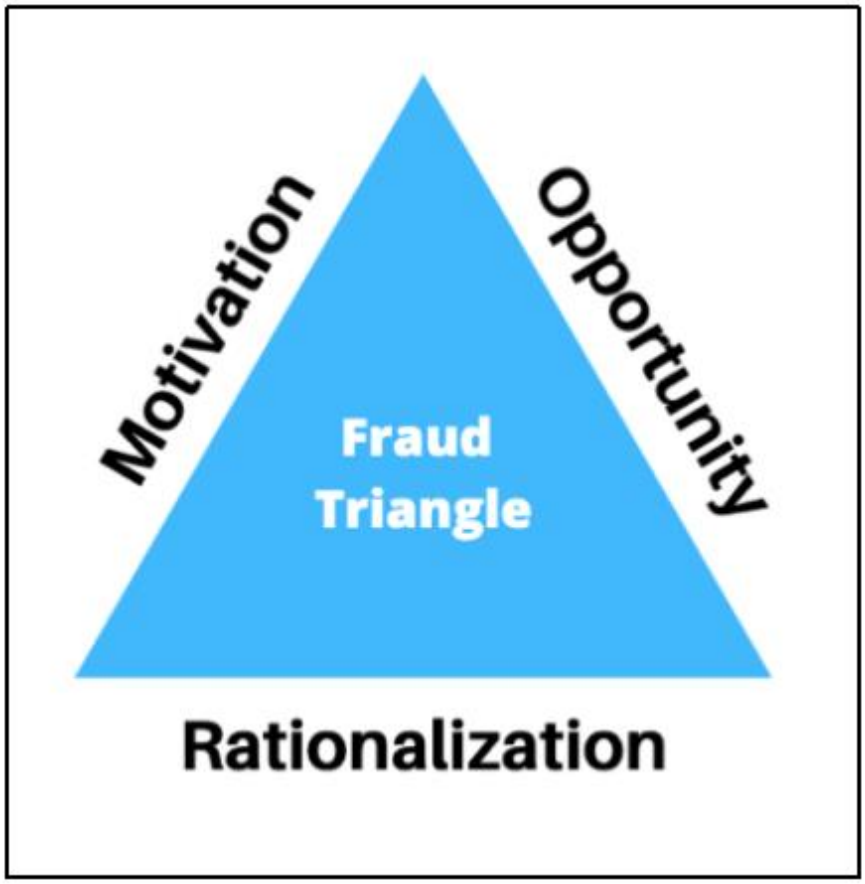


Chart 1: Fraud Triangle

By comprehensively evaluating these dimensions, anti-fraud professionals can proactively assess and mitigate fraud risks, making the fraud triangle an indispensable framework in the field of fraud typologies and prevention.

Types of Fraud in Nigeria

According to the Nigeria Inter-Bank Settlement System (NIBSS), in 2020, Nigeria lost about ₦5 billion (approximately $6.6 million USD) to fraud in 9 months depicting the surge of fraudulent activities in recent times[8]. An analysis of the prevalent fraud types derived from the 2022

[8] In 2020, Nigeria lost ₦5b to fraud in 9 months: What you need to watch out for (techpoint.africa) (5.6.2023)

National Inherent Risk Assessment of Money Laundering in Nigeria Report, reveals distinct categories to include; Mail Fraud (Business Email Comprise, email phishing) Identity Fraud (Driver License Fraud) Debit/Credit Card Fraud, Recruitment Scams, Voters Fraud, Internet Fraud (inclusive of romance fraud, cyber-squatting, electronic signature fraud, WhatsApp hack etc.). The findings of the 2022 National Inherent Risk Assessment of Money Laundering in Nigeria Report also identifies sectors that exhibit a heightened susceptibility to fraud. These sectors include Manufacturing, Real Estate, Extractive Industries, Academia, Public Service, and the Financial/Banking sector. Consequently, it is imperative to implement targeted preventive measures and vigilance within these sectors to effectively combat the pervasive threat of fraud in Nigeria.

The following highlights the most prevalent fraud types in Nigeria:

Advance Fee Fraud (419 Scam): This is perhaps the most common type of fraud in Nigeria. It involves individuals enticing victims through phones calls, email and social media platforms to participate in lucrative business deals, or lottery winnings. Individuals are more susceptible to this scam, where they innocently provide down payments or personal information, only to discover that the pledged funds or opportunities are nothing more than a deceptive scheme with no real existence. This is popularly referred to as “419”, which is coined from the section of the Nigerian Criminal Code Act, 1916 dealing with fraud.

Identity Theft: Identity theft refers to an unauthorized use of an individual’s personal information for fraudulent activities. This includes stealing bank details, bank/credit card information, social engineering, or creating fake identities.

Phishing and Online Fraud: With increased internet footprint globally, there has been an increase in online scams, Smishing, vishing and phishing attempts. Fraudsters create numerous fake websites and social media platform to trick individuals into providing their personal or financial information. Most times this scam can range from pretending to be a bank employee or a reputable organization to luring victims into fake investment schemes. With a rise in e-commerce services, fraudsters exploit merchants’ websites to steal vital customer data, mirroring legitimate or creating fake websites to scam customers and distribute goods of inferior quality compared to what is advertised on the website. Smishing is a cyber-attack that targets individuals through SMS (Short Message Service) or text

messages. The term is a combination of "SMS" and "phishing. "In a smishing attack, cybercriminals send deceptive text messages to lure victims into sharing personal or financial information, clicking on malicious links, or downloading harmful software or applications[9]. Vishing on the other hand involves telephonic conversation with the prospective victim.

Investment Fraud: Investment fraud refers to deceptive practices in which fraudster offer fake investment opportunities, Ponzi schemes, or high-yield investments with unrealistic returns. They typically use false information, present manipulated or false stock prices, promise unrealistic but very attractive short-term returns on investment, or employ persuasive techniques to lure victims into investing their money.

Debit/Credit Card Fraud: This type of fraud involves unauthorized use of credit or debit card information to make fraudulent purchases, withdrawals or obtain cash advances. It occurs through the use of stolen cards, card skimming devices, or online data breaches.

Chargeback Fraud: Chargeback fraud occurs when a consumer makes a purchase with their credit card and then disputes the charge with the credit card company, claiming that the transaction was unauthorized. This can lead to a chargeback, where the funds are returned to the consumer. However, in cases of fraud, the consumer may have actually made the purchase and is attempting to get a refund while keeping the goods or services. Merchants often face financial losses and increased fees due to chargeback fraud.

Insurance Fraud: Insurance fraud involves submitting false or exaggerated claims to insurance companies to receive undeserved benefits or compensation. This can include staging accidents, inflating the value of claims, or providing false information about injuries or property damage.

Employment and Job Scams: Fraudsters may target job seekers by offering fake job opportunities and promising high salaries or work-from-home arrangements. Victims may be asked to pay upfront fees, provide personal information, or perform tasks that are not legitimate.

[9] What Is Smishing? Examples, Protection & More | Proofpoint US

Charity and Donation Scams: Scammers exploit human empathy by setting up fake charities or soliciting donations for fabricated causes. They may use emotional appeals or high-pressure tactics to convince individuals to donate money, which is then pocketed by the fraudsters.

Tax Fraud: Tax fraud involves intentionally providing false information or engaging in illegal practices to evade or reduce tax obligations. This can include underreporting income, inflating deductions, or using fake documents.

Cybercrime: Nigeria has over the experienced an increase in cybercrime activities such as hacking, data breaches, and ransomware attacks[10]. Cybercriminals exploit vulnerabilities in the financial sector in order to gain unauthorized access, steal sensitive information and demand ransom payments. The banking sector is most susceptible to this type of fraud.

Bank Fraud: Bank fraud constitutes a financial offense wherein a financial institution or its services are exploited for personal benefit or to engage in illicit actions. It encompasses several methods, including fabricating accounts, employing fake identities, or tampering with account records. Additionally, it may encompass the unauthorized usage of stolen credit or ATM cards to access a financial institution's funds. This type of fraud is a significant offense, carrying severe consequences such as substantial fines, imprisonment, and potential revocation of business licenses.

Procurement Fraud: Procurement fraud is the unlawful manipulation of a procurement process to acquire contracts, good or services or to obtain an unfair advantage during the procurement process. There are many examples of schemes to engage in procurement fraud. Schemes may affect the bidding process, affect the awarding of a contract, or include fraud that occurs after being awarded a contract[11]. Procurement fraud is an issue of concern in Nigeria. The newly appointed chairman of the Economic and Financial Crimes Commission (EFCC), Mr. Ola Olukoyede, has revealed that Nigeria lost N2.9trillion to contract and procurement fraud between 2018 and 2020[12].

[10]Banks lose N5bn to fraudsters in nine months – NDIC Banks lose N5bn to fraudsters in nine months – NDIC | The Nation Newspaper (thenationonlineng.net) (Accessed 6.6.2023)
[11] https://www.schneiderwallace.com/practice-areas/whistleblower-claims/procurement-fraud/examples-of-procurement-fraud/
[12] https://leadership.ng/nigeria-lost-n2-9trn-to-contract-procurement-fraud-in-3-years-efcc-chairman/

It is important to note that fraud can take various forms fraudsters continuously adapt their techniques to appear legitimate. Staying informed, maintaining vigilance, and exercising caution when sharing personal or financial information is crucial to protect oneself from falling victim of fraudulent activities.

Electronic Fraud in Nigeria

Electronic fraud has emerged as a formidable challenge in Nigeria, distinguishing itself as a prominent facet of the broader fraud landscape. Unlike traditional forms of fraud, electronic fraud leverages technology to reach a vast and often unsuspecting audience, making it a preferred method for fraudsters. The prevalence of electronic fraud in Nigeria can be attributed to several factors, including the rapid digitization of financial services, and availability of internet. This convergence of technological convenience and criminal innovation has made electronic fraud a major concern, necessitating focused efforts to counter its impact on individuals and the economy at large.

In Nigeria's electronic fraud landscape, wallet accounts are frequently used due to their relative ease of access and flexibility. They provide a convenient avenue for perpetrators to channel and manipulate fraudulent proceeds without immediate detection. The anonymity and agility of these accounts make them a preferred tool for fraudsters seeking to obfuscate the paper trail of illegal transactions.

Despite their prominence in fraudulent activities, discussions about combating electronic fraud often overlook the pivotal role of wallet accounts. The recovery process concerning funds transacted through these accounts is particularly challenging. The intricate network of transactions and the lack of stringent oversight in some cases make it exceedingly difficult, if not impossible, to recover fraudulently acquired funds once they have been moved through wallet accounts. The complexities involved in tracking and retrieving these dispersed funds contribute to the perception that the recovery process associated with wallet accounts is highly ineffective, hence the reference to a "zero" recovery process.

To mitigate electronic fraud effectively in Nigeria, acknowledging and addressing the role of wallet accounts in the perpetuation of fraudulent activities is crucial. Implementing robust monitoring systems, stringent regulations, and enhanced security measures specifically

targeting these accounts can significantly bolster efforts to curb electronic fraud and improve the prospects of successful recovery of fraudulent proceeds.

The cashless policy in Nigeria was introduced to achieve the commendable objectives of reducing physical cash circulation, encouraging electronic transactions, and enhancing the efficiency and transparency of the payment system. Nonetheless, it is essential to recognize that any system, even electronic payment systems, can be susceptible to fraudulent activities. While the primary intent of the cashless policy was to mitigate fraud, it is acknowledged that certain fraudulent practices may have manifested in the context of electronic transactions[13].

At the third quarter general meeting of the Nigerian Electronic Fraud Forum, the Managing Director of Nigeria Interbank Settlement System (NIBSS) noted an upward trajectory in fraud incidents since 2019, culminating in a 377 percent (377%) rise from N3billion to N14.3billion in 2022.

His presentation also reviewed the statistics into fraud incidences reported in 2023 through the industry forum portal as at July, with the month of May having the highest number of fraud incidents with a count of 11,716 records, while the lowest count was recorded in June, totalling 6,240 incidents. Furthermore, his presentation noted that the volume of fraud for the first quarter (Q1) of 2023 stood at N5.1 billion with the figures for April, May, June, and July at N1 billion, N1.6 billion, N0.8 billion, and N1.2 billion respectively.

The analysis above indicates a 33.3% decline in the volume of fraud reported in the second quarter of 2023 from N5.1 billion to N3.4 billion.

The various forms of fraud mentioned should not be viewed in isolation, as instances of fraud could involve a combination of different deceptive practices. This highlights the significance of remaining vigilant and implementing countermeasures to tackle this emerging challenge in the ever-changing financial environment.

[13] Okey Ovat, The Central Bank of Nigeria's Cashless Policy in Nigeria: Benefits and Challenges; Journal of Economics and Sustainable Development; ISSN 2222-1700 (Paper) ISSN 2222-2855 Vol.3, No.14, 2012

CHAPTER THREE: LEGAL AND INSTITUTIONAL FRAMEWORK IN THE FIGHT AGAINST FRAUD IN NIGERIA

Legal Framework in the fight against Fraud in Nigeria

Nigeria has enacted a number of laws and regulations specifically targeting fraud and other financial crimes. The key legislations are the Nigerian Criminal Code Act 1916 and the Nigeria Penal Code 1960 with both legislations have sections specific to fraud. Section 214 of the 1999 Nigerian Constitution established the Nigeria Police Force as the national agency for the detection and prosecution of crimes in Nigeria. Similarly, the Nigeria Police Act, 2020 provide the framework for the Police Force to ensure cooperation and partnership between the police and the host communities in maintaining peace, combatting crime, protecting liberties, life, and property; and for related matters.

Economic and Financial Crimes Commission (Establishment) Act of 2004, which established the Economic and Financial Crimes Commission (EFCC) as the primary agency responsible for investigating and prosecuting economic and financial crimes in Nigeria[14].

The Advance Fee Fraud and Other Fraud Related Offences Act of 2006 is a critical legal framework in Nigeria's fight against fraud. This comprehensive law not only targets advance fee fraud but also encompasses a wide range of fraudulent activities. Section 7 of this legislation, dealing with the illicit acquisition and subsequent concealment of funds obtained from unlawful actions, centers on financial transactions associated with the proceeds derived from specific illegal activities. Engaging in such transactions with the purpose of either facilitating or concealing illegal activities or evading lawful financial dealings according to Nigerian law is a violation of this act. The legislation enforces strict consequences, including incarceration and financial penalties, for individuals knowingly participating in these actions. These stringent measures play a substantial role in discouraging fraudulent behaviour and safeguarding the financial well-being of both individuals and businesses in Nigeria.

The Mutual Legal Assistance in Criminal Matters Act of 2019 aims to establish reciprocal arrangements with other countries for the mutual assistance in prosecuting criminal cases. This assistance encompasses locating and identifying suspects, witnesses, and relevant

[14] Economic and Financial Crimes Commission - THE ESTABLISHMENT ACT (efcc.gov.ng) (Accessed 6.6.2023)

materials for criminal proceedings. Additionally, the Act seeks to address the identification, tracing, freezing, restraining, recovery, forfeiture, and confiscation of proceeds, property, and instrumentalities of crime. It also covers interception of telecommunications, electronic surveillance, property dealings restraint, and asset freezing related to recoverable, forfeitable, or confiscatable assets linked to offences. Moreover, the Act allows for any form of assistance that complies with the requesting State's municipal law.

The Proceeds of Crime (Recovery and Management) Act, 2022 in Nigeria aims to establish an effective legal framework for recovering and managing proceeds of crime, including assets obtained unlawfully, and to facilitate the forfeiture of such assets. It also introduces non-conviction-based procedures for asset recovery, strengthens collaboration among relevant organizations, and outlines the process for managing and disposing of forfeited properties on behalf of the Federal Republic of Nigeria.

Other relevant laws include the Money Laundering (Prevention and Prohibition) Act, 2022, Cybercrime (Prohibition, Prevention, etc.) Act, 2015, the Banks and Other Financial Institutions Act, 2020, the Investment and Securities Act 2007 and the Independent Corrupt Practices and Other Related Offences Commission Act, 2000.

These laws, though not an exhaustive list, serve as a legal basis serve as a legal basis for combating different types of fraud and financial crimes in Nigeria.

Institutional Framework in the Fight Against Fraud

Federal Ministry of Justice: The Federal Ministry of Justice in Nigeria serves as the legal branch of the federal government, primarily responsible for presenting cases in the judiciary that are either initiated or taken up by the government. The plays a multifaceted role in addressing fraud matters by providing legal support, facilitating investigations, influencing legislation, and contributing to policy development in order to combat and prevent fraud within the country, and collaborate with international counterparts and organizations to address cross-border fraud issues. The Central Authority Unit (CAU) of the FMOJ receives and dispatches all incoming and outgoing requests for Mutual Legal Assistance (MLA) and extradition to relevant law enforcement authorities (LEAs) and foreign counterparts through diplomatic channels via the Protocol Department at the MOFA. This Unit is directly under the supervision of the

Honourable Attorney-General of the Federation and Minister of Justice who is the chief law officer of the Federation.

Nigeria Police Force: Section 4 of the Nigeria Police Act, provides as follows, "The Police shall be employed for the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of life and property and the due enforcement of all laws and regulations with which they are directly charged". The Nigeria Police Force established the Cybercrime Unit in 2017 to combat cybercrime. The unit is equipped with modern forensic tools which are manned by well-trained detectives with IT background. It has an enhanced capability to analyse various digital devices, collect evidence with high tech digital forensic equipment, examine documents of various file types, amongst other critical functions[15].

Economic and Financial Crimes Commission (EFCC): The EFCC is Nigeria's leading agency for investigating and prosecuting economic and financial crimes. It is an autonomous institution saddled with powers to arrest, detain, and prosecute individuals involved in economic and financial crimes. The EFCC collaborates with other law enforcement agencies, such as the Nigeria Police Force, Independent Corrupt Practices Commission and Nigerian Financial Intelligence Unit, to ensure effective enforcement of anti-fraud laws.

National Cybersecurity Coordination Centre: Institutionally fortifying Nigeria's fight against cybercrime, the National Cybersecurity Coordination Centre (NCCC) has been established as a pivotal component. The NCCC serves as the linchpin for seamless coordination and effective monitoring of cybersecurity efforts, aligning with the national cybersecurity roadmap. Mandated by Section 41 of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015, the Office of the National Security Adviser (NSA) spearheads this initiative. The NCCC's primary purpose is to execute Nigeria's national cybersecurity program in compliance with domestic laws and international standards. It operates as both a domestic and international cybersecurity hub, with a strategic structural model that aligns with the responsibilities of the Office of the National Security Adviser, the National Cybercrime Advisory Council, and other pertinent frameworks outlined in The Act[16].

[15] https://incb.npf.gov.ng/about%20us.php
[16] https://ctc.gov.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_24223825.pdf

Nigerian Financial Intelligence Unit (NFIU): The NFIU is the central body in Nigeria responsible for requesting, receiving, analysing, and disseminating financial intelligence to relevant law enforcement agencies. The Unit plays a pivotal role in identifying suspicious financial transactions and supporting investigations related to fraud and money laundering.

Central Bank of Nigeria (CBN): The CBN plays as a regulator a pivotal role in combatting fraud within the financial sector of the economy, through the supervision of Banks and Other Financial Institutions[17]. It establishes and enforces regulations in order to ensure integrity in the banking system. Some of these regulations include; Know Your Customer (KYC) requirements, Anti-Money Laundering (AML) measures, and Cybersecurity guidelines. The CBN also engages with other relevant stakeholders to develop and implement policies that enhance financial transparency and prevent fraudulent activities in the banking sector.

Securities and Exchange Commission: The Securities and Exchange Commission (SEC) is a Government Agency mandated to regulate and develop the Nigerian Capital Market. The SEC's role include developing the Capital Market, promoting investor protection, ensuring market transparency, regulating securities offerings, licensing and supervising market participants, enforcing market rules and regulations to maintain the integrity and stability of the Nigerian capital market.

National Insurance Commission: The National Insurance Commission (NAICOM) was established in 1997 by the National Insurance Commission Act 1997 with responsibility for ensuring the effective administration, supervision, regulation and control of insurance business in Nigeria and protection of insurance policyholders, beneficiaries and third parties to insurance contracts.

The Special Control Unit against Money Laundering (SCUML): The Special Control Unit against Money Laundering (SCUML) operates as a department within the Economic and Financial Crimes Commission with the primary task of supervising designated non-financial businesses and professions[18] to ensure their compliance with anti-money laundering laws and

[17] Other Financial Institutions" as non-bank financial institutions that provide financial services and products, but are not classified as deposit money banks (commercial banks). These institutions may offer specialized financial services and include entities such as microfinance banks, finance companies, development finance institutions, bureau de change, payment service providers, and other financial intermediaries.

[18] DNFBPs, which stands for Designated Non-Financial Businesses or Professions, encompass non-financial institutions and various professions that carry a risk of being exploited for money laundering and terrorism

regulations. SCUML has several key responsibilities, which include registering and certifying these designated entities in line with the relevant legal provisions, monitoring and supervising their operations, and imposing administrative fines to ensure compliance.

Self-Regulatory Bodies (SRBs), and Industry Associations: These bodies play a vital role in combating fraud by setting ethical standards, monitoring compliance, enforcing regulations, providing education and training, and collaborating with stakeholders to ensure the integrity of their respective industries.

Designated Courts: Nigeria has also designated courts to handle economic and financial crimes cases. These include the Federal High Court and the High Court of the Federal Capital Territory, which have jurisdiction over criminal matters related to fraud and financial crimes.

International Cooperation: Nigeria engages actively in international cooperation to fight fraud and financial crimes. Nigeria has signed a number of treaties such as the mutual legal assistance treaties with several countries, allowing for the exchange of information and collaboration in investigating cross-border crimes[19]. Nigeria is also an active member of international organizations such as the International Criminal Police Organization (INTERPOL), which facilitate global efforts to combat fraud and money laundering.

In addition to the above-mentioned institutions, other competent authorities, ministries, departments and agencies are obliged to establish and enforce strong ethical codes to mitigate fraud activities. Efforts are also in place to strengthen the legal, regulatory, and institutional framework to address fraud in Nigeria. However, challenges persist due to insufficient resources, corruption, and the continually changing landscape of fraud. Overcoming these challenges demands a sustained commitment and collaboration among government agencies, financial institutions, civil society organizations, and international partners.[20].

financing. You can find the specific sectors classified as DNFBPs in Section 30 of the 2022 Money Laundering Prevention and Prohibition Act.

[19]TREATIES RATIFIED BY NATIONAL ASSEMBLY OF NIGERIA (lawnigeria.com)

[20]Fight Against Corruption In Nigeria: Challenges and Prospects for Sustainability, By Nuhu Ribadu - Premium Times Opinion (premiumtimesng.com) Accessed 5.6.2023)

CHAPTER FOUR: TYPOLOGIES OF FRAUD IN NIGERIA, ANALYSES OF CASE STUDIES, REDFLAGS AND INDICATORS

It is critical to analyse the typologies and case studies that highlight the many strategies, actors, and contexts involved in order to comprehend the dynamics of money laundering through fraud.

A typology is a classification system that groups comparable cases together based on their qualities, whereas a case study is a detailed examination of a specific instance or circumstance. Typologies and case studies, taken together, provide insights into the patterns and trends of money laundering through fraud, as well as the obstacles and opportunities for prevention, detection and prosecution.

The case studies featured in this report were furnished by law enforcement authorities after conducting investigations. These studies illustrate the various manifestations of fraud in Nigeria, the connections between different types of fraud, and the vulnerabilities and loopholes that perpetrators exploit to carry out these fraudulent activities.

Typology 1: Laundering of Proceeds of Fraud through Cryptocurrency Platforms

CASE STUDY 1– FRAUDULENT SCHEME AND ILLEGAL CRYPTOCURRENCY OPERATION
In 2021, the EFCC received a petition from a foreign LEA investigating a case of alleged fraud of **($349,000**) involving two fraudsters believed to be Nigerian citizens. Information gathered showed that the suspects had left Nigeria for Kenya. Bank statements analysis of the two suspects revealed that they received payments regularly from the same account. Further scrutiny revealed that the payer to the accounts of both suspects was a final year student in a Nigerian university, who had a turnover of over **N1.2 billion** (approx. **$1.6 million USD**) in one of his accounts. The moneyman was arrested and interrogations revealed that he was a tech-savvy individual whom knowingly provided fiat value for cryptocurrency to fraudsters, including the two suspects that prompted the investigation. Investigations also revealed that the money man purchased a luxurious vehicle and lived in a well-furnished apartment. One luxurious vehicle and jewelries were recovered from him. Legal Opinion is waited for the prosecution of the case.
Indicators/techniques/methods ❖ Payments came in regularly from a particular questionable account to both suspects.

- ❖ A university student purchased a luxurious vehicle, expensive jewelleries and lived in a well-furnished apartment.
- ❖ A university student with a turnover of over ₦1.2 billion (approx. $1.6 million USD) in one of his accounts
- ❖ Use of bank accounts to launder proceeds received from fraudulent sources

Jurisdictions Involved

Kenya, Nigeria

Source: EFCC

CASE STUDY 2– LAUNDERING OF PROCEEDS FROM CRIMINAL CONSPIRACY, CYBERCRIME, ADVANCED FEE FRAUD THROUGH CRYPTOCURRENCY

This deals with an Intelligence Report sent to the **EFCC** by the **Nigerian Financial Intelligence Unit** on the account activities of one **MS**, a waitress working at XXX Hotels in Nigeria.

On receipt of the intelligence, investigators commenced investigation immediately and gathered intelligence from bank accounts linked to the suspect.

Intelligence was also requested from competent authorities including Binance – a Centralized Crypto Exchange, wherein the suspect held a wallet account. Investigations further revealed that the suspect was a legitimate crypto exchange service provider who was contracted by one **HB** to exchange Crypto worth over **$2,000,000.00** to cash on behalf of one "**MZ**" who allegedly resides in Vietnam.

The Principal Suspect –**HB**, a middle man in this transaction, utilized the proceeds of sale in the purchase of properties both within and outside Port Harcourt, Rivers State valued at over **N315, 000,000.00** (approx. **$416,000 USD**).

'MZ' is presently avoiding apprehension due to suspicions about the illegitimate source of the sold cryptocurrency."

All properties linked to the suspect were traced and an application for Interim Forfeiture has also been made by the Commission to the Federal High Court

Indicators/techniques/methods

- Transactions that do not match profile (waitress transacting **$2,000,000.00**)
- Use of cryptocurrency platform to exchange huge amount of cash worth $**2,000,000**
- Use of middle man (**HB**) by **MZ** who is in country Vietnam

- Purchase of properties within and outside Port Harcourt over **N315, 000,000.00** (approx. **$416,000 USD**).

Jurisdictions Involved

Nigeria (Abuja/Port Harcourt)/Vietnam

Source: EFCC

CASE STUDY 3– LAUNDERING OF PROCEEDS FROM CYBERCRIME THROUGH CRYPTOCURRENCY PLATFORM AND BANK ACCOUNTS

The petitioner alleged that on 30th June 2022, the company discovered a loophole in their Nigerian payment solution which was exploited by **Mr EI**. The petitioner created transactions worth **$10,000** but the transaction that appeared on the petitioner's end was **$4,000,000** (the "Scam"). Out of the total amount inputted, the cumulative sum of **$3,000,000** was fraudulently withdrawn by **Mr EI** via cryptocurrency trading platforms. **Mr EI** laundered the illicit funds using different third parties bank accounts via peer-to-peer[21] exchange of the virtual asset to fiat money and the naira equivalent subsequently paid by the third parties into his local bank account.

Indicators/techniques/methods

- Transaction of **$10,000** made to appear as **$4,000,000**
- Use of cryptocurrency platform to withdraw huge sums of money (**$3,000,000**)
- Use of third-party bank Accounts via peer-to-peer virtual asset exchange
- Multiple payments of huge sums to the same account in local currency

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 4 – MONEY LAUNDERING OF PROCEEDS FROM ROMANCE SCAM THROUGH CRYPTO WALLET

During a sting operation conducted by the EFCC in 2021, a fraud suspect named Mr. YY was apprehended and questioned following a complaint filed a victim of a suspected romance scam who had been persistently trying to contact him, and he had refrained from responding to her for

[21] Peer-to-peer (P2P) refers to a decentralized network or system in which participants (peers) can directly interact and share resources, services, or information with one another, without the need for a centralized intermediary.

several days. Forensic analysis of the device revealed on **Mr YY** revealed that he had portrayed himself as an American Surgeon on a UN Mission to the Middle East to the victim who was a Korean-American. He convinced her to financially support him through crypto payments on the grounds that cash payments are difficult to carryout. **Mr YY** promised his victim that he would marry her on his return. He also informed the victim that he was expecting a **$5 million** payment with which they could start their lives together. At the point of arrest, bitcoin worth over **$95,000** was recovered from him. Other assets recovered were a brand-new Mercedes 350 4matic, a laptop and an iPhone 13. He was charged to court and convicted while the assets were ordered to be forfeited to the victim.

Indicators/techniques/methods

- Receiving huge funds under the disguise of Marriage
- Portraying to be an American surgeon on a UN Mission to the Middle East
- Receipt of crypto payments from unrelated entity ($95,000)
- Purchase of luxury items above individual's means
- Claiming huge expected payment ($5 million)

Jurisdictions Involved

United States of America/Nigeria

Source: EFCC

CASE STUDY 5– MONEY LAUNDERING OF PROCEEDS FROM DISASTER FRAUD

A sting operation carried out by the **EFCC** in Lagos led to the arrest of a 33-year-old man around the Lekki axis named **Mr RF**. He was involved in Covid-19 unemployment claims scam. In his possession were several foreign bank account information, emails, driver's licenses and Social Security Numbers (SSNs) of US citizens and IDs stored in Laptop and Mobile devices which he uses to prove account ownership for other scammers to receive Covid-19 unemployment funds from the Government and pays them in bitcoin (BTC). He also provided IDs for others, and when payments were made to the foreign accounts, he controlled them, taking his percentage, and remitted it to the fraudsters in BTC. Investigations revealed that the money was used to live a lavish lifestyle and to acquire expensive pieces of jewellery. He was convicted while a Mercedes Benz and some pieces of expensive jewelleries were recovered from him. Assets recovered from him were forfeited to the Federal Government of Nigeria.

Indicators/techniques/methods

- ❖ Use of several foreign bank accounts, emails, driver's licenses of US citizens and SSNs and IDs by one person
- ❖ He provides IDs for others and when payments are paid to the foreign accounts, he controls it.
- ❖ **Mr. RF** provides accounts for scammers to receive the claims and pays them in BTC
- ❖ Purchase of luxury items outside known legitimate means

Jurisdictions Involved

United States of America/Nigeria

Source: EFCC

CASE STUDY 6– IMPERSONATION AND LAUNDERING OF PROCEEDS DERIVED FROM FRAUD THROUGH CRYPTOCURRENCY

A media publication in September 2022 triggered this investigation.

A suspect presented himself as an EFCC official using counterfeit IDs and videos, which he displayed to the victim. The victim had already fallen victim to a prior fraud, and the suspect assured her that he could retrieve her lost funds. He informed her that he also traded in cryptocurrencies and could help her invest. The victim was convinced and this led her to raise funds some of which she borrowed. She bought the cryptocurrency and transferred **€45,000** into four wallets which the suspect provided.

Using the information he had provided to the victim which was also published, the EFCC arrested the suspect and an investigation revealed that he had converted money in his crypto wallet to fiat which was then used to buy shoes, clothes, wristwatches, land and live lavishly.

He was charged and convicted of Impersonation, Computer Fraud, Obtaining Money under False Presence, and Money Laundering.

Indicators/techniques/methods

- Pretence to be EFCC Official (or a person of privilege/power) with Fake IDs and Videos
- Use of different crypto wallets to receive funds from victims
- The lifestyle and activities of the suspect not in line with profile

Jurisdiction Involved

Nigeria

CASE STUDY 7– MONEY LAUNDERING OF PROCEEDS FROM ROMANCE FRAUD THROUGH CRYPTOCURRENCY AND BANK ACCOUNTS

In 2022, the **EFCC** carried out a sting operation in Lagos during which one of the suspects escaped but his brother was apprehended. Interrogations were conducted with the brother in custody who revealed his involvement in romance scams and that it was his escapee brother who provided the foreign accounts that warehoused the proceeds of their crime and proceeds shared between them. This triggered an investigation on the account of the escapee brother and a particular inflow of thirty Million Naira **N30,000,000.00** (approx. **$39,628.91 USD**) into his account aroused curiosity. Further requests for the source of the lodgement revealed a **Company A** that had a turnover of fifty-seven billion **N57,000,000,000.00** (approx**. $75,294,938.20 USD**) for the one year it was operated. Seven other companies that made huge sums of deposits to the account were also identified. **Company A's** account opening package revealed a young Nigerian lady (not part of the scam) whose other personal account showed only small credits with a monthly salary of about **N50,000** (approx. **$66.05**). The lady was arrested but she denied knowledge of the account with the **N57,000,000,000.00** (approx**. $75,294,938.20 USD**). Investigation revealed C**ompany A's** account was only a front and was created in connivance with a Chinese lady and the bank manager. The Chinese lady travelled back to China from where she operated the account by buying Cryptocurrency and making payments in Naira from this designated account. It was discovered that the escapee brother was one of those selling Cryptocurrency to this Chinese.

The Chinese woman was eventually arrested and the investigation is still ongoing.

Indicators/techniques/methods

- Use of multiple foreign accounts
- Large transfer of funds **N30,000,000** (approx. **$39,628.91 USD**) from company account in the name of a lady that earns only **N50,000** (approx. **$66.05**)
- Use of cryptocurrency to conceal proceeds of crime
- Large turnover on company account within a short period without verified business activity
- Use of front company to received proceeds from fraud
- Collusion with bank staff to create a fictitious bank account with KYC details of a third-party

Jurisdictions Involved

China/Nigeria

Source: EFCC

CASE STUDY 8– MONEY LAUNDERING OF PROCEEDS FROM FRAUD THROUGH CRYPTOCURRENCY

The **EFCC** received a complaint from an Indigenous Fintech company that provides Cryptocurrency Exchange Services reporting a loss of **Ethereum 65** worth about **$100,000**. This became evident when there was a discrepancy between their customers' deposits and payouts, and the balance didn't match during the "Sweep" process (the routine process of moving funds in depositors' crypto wallet addresses to their central hot wallet). A report was made to the Lead Technical Engineer and suddenly, a return of the **Ethereum 65** was made from a non-customer wallet.

This triggered their report to the **EFCC** and an investigation was launched accordingly. During the investigation, the suspicious transactions were traced to multiple non-custodial wallet addresses. This then was linked to the activities of most of the non-custodial wallet addresses involved in the fraud process to the cryptocurrency wallet address of the same Lead Engineer. It was discovered that the Lead Engineer edited the smart contract (an automated instruction on the Fintech Etherium blockchain) which then swept the balances from the customer wallets to his own controlled non-custodial wallet. He achieved this, having stolen their private keys.

Upon the arrest of the Lead Engineer, Forensic analysis was done on his laptop and this revealed a CSV file containing almost (300,000) users private key which he was able to perpetuate the fraud. The total loss aggregate was about **$1 million** and he restituted the Fintech Company with the said sum of money. Thereafter, the suspect was charged to court and trial is ongoing

Indicators/techniques/methods

- Abuse of office and expertise
- Transactions from different customer wallets to different non customer wallets
- Diversion of customer funds for personal gain
- Fraudulent retrieval of customer private information

Jurisdiction Involved

Nigeria

Source: EFCC

Typology 2: Use of Ponzi Schemes

CASE STUDY 9– LAUNDERING THE PROCEEDS FROM A PONZI SCHEME THROUGH A LEGAL PERSON REGISTERED AS A CRYPTOCURRENCY AND REAL EASTE INVESTMENT COMPANY

The **EFCC** received a petition from 25 victims who reported that they were defrauded by **Mr. BBD** and his cohorts in a pyramid scheme disguised as an investment business.

Mr. BBD registered company **PMZ Limited** with the Corporate Affairs Commission (CAC) having himself, his wife and sister registered as directors of the company. He went further to rent an office space in Port Harcourt which was tastefully furnished to attract unsuspecting victims. Thereafter, the suspect recruited staff whose job is to advertise the investment to the public and lure them into investing with the company. The suspect also recruited his friend **Mr. MXR** and made him the Chief Operating Officer (COO) of the company. They proceeded to open bank accounts with several commercial banks having **Mr. BBD** as signatory A, **Mr. MXR** as signatory B and the accountant as signatory C in all the company's accounts, with the mandate on the accounts allowing signatory A to sign alone. This allows **Mr. BBD** to withdraw funds from the accounts without any other of the signatories co-signing.

To sell the scheme, the company portrayed images of purported properties owned by the company and profits made. They ensured that the first set of investors received payment as return on investment (ROI) to lure more people into investing with them. **Mr. MXR** was the intermediary between the victims and the company while **Mr. BBD** was barely known. **Mr. BBD** and his accomplices laundered the victims' money by acquiring properties in their personal names and living luxurious lifestyles. They also laundered part of the funds using cryptocurrency. Investigations revealed that victims were defrauded of about **₦1 billion** (approx. **$1,320,963.82 USD**).

The prime suspect **Mr. BBD** fled the country to another African country when the victims realized they had been defrauded. His accomplices are currently being prosecuted while efforts are being made to arrest and prosecute the prime suspect.

Indicators/techniques/methods

- Newly incorporated companies advertised as investment companies with no director having any known investment experience, and not under the regulatory purview of the Securities and Exchange Commission (SEC).
- Newly opened corporate accounts receiving funds from different persons and may have narration as "investment"

- Withdrawals from bank accounts by only one signatory without regards to the other signatories.
- Funding of lifestyle from accounts of corporate entities.
- Investment companies having family members as directors.
- Transaction dynamics on accounts of investment companies that do not show inflows from return on projects executed or investments made.
- Inflows from different persons followed by outflows to different unrelated persons.
- Purchase/development of real estate meant for investment in the personal names of directors and staff of investment companies.

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 10– LAUNDERING OF PROCEEDS FROM PONZI SCHEME THROUGH CRYPTO WALLET

A petition was filed by **Mr. K. Esq**. for **ABC Union** on behalf of over 50 Nigerians against **TC Investment Ltd**, its Chairman and Managing Director. The petitioners claimed that victims were lured to invest in **TC Investment Ltd** with a minimum of **₦50,000** (approx. **$66.05**) for 20% monthly interest payment. After two months, they shut down the offices and disappeared with investor funds. Investigations revealed that Managing Director **Mr. EN** transferred **₦165,601,720.00** (**$218,753.88 USD**) from a Commercial Bank account to another corporate account. The suspect tried to launder the funds by investing in Bitcoin and pay other investors' pending investments. The case is still under investigation and possible prosecution.

Indicators/techniques/methods

- Investment of **₦50,000** (approx. **$66.05**) that would yield 20% profit monthly
- Rate of return on investment not comparable to financial market rate.
- Huge transfer of **₦165,601,720.00** (**$218,753.88 USD**) from commercial account to company account
- Use of crypto currency to launder proceeds from fraud.

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 11– MONEY LAUNDERING OF PROCEEDS FROM PONZI SCHEME THROUGH PURCHASE OF FOREIGN CURRENCY

This pertains to a reported case involving the diversion of investor funds and obtaining money under false pretences.

The **EFCC** received an Intelligence Report from the **NFIU** on a likely money laundering purported by a **Dr. XX** and the Management of **YY Asset Investment Limited**. The Intelligence alleged that **YY Asset Investment Limited** posed to be specialized in investment brokerage and management for clients but the company was neither registered with the Central Bank of Nigeria or the Securities and Exchange Commission. They raised funds from the public for investment in their diverse businesses. Based on the gathered intelligence, the management of YY Asset Investment Limited redirected the entire sum of Seven Hundred Million Naira (**N700,000,000.00**) (approximately **$924,674.67 USD**) received from investors to settle preexisting debts.

Investigations into the case revealed that the Managing Director, **XX** received funds from the seven (7) complainants to the tune of three hundred and twenty-nine million, six hundred thousand Naira (**₦329,600,000.00)** (approx. **$435,389.67**). Investigations also revealed that out of the funds received, the sum of sixty-five million, three hundred and ninety thousand Naira (**₦65,390,000.00)** (approx. **$86,377.82**) was converted to dollars and used for personal gains.

Indicators/techniques/methods

- Special Investment and Management Broker without registration with CBN and SEC
- Use of investors' funds to pay-off existing debts (**₦700,000,000.00)** (approx. **$924,674.67 USD**)
- Non-payment of return on investment nor refund of the principal
- Huge amounts of funds received from different individuals (**₦329,600,000.00)** (approx. **$435,389.67**).
- Use of currency exchanges to launder part of proceeds of (**₦65,390,000.00)** (approx. **$86,377.82)** derived from fraud.

Jurisdiction Involved

Nigeria

Source: EFCC

Typology 3: Use of Bureau De Change Operators

CASE STUDY 12– MONEY LAUNDERING OF PROCEEDS FROM FRAUD THROUGH BUREAU DE CHANGE
This deals with an alleged case of Criminal Breach of Trust and Obtaining Money under False Pretence reported to the **EFCC** on 20th October, 2020 by **Mr. R** against **XXX** and 6 others. The petitioner alleged that he was contacted by his brother **Mr. Y** who resides in London to raise the sum of six hundred and fifty-three thousand US Dollars (**$653,000**) to be delivered in Dubai on behalf of **XXX** and **ZZZ** both resident in London while they pay the equivalent in UK Pounds to his brother. The Petitioner further alleged that he paid a total sum of three hundred and seven million, twenty-nine thousand, five hundred and twenty-five Naira (**₦307,029,525.00**) (approx. **$405,574.90 USD**) to one **Alhaji B**, a Bureau de' Change Operator based on the agreement that he would facilitate the availability of the money and deliver the dirham equivalent to one **CCC**, the agent of **XXX** and **ZZZ** in Dubai. As a result **Alhaji B** through his agent **U** delivered the sum of two, million, three hundred and ninety-eight, six hundred and eighty-eight Dirham (**2,398,688AED**) to **CCC.** However, agent **CCC** transferred the naira equivalent back to Nigeria to two accounts unrelated with the transaction. Investigation revealed that Alhaji B did deliver the agreed sum through his agent **U** to **CCC** for onward delivery to **XXX** as agreed with the petitioner, however, **CCC** denied knowledge of **XXX** and **ZZZ** but rather stated that he was communicating with one J who instructed him to send the Naira equivalent of the Dirham back to Nigerian accounts. Analysis of accounts revealed that the money was exchanged between various Bureau de Change operators who were able to provide their customers except one **LAQ** who claimed to have given cash to one **Mr B** who he does not know his where about. Investigation established the predicate offences of criminal breach of trust and obtaining money under false pretence against **XXX** and **ZZZ** who initiated the transfer from the petitioner to Dubai. More so, the offence of money laundering can also be established against all the suspects who acted as vehicle for the transfer of the funds in order to conceal the origin and source of the funds. Meanwhile investigation has been concluded and the case file and is pending prosecution.
Indicators/techniques/methods

- ❖ Transfer of huge amount of funds (**N307, 029,525.00**) (approx. **$405,574.90 USD**) in Naira to Bureau de Change on behalf of a beneficiary in UK
- ❖ Conversion of Naira to Dirham (**2,398,688AED**) through a third-party Agent in Dubai
- ❖ Conversion of Dirham (**2,398,688 AED**) to Naira to a company account **T & Sons Investment Limited** in different banks **F** and **D.**
- ❖ Bureau de change operators transacting out of scope of authorized activities as stipulated by the CBN

Jurisdictions Involved

Nigeria/ UAE/UK(London)

Source: EFCC

CASE STUDY 13: LAUNDERING OF PROCEEDS FROM EMPLOYMENT FRAUD THROUGH BUREAU DE CHANGE TO PURCHASE REAL ESTATE AND VEHICLES

This deals with a written petition by one **Mr A** against **Mrs V** wherein the complainant paid the sum of **$300,000.00USD** in cash to the suspect sometime in June, 2022 to facilitate his appointment as the Managing Director of a government agency.

Investigation revealed that from the sum of **$300,000.00USD** received by the suspect, **N88,000,000.00 (approx. $116,244.81)** was used to purchase a Four Bedroom Duplex located in Abuja. The suspect also purchased two vehicles (Toyota Hilux and Toyota Venza 2020 Model) from an auto dealer located at Central Business District, Abuja in the sum of **N20,000,000.00** each. **(approx. $26,419.27).**

The implication of this revelation is that the money collected by the suspect was laundered through a Bureau De Change operator. That she used the Bureau De Change operator to pay for the said property and the vehicles. In the course of the investigation, the proceeds of crime i.e., the Four Bedroom Duplex and the two vehicles which are; Toyota Hilux and Toyota Venza 2020 Model were recovered from the suspect.

Iinvestigation has since been concluded and the case file has been forwarded to Legal and Prosecution Department for vetting and advice.

Indicators/techniques/methods

- Employment Scam
- Laundering of proceeds of crime for the purchase of assets.
- Bureau De Change Operator (third party) facilitated the acquisition of assets for the suspect

- Criminal Diversion of funds using Legal entity

Jurisdiction Involved

Abuja, Nigeria.

Source: EFCC

CASE STUDY 14– LAUNDERING FUNDS DERIVED FROM LOVE SCAM THROUGH BUREAU DE CHANGE OPERATORS

The **EFCC** received a Mutual Legal Assistance request from the **Swiss Federal Council** in respect of one of its citizens **Ms DSF**. The case involved a suspect **Ms. MDC,** a female based in Nigeria who posed as a male and was communicating with **Ms DSF** through a love dating application. A romantic relationship was established with a promise made by **Ms. MDC** to marry **Ms. DSF**. Ms. MDC exploited the trust established with Ms DSF by extorting funds continuously demanding financial support under the guise of running a charity organization.

To facilitate the fraud, **Ms. MDC** opened a joint bank account with her aged father where the proceeds were paid into. She laundered the proceeds of the crime through Bureau de Change Operators with the help of her father. **Ms. MDC** absconded to a foreign country with part of the laundered funds while her father has been arrested, convicted and part of the funds recovered.

Indicators/techniques/methods

- Inflows from foreign jurisdictions to unrelated accounts with narrations such as “support”, “charity”, “help”
- Inflows from foreign jurisdictions followed by outflows to accounts of Bureau de Change Operators
- Newly opened accounts receiving funds from foreign jurisdictions
- Receipt of funds in high velocity from sender whose relationship with beneficiary is not established

Jurisdictions Involved

Switzerland/Nigeria

Source: EFCC

Typology 4: Use of Bank Accounts to Launder Proceeds of Fraud

CASE STUDY 15 – MONEY LAUNDERING OF PROCEEDS FROM BUSINESS EMAIL COMPROMISE THROUGH BANK ACCOUNTS
The **EFCC** received an intelligence report from the United States **Federal Bureau of Investigation (FBI**), in relation to case bordering on conspiracy, money laundering and obtaining money by false pretence. The intelligence revealed that the suspect **Mr MM** is into various forms of internet fraud including Business Email Compromise (BEC), Bank Fraud and Wire Fraud. It further alleged that evidence recovered from the mobile phone of **Mr NT** who was arrested and investigated by the agency (**FBI**) indicated that **Mr. MM** plays a prolific role in laundering proceeds of criminal activities between Nigeria and United States of America. On receipt of the intelligence, investigation commenced into the lifestyle and activities of the suspect. He was subsequently arrested by the **EFCC** and several accounts linked to him were placed on (Post No Debit)[22] while a total of thirty-four thousand dollars (**$34,000**) was subsequently recovered from the suspect. On conclusion of the investigation, the suspect was convicted at the High Court of Justice while the recovered money was forfeited to the **FBI** for onward transmission to the victims in the United States of America.
Indicators/techniques/methods • Use of multiple bank accounts • The lifestyle and activities of the suspect not in line with profile of suspect in KYC information • Wire transfers between Nigeria and United States • Transfers from foreign jurisdictions **Jurisdictions Involved** United States of America/ Nigeria

Source: EFCC

[22] "Post No Debit" is a banking term indicating a temporary restriction on a bank account, during which no debits or withdrawals are permitted for a specified time.

CASE STUDY 16– LAUNDERING CRIMINAL PROCEEDS FROM IDENTITY THEFT THROUGH BANK ACCOUNTS BY AN ORGANISED CRIMINAL NETWORK

The NFIU received a spontaneous disclosure from the **Financial Crimes Enforcement Network (FINCEN)** following investigations conducted by the **Federal Bureau of Investigation (FBI)** on **Mr. PD** and **Mrs. PD.** The **NFIU** generated an intelligence report which was sent to the EFCC for investigations.

The **FBI** alleged that the suspects, a married couple residing in the USA initiated and perpetuated a significant money laundering scheme, defrauding over 150 victims primarily in the USA and transferred substantial amount of the proceeds to Nigerian bank accounts belonging to one **Ms. ACE**.

The **EFCC** commenced investigation by through a cash flow analysis of the bank statements where various inflows from the suspects were traced to. It was revealed that **Mr. PD** usually instructs **Ms. ACE** to transfer funds to various people one of whom was **Mr. LE**, who was eventually arrested. Further investigations into **Mr. LE** revealed that he was an internet fraudster who stole the identity of one **LS** a United States of America citizen to defraud **Ms CC**., also an American citizen, of the sum of **$11,500** received through cash mailing.

The **EFCC** recovered the sum of **$11,500** from **Mr. LE** and he has been convicted of impersonation and was sentenced to five years imprisonment with an option of fine while the recovered money was restituted to the victim.

Indicators/techniques/methods

- Frequent and significant inflows to bank account from different offshore accounts
- Offshore inflows followed by transfers to different domestic parties
- Transactions not in line with profile of accounts

Jurisdictions Involved

United States of America/Nigeria

Source: EFCC

CASE STUDY 17– ROMANCE SCAM AND MAIL PHISHING

A petitioner, **RB** allegedly met one **MK**. (whose real identity is **FB**) on a dating site called "Plenty of Fish" and a romance scam was initiated which led **RB** to send 5 bitcoin transactions totalling **32,130CAD** to the said **MK**.; 5 wire transfers to JS totalling **21,347.21 CAD** and 4 wire transfers to **FB** totalling **23,859.50 CAD** between November 2019 and February, 2020.

Investigations established that the complicit mule, **JS** received the cumulative sum of **$21,347.21USD** through his account in Turkey from the victim, **RB**. Through intelligence gathering, his identity was unravelled and his bank account in Nigeria was identified. Analysis of the statement of account of **JS's APY Bank of Nigeria** account revealed that the suspect used Alternative Remittance System (a.k.a Hawala) to transfer the naira equivalent from his Turkish account, in the cumulative sum of **₦4,918,550.00** (approx. **$6,497.23USD**) with misleading transaction descriptions (such as "house rent", "fees for house rent" and "flight ticket") to **FB's** account in Nigeria, and retained a 30 per cent of the inflow being **$21,347.21USD** (based on estimation).

Also, analysis of **FB's** Nigerian account revealed that the five-bitcoin transaction inflows he received from the victim, **RB** using a fictitious identity (**MK**.) were sold to one **JF** who confirmed this upon his arrest as he (**JF**) made cumulative deposit in the sum of **₦6,986,000** (approx. **$9,228.25USD**) to FB's bank account.

Furthermore, to launder the proceeds of his criminal activities, **FB** withdrew the cumulative sum of **$23,859USD** he received directly from the victim into his USD domiciliary account in Nigeria via cash and exchanged using the services of different Bureau de Change operators to the tune of **₦6,256,250** (approx. **$8,264.28**). The funds were subsequently deposited in his naira account by the Bureau de Change operators.

Although, the principal suspect, **FB** is still at large, effort is being intensified to apprehend him. However, his accomplice, JS who received the cumulative sum **$21,347.21 CAD ($16,300 USD)** has been apprehended, and the said amount received was recovered from him.

Indicators/techniques/methods

- Receipt of multiple payments from the victim into bank account of suspect without clear justification for payments
- Naira equivalent in the cumulative sum of **₦4,918,550.00** (approx. **$6,497.23USD**) from his bank account with misleading transaction descriptions (such as "house rent", "fees for house rent" and "flight ticket") to that of FB's account.
- Withdrawal of cumulative sum of **$23,859** he received directly from the victim into his USD domiciliary
- Bureau de change operators transacting out of scope of authorized activities as stipulated by the CBN

Jurisdictions Involved

Turkey/Nigeria

Source: EFCC

CASE STUDY 18– MONEY LAUNDERING OF PROCEEDS FROM CONSPIRACY AND CRIMINAL CONVERSION OF FUNDS THROUGH THE BANKING SYSTEM

This deals with a report of financial fraud made to the Economic and Financial Crimes Commission by **Comrade J** of **a civil society** against the Group Chairman of a commercial holdings company, **Mr. A**, Bank Officials of Bank BR.

The Petitioner (**Comrade J**) alleged that the Principal Suspect **Mr. A** has perpetrated dubious financial fraud using the Commercial Bank shareholders' and customers' funds without recourse to CBN guidelines and the Bank's internal procedure. He further alleged that the suspect in connivance with top management of the Bank approved unsecured loans valued at eighteen million Naira (**₦18,000,000.00**) (approx. **$23,777.35 USD**) to Companies that he had interests in. It was further alleged that Mr. A forced the former GMD of the Bank to write off a debt of twenty-six million Naira (**₦26,000,000.00**) (approx. **$34,345.06 USD**) he collected from the Bank's Trustees Limited without the knowledge and consent of the Bank.

The findings of the investigation indicated that a prima facie case of Conspiracy, Criminal Conversion of Funds can be substantiated against the suspects. Investigation revealed that all the loans were not utilized for the purpose they were meant for, thus the funds were obtained under false pretences. The fraud was perpetrated using the shareholders and customers funds during the tenure of **Mr. A,** the Chairman, the Group Managing Director **Mr. B** and **Mrs. C** the Executive Director of Bank **BR** in Nigeria without regard to due process.

Further investigation unearthed loans disbursed to **Company TK Limited** to the tune of (**₦6,412,000,000.00)** (**approx**. **$8,470,020.06USD**) were laundered using several 3rd party accounts linked to **Mr. A** which he converted for his personal use. It was also established that **Company TK Limited** issued loans to three other companies in a drive to liquidate the exposure following the directives of **Mr. A**. It was further discovered that in like manner, that an associate of **Mr A**, **Mrs. UU** through three companies acher Companies- **CB Limited**, **OJ Nigeria Limited** and **OO Energy Limited** s

The total sum of (**₦6,500,000,000.00**) (**approx. $8,586,264.88USD**) has been fully recovered from the main suspect, **Mr. A** and same released to the Management of the Commercial Bank Nigeria Plc. while, the total sum of (**₦168,000,000.00**) (approx. **$221,921.92USD**) was recovered from Mrs.

UU leaving the outstanding sum of (**₦5,882,000,000.00**) (**approx.$7,769,909.24USD**) traced to her Companies

Indicators/techniques/methods

- Using the Commercial Bank shareholders and customers funds contrary to CBN guideline and the Bank's internal procedure.
- Approval of unsecured loans valued at (**₦18,000,000.00**) (approx. **$23,777.35 USD**) to Companies that Mr. A has vast interest in.
- Writing off a staggering amount of (**₦26,000,000.00**) (approx. **$34,345.06 USD**) collected by **Mr A** from the Bank's Trustees Limited without the knowledge and consent of the Bank.
- Loans collected were not utilized for the purpose they were meant for; thus, the funds were obtained under false pretences.
- Loans disbursed to the tune of (**₦6,412,000,000.00)** (approx. **$8,470,020.06USD**) were laundered using the accounts of **HO Limited**, **H Flour Mills Plc**, **H Group Limited** and **H Oil and Gas Limited**

Jurisdiction Involved

Nigeria

Source: EFCC

Typology 5: Laundering of Funds from Chargeback Fraud

CASE STUDY 19 – LAUNDERING FUNDS DERIVED FROM CHARGEBACK FRAUD THROUGH AGENCY BANKING

ANX Limited submitted a petition to the EFCC, accusing certain individuals of defrauding the company through the use of chargeback schemes. The complainant alleged that during its audit in October, 2021, it noticed various unauthorized chargeback resulting from a network glitch. Upon investigation, it was discovered that the company lost **₦1.1 Billion (approx. $1,453,060.21 USD)** of which **₦294,165,200.00** (**approx. $388,581.59 USD**) impacted accounts domiciled in Benue and Nasarawa States.

Investigation carried out by the **EFCC** established that the suspects are part of the syndicate that are into funds transfer scams using dispense error popularly known as chargeback; a Money Laundering Scheme where structured payments below threshold are debited from an account, returned and then debited finally to several accounts in piecemeal making it look like everyday transactions with the POS as a the most preferred means of withdrawal by the ultimate

beneficiaries. Four of the POS Agents within the Northern Region accounted for 82% of the total chargeback totalling **N834 Million (approx. $1,101,683.83 USD)**

Indicators/techniques/methods

- Structured reversed transactions which are moved across several accounts
- Multiple account transfers from a corporate account to accounts of agent banks
- Structured payments below threshold

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 20 – STR ON CHARGEBACK FRAUD USING BANK ACCOUNT

The **NFIU** received a suspicious transaction report from a financial institution on a client **Mr. XY**. The financial institution observed a cycle of who receives an unjustifiable inflow from a specific merchant as reversal with narration as chargeback, following which funds were withdrawn immediately.

Analysis revealed that Mr XY purchased products online using his credit card, but would request for reversals claiming that purchases were made without his approval or the product requirement and standard was not reached. Analysis also showed that **Mr. XY** opened this account primarily for the purpose of chargeback in order to be mining his fraudulent claims and proceeds.

Indicators/techniques/methods

- ❖ Reversed narrated as "Chargeback "amount was withdrawn instantly.
- ❖ Account reveals several other similar reversal transactions with same pattern
- ❖ Information on Subject shows different contradicting information
- ❖ No economic Justification for transactions
- ❖ Constantly, claims that the purchase was made without his approval or the product requirement and standard was not reached
- ❖ Some of the reversals have no corresponding outflow transaction.
- ❖ The reversals were all immediately withdrawn through POS.
- ❖ The nature of the inflow and the speed of withdrawal appears to be suspicious

Jurisdiction Involved

Nigeria

Source: NFIU

CASE STUDY 21 – STR ON LAUNDERING PROCEEDS OF CHARGEBACK FRAUD THROUGH POS OPERATORS
In an STR filed with the **NFIU**, it was reported that **Mr. AOG** established a banking relationship with Bank **W**. On 06/06/2022, **Mr. AOG** made an online purchase of two items worth **₦399,000.00** (Three Hundred and Ninety-Nine Thousand Naira Only) (approx. **$527.06USD**) in 2 (Two) tranches and suddenly, on 16/06/2022 same amount was reversed, and withdrawn instantly. It is noteworthy that **Mr. AOG** runs a Barbing Business with a total annual turnover not exceeding **₦500,000.00** (Five Hundred Thousand Naira Only) (approx. **$660.48USD**). A review of **Mr. AOG's** account further revealed six other similar reversal transactions with the same pattern indicating that **Mr. AOG** may be violating the protection policy of online merchant and forcefully receiving chargeback after goods were received. Total inflow and Outflow stood at **₦7,050,500.00** (approx. **$9,313.46 USD**) and ₦7,329,500.00 (approx. **$9,682.00USD**) respectively as at the time of the report. Also, thirty three percent (33%) of the inflow comes from the **Mr. AOG's** account from other Banks, while Sixty Seven percent (67%) comes from different POS agents, Similarly, all outflow were made through Several POS agents.
Indicators/techniques/methods ❖ Reversed amount was withdrawn instantly. ❖ Account reveals six other similar reversal transaction with same pattern ❖ Information on Subject shows different contradicting information ❖ No economic Justification for transactions ❖ Receiving charge back after goods were delivered. **Jurisdiction Involved** Nigeria

Source: NFIU

Typology 6: Laundering Proceeds from Business Email Compromise (BEC) Fraud

CASE STUDY 22– Business Email Compromise (BEC)
The **NFIU** in its intelligence report to the **EFCC** stated that it received a spontaneous disclosure from a sister FIU involving **KV Ltd** and **CB Ltd** related to a Business Email Compromise matter. The report notes that three wire transfers totalling **$80,000USD** were sent to the bank accounts of the mentioned entities domiciled in two commercial banks on 12th, 14th and 15th May 2020 by O Bank in the USA. The victims alleged that unknown subjects used different domains and cloned a letter

in a company's name to pose as employees working for the company and sent wiring instructions to the company's tenants.

Investigation revealed that the receiver of the **$80,000USD** is one **LR** who was dating one of the suspects **JL**, and who used her account as collection account for the proceeds of her boyfriend's criminal activities. On receiving these funds, she wired **$55,000USD** and **$25,000USD** to two Nigerian companies, **VL Ltd** and **BB Ltd** respectively.

The operator of **VL Ltd** sold the **$55,000USD** he got to a money exchanger, **DNM Ltd** through a middle man named **JS**. **DNM Ltd** sent **₦11,000,000.00** (**approx. $14,530.60USD**) through the same middle man and ₦12,600,000.00 (**approx. $16,644.14**) directly to **VL Ltd** Naira account. On receiving this total sum of **₦23,600,000.00 (approx. $31,174.74USD)**, **VL Ltd** transferred **₦10,500,000.00 (approx. $13,870.12USD**) to the bank account of **LR's** boyfriend, **JL,** whom paid **₦7,138,282.00** (**approx. $9,429.41USD**) for a duplex bought in JL father's name; and transferred **₦5,700,000.00** (**approx. $7,529.49USD**) to an unknown individual.

For the **$25,000** received by **BB Ltd**, the owner of **BB Ltd**, **Mr P** transferred **₦4,250,000.00 (approx. $5,614.10USD)** from his personal bank account (not from **BB Ltd bank** account) to **JL's** bank account and **₦6,000,000.00 (approx. $7,925.78USD)** to the **JL's** sibling account in order to obfuscate the paper trail.

On this basis, **JL** is the principal suspect who defrauded the two companies, **KV Ltd** and **CB Ltd** and all the other entities and individuals assisted him in laundering the proceeds.

Indicators/techniques/methods

- Use of BDC to quickly change foreign currency received from foreign jurisdiction
- Use of a third-party account for collection of transfers from foreign jurisdiction and distribution in domestic accounts
- Receiving payments in foreign currency without corresponding business activity or sale of goods
- **Jurisdictions Involved**

United State of America/ Nigeria

Source: EFCC

CASE STUDY 23– MONEY LAUNDERING OF PROCEEDS FROM BUSINESS EMAIL COMPROMISE THROUGH BANK ACCOUNTS

Following a tip-off from reliable sources, the operatives of **EFCC** Advance Fee Fraud Section, Headquarters on the 31st May, 2023 raided a property in Abuja, Nigeria where three (3) suspects were arrested amongst them is one **YO** who is in custody.

Investigation conducted so far has been able to reveal that the suspect together with a syndicate diverted **$210,525.20** belonging to company based in the USA as part payment for a **$500,000** transaction in a BEC Scheme. The suspect as a middleman in the above transaction provided a USA bank account details gotten from another co-conspirator based in Dubai which was used to receive the funds.

The said sum passed through another account before it was paid in Dirham to a Dubai exchanger provided by the main suspect. **YO** was further credited a sum of **₦2,089,000.00(approx. $2,759.49)** as his share from the transaction into his account

Indicators/techniques/methods

- Use of false email address that looks authentic with the aim to receive funds
- Use of multiple bank accounts
- The lifestyle and activities of the suspect not in line with profile
- Wire transfers from parties not-related to subject
- Transfers from foreign jurisdictions for unjustifiable reason
- Transfer to Currency exchanger in a foreign country

Jurisdictions Involved

(Dubai) UAE/Nigeria

Source: EFCC

CASE STUDY 24–BUSINESS MAIL COMPROMISE AND MAIL PHISHING

In a joint investigation with the **FBI** in 2021, the **EFCC** received a report that through Business Email Compromise, an **ANV** business had lost **$1 million**. The suspects had set up a domain and a mailing service that appeared similar to that of the American company's business partner **company A** was meant to make payments for services rendered by its business partner.

The **A company** received a second mail purported to have come from its business partner requesting that the money be paid in a designated account so that they can avoid excessive taxes.

Preliminary investigation revealed that the IP address was a VPN and the email to the domain linked with the details of the subscriber paying for the hosting which was linked to the social media accounts of one of the perpetrators here in Nigeria. With the full name known, Bank Verification Number (BVN) profiling was conducted which revealed all the bank accounts of the suspect. Hence, letters of investigation were done to the banks and responses received were duly analysed after which the suspect was arrested and his arrest led to the apprehension of the second accomplice, a Nigerian who live in Country DCX. He was also arrested in a high-brow area of HX State. The second accomplice provided the account details into which the Country **A Company** made payment of **($1) million** and he said it was gotten from a Country L National. The ($1) million was shared among the three i.e., the two suspects and the National of Country L. The First suspect used the share of the proceeds of crime to travel to DCX, purchase luxurious pieces of jewellery, buy cars and reside in posh areas in HX State. The second suspect used his portion to relocate to Country S. Some recoveries in assets and cash have been made from the two suspects who are being prosecuted, while the L National is still at large.

Indicators/techniques/methods

- Use of proceeds of crime for travels, purchase of luxurious pieces of jewellery, cars and rent or purchase high end property
- A domain and a mailing service that appeared similar to that of the Country A company's business partner

Jurisdictions Involved

United State of America/ Nigeria

Source: EFCC

CASE STUDY 25 – MAIL FRAUD BUSINESS AND E-MAIL COMPROMISE AND MAIL PHISHING

In the joint investigation with the **FBI** in 2021, a of loss of over **$1.4 million** from a university in the United States of America to Business Email Compromise was received. The University carrying out a construction project had engaged a local contractor and at the point of making certain payments, the school received an email purported to have come from the real contractor stating that they wanted the money wired to a preferred account in another state. The University made the payment accordingly and when this was done. The university realized it had been defrauded when the real company/ contractor kept asking for its payments.

Investigations revealed that the money in the account in Texas had been wired to a domiciliary account in Country N in two tranches.

The receiving account, A then depleted **$800,000** to a Bureau De Change (BDC) Operator and then withdrew the balance in tranches. From the account of the BDC Operator, the monies were further moved to the cronies of the owner of account A. An arrest of the BDC operator led to the apprehension of the suspect **A**, who feigned that he was a real estate operator and had dealings with one **Mr. AD**, who made the payments to him from the **Country U**.

With no evidence to support his claims, it was discovered that he had a similar case in the Abuja office but was unable to withdraw the money before he got caught up.

It was also discovered he had been convicted in the US for Wire Fraud. Assets traced to the crime included a house, (8) cars and two haulage trucks, and some money in the bank which are on temporary forfeiture pending the outcome of the ongoing trial.

Indicators/techniques/methods

- Use of false email address that looks authentic with the aim to receive funds
- Continuous transfer of foreign currency to BDC after receiving payment from foreign jurisdiction
- No prior history of business activity leading to receiving significant amount of foreign currency from foreign jurisdiction
- Nature of business activity cannot be ascertained or matched with foreign currency received from foreign jurisdiction
- Account owner had previously been convicted for Wire Fraud in the United States of America

Jurisdictions Involved

United States of America/ Nigeria

Source: EFCC

Typology 7: Fraud in Relation to Trade Based Money Laundering

CASE STUDY 26 – FORGERY AND TRADE BASED MONEY LAUNDERING

In 2020, The Lagos Command of the **EFCC** received a report from a local bank on an alleged **$15 million** trade-based Money Laundering carried out using a Form M processed on behalf of a customer who is a clearing agent. He had under-declared on the Form M by filling information for **$90 000** worth of vegetable oil products. He however presented the same Form M for customs

clearance and documentation to enable clearance of 140 metric tons of margarine worth **$15 million**. He had two customers who engaged him to clear their goods but he criminally intended to use a single Form M for the **$90,000** worth of goods. He ultimately wanted to avoid paying duties for the 140 metric tons of goods worth **$15 million**.

The goods were impounded by the Nigeria Customs Service and he was issued a Debit Note for not declaring the 140 metric tonnes. The actual customer had to pay an agreed rate after having been cleared as he was not criminally involved. The clearing agent was charged to court for forgery and was convicted.

Indicators/techniques/methods

- Use of the same form M form (of **$90,000** vegetable oil) to clear different products (140 metric tons of margarine) worth **$15 million**
- The clearing agent had under-declared on the Form M by filling information for **($90 000**) worth of some vegetable oil products

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 27 - USE OF LOCAL PURCHASE ORDERS FOR FRAUD

The NCB received a petition from a Financial Institution incorporated in Nigeria. The complainant noted that it was approached by a company registered in Nigeria to finance two Local Purchase Orders (LPO) for a governmental organization to supply twenty armoured vehicles. Consequently, the sum of **N330,000,000** (**approx. $435,918.06**) and **$500,000** LPO finance facility was disbursed to the company for execution of the contract. Domiciliary arrangement was also put in place to ensure payments for the contract were made directly to the Financial Institution. However, four years later, the suspect informed the Financial Institution that the vehicles bought with the disbursement were held by authorities at Dubai, United Arab Emirates for inability to provide End User Certificate.

The suspect in this matter was discovered to have deliberately intended to defraud the Financial Institution as there were no cars intercepted in Dubai as claimed. Further investigation also revealed that the organization which awarded the contract revoked his contract along the line for failure to meet up with the deadline.

Indicators/techniques/methods

- ❖ Use of LPO from government organisations to appear legitimate
- ❖ Sourcing supply of specialised vehicles at foreign jurisdictions known for very high cost of shipment
- ❖ Extended delay in execution of contract without justification

Jurisdictions Involved

United Arab Emirates/ Nigeria

Source: INTERPOL-NCB

CASE STUDY 28– TRADE BASED MONEY LAUNDERING IN RELATION TO AGRICULTURAL EQUIPMENTS

Investigations carried out by the United States Government revealed a case of trade-based money laundering involving two suspects of Nigerian origin and a prominent US-based company specializing in the sale of farming equipment and precision cutting tools.

The two suspects, between 2014 and 2020, deceived victims by convincing them to transfer money into the account of the US-based, under the guise of purchasing farming tools. Subsequently, the tools were shipped to Nigeria and sold for substantial amounts for their personal gains.

Investigations revealed that the company did not comply with US AML legislations by receiving funds from numerous depositors that were unrelated to the recipient of the invoice and cargo, thereby unknowingly warehousing funds of defrauded entities.

The US government however was able to ascertain that the company was not accomplice in the fraud scheme, rather was exploited as a result of its lax policies on customer due diligence, which allowed the suspects to exploit the company's operations for the purpose of collecting fraud proceeds.

The company avoided prosecution by agreeing to pay a $1.7 million for unintentionally serving as an intermediary for two Nigerian suspects.

Indicators/techniques/methods

- ❖ Receipt of funds from different entities unrelated to the invoice or recipient of the agricultural products.

Jurisdictions Involved

Nigeria/ USA

Open Source

Typology 8: Fraud in Pension Funds Administration

CASE STUDY 29– MONEY LAUNDERING OF PROCEEDS FROM CRIMINAL CONSPIRACY, BREACH OF TRUST, FRAUDULENT CONVERSION OF PENSION FUNDS, THEFT

A written petition dated 16th October, 2020 signed by **OA** for **XXX Pensions Limited** against **Mr. JD** & Others. The petitioner alleged that the suspects fraudulently converted funds meant for next-of-kin to deceased clients of **XXX Pensions Limited**. Their modus operandi is to invite the next-of-kin of deceased clients and collect necessary documents to facilitate the payment of the death benefits of their principal. The documents collected are then utilized to open fraudulent accounts with various banks. That they then inflate benefits meant for the next-of-kin and ask them to transfer the excess to their company. It was further alleged some benefits were paid to some fraudulent accounts which does not belong any next- -of-kin and the account holders were instructed to transfer the funds also to the suspects' companies' accounts. That the total sum of **₦94,033,000.00** (**approx. $124,214.19USD**) was discovered to have been fraudulently diverted, hence the petition. Upon receipt of the petition, the complainant was invited, he reported and volunteered his statement. BVN search was conducted on the suspects' and all accounts linked were retrieved. Letters of investigation were written to Corporate Affairs Commission (CAC), Securities & Exchange Commission (SEC), and twelve (12) commercial banks respectively requesting for the registration details of the companies, as well as the account opening packages and statement of accounts of the purported Next-of-Kin. Responses were received and analysed. Investigations revealed that the total sum of **₦129,821,209.00** (**approx.$171,489.12USD**) was fraudulently diverted between December 2014 to September 2017. The suspects were invited to the station during which they volunteered their statements under caution and were subsequently released on administrative bail to reliable sureties. The sum of **₦83,907,661** (**approx. $110,838.98USD**) was recovered and same released to the complainant on bond.

Preliminary findings revealed the following facts;

i. That the 2nd suspect; was a staff **XXX Pensions** in the Business Development Department; manning A, T, G and B States.
ii. That he is also the Managing Director SG Services limited.
iii. that as the field officer, his responsibilities include interacting with next of kins of deceased clients and also collecting all necessary documents to facilitate the payment of benefits for onward submission to the **XXXX Pension Headquarters**.

iv. That he fraudulently opened bank accounts in two (2) banks using several aliases as purported next of kins to deceased clients of the complainant.

v. That the accounts fraudulently received a total sum of **₦129,821,209.00** (**approx.$171,489.12USD**) as benefits for deceased clients from the complainant.

vi. That he instructed the recipients to transfer the funds to his company, SG Services Limited's with one of the commercia banks.

vii. That he transferred the sum of **₦104,375,891.00** (**approx. $137,876.77USD**) to a third party**, MJ** while retaining the balance of **₦25,445,318.00** (**approx. $ 33,612.34**) as his own share of the largesse.

viii. That the third party, **MJ** is the promoter of **MC Society Limited** and was also the Head of Benefits Administration Department of **XXX Pension Limited**.

ix. That **MJ** transferred the sum of **₦40,848,750** (**approx. $53,959.72USD**) to a Bureau De Change (BDC) company named **HS Nigeria Limited**.

x. That the prime suspect also transferred the sum **₦37,165,779.00 (approx. $49,094.65USD)** to the 3rd suspect as his share and retained the balance.

xi. That the 3rd suspect was the database administrator and information Technology expert and a former staff of the complainant.

xii. That the 3rd suspect abused his office by using his expertise to inflate balances of deceased clients in connivance with the prime suspect.

xiii. That the prime suspect continued using the 2nd suspect to perpetrate the fraud for two years despite the 2nd suspect being sacked by the complainant.

That a Honda Vehicle and a landed property were recovered from the 3rd suspect by the petitioner who later informed the Team.

Indicators/techniques/methods

- Opening of various fraudulent accounts with clients' documents
- Inflating pension benefits of deceased clients
- Payment of funds to fraudulent accounts that do not belong to clients next of kin
- Transfer of funds from clients to pension staff company accounts
- Suspects are the managers of business accounts (SG Services)
- Suspects are promoters of cooperative societies (ALC Society, MC society)
- Abuse of office by accessing privilege information on clients

- ❖ Suspects are all from the same organization XXX Pensions
- ❖ Transfer of Large sums to BDC - **~~₦~~40,848,750** (**approx. $53,959.72USD**)
- ❖ Purchase of property and vehicle

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 30– MONEY LAUNDERING BASED ON AN ALLEGED CASE OF PENSION FRAUD, ABUSE OF OFFICE (CRIMINAL BREACH OF TRUST) AND GRATIFICATION.

This is a case of Pension Fraud and abuse of office by a government officer.

The Pension Transitional Arrangement Directorate (PTAD) received complaints from a pensioner and a next-of-kin of a deceased pensioner, reporting unsolicited calls from an unidentified individual demanding a processing fee to expedite the payment of arrears owed to the pensioners.

The complaints were forwarded to the EFCC to investigate. The investigation exposed the unidentified caller to be T. Uche, a Federal Auditor posted to PTAD from the Office of the Auditor General of the Federation. Investigations further revealed that the suspect exploited information available in pensioners files and demanded funds to process their entitlements. The suspect provided the account details of one Chukwu O, a nephew to his wife, as a collection account to receive the payments.

Analysis of the account of Chukwu O revealed an aggregate credit of **One Million, Six Hundred and Sixty Thousand, Nine Hundred and Thirty Naira** (N1,660,930.00) **(approx. $2,194.0)** being the proceeds of crime from pensioners and next of kin of pensioners between 15th December, 2017 and April, 2018. Analysis also revealed a cash withdrawal of **Seven Hundred and Thirty-Nine Thousand Naira** (N739,000.00) **(approx. $976.1)** on 6th April, 2018 by D. Chukwu O. from his bank account and a corresponding cash deposit of **Eight Hundred and Sixty Thousand Naira** (N860,000.00) **(approx. $1,136.0)** paid into the T. Uche's account with the same bank.

During interrogation, the principal suspect T. Uche admitted to collecting money as "appreciation" from some pensioners whom he had helped to process their pension benefits.

Case is currently being prosecuted in the court of law.

Indicators/techniques/methods

- ❖ Phone calls to pensioners to pay a processing fee

- ❖ A third-party account is utilized to store funds, effectively introducing a degree of separation between the suspect and the proceeds of the crime.
- ❖ Cash deposits from the third-party's account into the suspect's account within the same bank are made with the intention of circumventing an audit trail

Jurisdiction Involved
Nigeria

Source: EFCC

Typology 9 Money Laundering by Organised Criminal Groups

CASE STUDY 31 – FORGERY AND TRADE BASED MONEY LAUNDERING

Three suspects were arrested in Lagos, Nigeria in 2020 following a joint INTERPOL-Group-IB and **Nigeria Police Force** cybercrime investigation. The Nigerian nationals were believed to be members of a wider organised crime group responsible for distributing malware, carrying out phishing campaigns and extensive Business Email Compromise scams. The suspects were alleged to have developed phishing links, domains, and mass mailing campaigns in which they impersonated representatives of organisations. They then used these campaigns to disseminate 26 malware programmes, spyware and remote access tools.

These programmes were used to infiltrate and monitor the systems of victim organisations and individuals, before launching scams and syphoning funds. According to Group-IB, the prolific gang was believed to have compromised government and private sector companies in more than 150 countries since 2017. Group-IB was also able to establish that the gang is divided into subgroups with a number of individuals still at large.

Investigation of the money trail revealed that the suspects used the bank and cryptocurrency accounts of their foreign counterparts to receive payment. Further investigation revealed that the suspects used a bank account provided by their counterparts in the UK, US and Thailand to receive criminal proceeds from victim companies. The suspects have been charged with unlawful interception, computer-related fraud, advance fee fraud, and money laundering. So far, a Mercedes Benz has been confiscated & suspects' accounts have been frozen and undergoing forfeiture in court.

Indicators/techniques/methods

- ❖ Use of bank accounts and crypto wallets of members from different parts of the world (cross border transactions).

- ❖ Multiple inflows from different and unrelated parties to single accounts mostly from different jurisdictions.
- ❖ Purchase of luxury vehicle.

Jurisdictions Involved

Nigeria, UK, US, Thailand

Source: INTERPOL-NCB

CASE STUDY 32 – TRADE-BASED MONEY LAUNDERING & PROFESSIONAL MONEY LAUNDERING FACILITATION BY ORGANISED CRIMINAL GROUPS INVOLVED IN FRAUD

On 27th December 2022 the **INTERPOL-NCB** received a message through the Financial Crime and Anti-Corruption Centre from **INTERPOL Dublin** on a case of trade-based money laundering amounting to **1,706,521 Euros**.

The case involved a company **MPZY Technologies** registered in Nigeria which receives goods bought by proceeds of money laundering and fraud from **LSDU** a pharmaceutical company incorporated in Dublin, Ireland.

Mr. ODF orders goods for his company **MPZY Technologies** from **LSDU** in Dublin and then sends the invoice to **HBLA Ltd**, a Dublin-registered company owned by Nigerians which he was introduced to that carries out forex transactions. **Mr. ODF** was reported to have subscribed to the services of **HBLA Ltd** as a means of settling his invoice due to CBN's policy on restriction of forex sale and he was beginning to record losses as a result of not consistently supplying products in Africa.

The Directors of **HBLA Ltd** who are part of a Nigerian confraternity, the **Neo Black Movement of Africa** otherwise known as **Black Axe** facilitate the payment of the forex payment to **LSDU**.

Investigations revealed that members of the organised criminal group having defrauded people from accross 3 countries (especially China and Germany) received funds into bank accounts opened with fake documents in Dublin. They then proceed to withdraw the funds using ATM cards and deposit the funds in another account from which they make transfers to **LSDU** to settle the invoice sent by **MPZY Technologies**. While **HBLA Ltd** presents itself to be into forex, there was no evidence or direct payments from the company's account or personal accounts of its directors to settle the invoices, rather the accounts operated by the organised criminal group was used to make the payments to **LSDU**. **Mr. CVLD**, a member of the organised criminal group was arrested in Dublin and provided useful information on the operations of the group.

Further investigations in Nigeria revealed that **Mr. JK** whom is believed to be a member of the criminal group and **Ms. YD** who is his mistress operate Naira bank accounts from which the Naira equivalence of payments for the invoices are made by **MPZY Technologies** after which they are transferred to Naira accounts operated by directors of **HBLA Ltd**. **Ms. YD** informed investigators that her boyfriend **Mr. JK** whom is married and is a citizen of Ireland asked her to open the bank account and handover the details to another lady in Dublin **Ms. LLA** as part of requirements for her to secure a visa to Europe stating that there has to be evidence of huge transactions on the account for the embassy to consider her visa application.

Investigation on the matter is ongoing with efforts in place to arrest the **Mr. ODF** the MD/CEO of **MPZY Technologies** who is allegedly out of the country on medical grounds.

Indicators/techniques/methods

- Trade-based money laundering
- The criminal group utilizes a complex layering process to obscure the origin of the funds by receiving funds into bank accounts opened with fake documents in Dublin, withdraw the funds using ATM cards, and then deposit the funds into another account.
- **HBLA Ltd**, a Dublin-registered company owned by Nigerians, acts as an intermediary. It presents itself as a forex company, but there is no evidence of direct payments from the company or its directors to settle invoices. This suggests the use of a front company to facilitate the movement of funds.
- The criminals conduct international transactions involving multiple countries, including China and Germany, to further complicate the money trail and evade detection.
- The existence of multiple bank accounts operated by different individuals involved in the scheme, such as **Mr. JK** and **Ms. YD**, points to an effort to spread and launder the funds through various accounts.
- The criminals open bank accounts in Dublin using fake documents, a common tactic to hide their true identities and the illicit origin of funds.

Jurisdictions Involved

Nigeria, China, Germany, Ireland, United States of America

Source: INTERPOL-NCB

Typology 10 Laundering the Proceeds of Capital Market Fraud

CASE STUDY 33 – MONEY LAUNDERING BASED ON ALLEGED FRAUDULENT SALE OF SHARES

A case of Fraudulent Sales of Shares was reported by Mr. TJ. on behalf of the estate of Late PPP against one Mr. OG.

The complainant alleged that an individual who had been impersonating the late PPP has illegally acquired a significant portion of his stock holdings from multiple companies. He further alleged that the said imposter has been receiving dividends from the said shares without his client's knowledge.

Parallel financial investigation was carried out and letters written to all relevant / competent authorities such as commercial banks, various securities registrars, and different stock broking firms. Responses were received and thoroughly analyzed.

Investigation revealed that the suspect, Mr. OG opened an account in the name of Pa S. Bol with three different Banks using a forged identity document. The suspect sold shares belonging to PPP in four different stock broking firms valued at N2,267,784.49 **(approx. $2,995.6)** and gave the stock broking firm mandate to sell the shares belonging to Late PPP with proceeds paid into accounts owned by the suspect. The suspect also collected dividend to the tune of N3, 943,222.85 **(approx. $5,208.8)**.

The EFCC ascertained that the Mr OG is an imposter who fraudulently sold shares belonging to a deceased person. The case file forwarded to Legal and Prosecution Department for vetting and advice.

Indicators/techniques/methods

- The use of forged documents to operate bank and stockbroker accounts.
- Fraudulent Sale of Shares
- Impersonating the actual owner of the stocks
- Stealing by converting the proceeds from the fraudulent sale of stocks

Jurisdiction involved

Lagos, Nigeria

Source: EFCC

CASE STUDY 34 – LAUNDERING PROCEEDS OF FRAUDULENTLY AQUIRED DIVIDENT WARRANTS THROUGH FICTITIOUS BANK ACCOUNTS

The EFCC received a petition filed by one T Wills against a syndicate of fraudsters. The petitioner claimed that between 2012 and 2016, unidentified fraudsters intercepted and redirected dividend warrants from various companies.

Using information provided by the petitioner, in addition to feedback received from financial institutions and other competent authorities, the EFCC launched an investigation which revealed that a Mr. K had opened an account with a commercial bank bearing the name of the complainant. A review of the account opening package indicated inadequate KYC/CDD as some of the documents were forged. The suspect used the account to clear/ receive all the dividends belonging to the complainant.

Proceeds of crime amounting to N12,300,000.00 **(approx. $16,247.8)** was recovered for the complainant.

The investigation has been concluded and case file has been forwarded to Legal and Prosecution Department for vetting and advice.

Indicators/techniques/methods

- ❖ Stealing by Conversion of Dividend Warrants
- ❖ Forgery of Documents
- ❖ Proceed from the Stealing and conversion of dividend warrants was laundered into the fraudulent account operated by the suspect.

Jurisdiction Involved

Lagos, Nigeria

Source: EFCC

CASE STUDY 35: LAUNDERING PROCEEDS OF FRAUDULENTLY CONVERTED SHARES THROUGH BANK ACCOUNTS OF A BROKER DEALER

Mr Mut filed a petition to the EFCC against Mr. J, and F Financial Limited alleging that the suspects had fraudulently sold and diverted his shares valued at N45,752,314.90**. (approx. $60,437.1)**

The EFCC launched an investigation using information provided by the petitioner and feedback received from commercial banks and relevant competent authorities such as NGX Regulations, Corporate Affairs Commission, Securities and Exchange Commission, and Central Securities Clearing System.

Investigation revealed that Mr. J is the Managing Director of F Financial Limited which is licensed to act as a broker – dealer on the floors of the Nigeria stock exchange. Mr. Mut deposited some of his shares with F Financial Limited. Mr. J misused his authority as a stockbroker, deceitfully selling the complainant's shares with nine securities without authorization. The funds generated from the sale were also misappropriated for Mr. J's personal benefit.

Proceeds of crime was judiciously traced to the suspect's bank accounts and the sum of N20,000,000.00 **(approx. $26,419.2)** has so far been recovered from the suspect. However, Investigation is still ongoing and suspect is currently at large. Effort is currently being made to apprehend him for prosecution.

Indicators/Techniques/Methods

- ❖ Misuse of authority as a stock broker
- ❖ Proceed of crime laundered using personal bank accounts

Jurisdiction Involved

Nigeria

Source: EFCC

CASE STUDY 36: MONEY LAUNDERING BASED ON ALLEGED FRAUDULENT SALE OF SHARES BY A STOCKBROKING FIRM

This deals with an alleged case of fraudulent sale of shares and criminal conversion of funds reported by Engineer GI against FM Investment Limited. The complainant alleged that the suspect being a stock broking firm, sold shares valued at the sum of **N24,954,719.14 (approx. $32,964.2)** belonging to the complainant without his knowledge.

On receipt of the petition, several letters of investigation activities were written and dispatched to commercial banks, Corporate Affairs Commission and the Nigerian Exchange Group Plc.

Investigation revealed that FM Investment Limited was inactive on the floor of the Nigerian Exchange Group as at the time of the report and was initially registered with the Securities and Exchange Commission as a dealer before it was reclassified as a broker in 2015. Also, the 6,007,844 units of Nigerian Exchange Group Plc allotted to MF Investment under the scheme of demutualization have not been credited to MF Investment Limited due to some unresolved complaints against them.

The proceeds from the fraudulent sale of 311,747 units of shares valued at **N4,106,767.79 (approx. $5,424.8)** belonging to Engr. GI was paid to the account of M.I Limited, using a mandate form completed by one Mr. GB.

So far, the sum of **N19,300,000.00** has been recovered for petitioner.

The investigation is being concluded.

Indicators/techniques/methods

- ❖ Fraudulent Sale of Shares
- ❖ Impersonation
- ❖ Proceeds of crime laundered using a third-party bank account

Jurisdiction(s) involved

Lagos, Nigeria

Source: EFCC

Typology 11 Laundering the Proceeds of Procurement Fraud

CASE STUDY 37 – LAUNDERING OF PROCEEDS FROM CRIMINAL CONSPIRACY, CRIMINAL MISSAPPROPRIATION OF PUBLIC FUNDS, AND PROCUREMENT FRAUD THROUGH CITIZENSHIP BY INVESTMENT, REAL ESTATE, CAPITAL MARKET AND LEGAL PERSONS

The EFCC received an anonymous tip on the activities of a Cotton Association, some agricultural mechanization companies and some Prime Anchors of the Central Bank of Nigeria's Agric Programme to cotton farmers across the Country.

It was alleged that some of the individuals successfully processed CBN loan through a commercial bank, using fake collaterals which was enabled by a staff of the bank.

Investigations conducted revealed that the Prime Anchors obtained the loan in connivance with one Mrs T who is the Head of Agriculture Business in the Commercial Bank which received the over **N2,000,000,000** (a**pprox.**, **$2,641,927.65**) from the Central Bank for the benefit of the cotton farmers. Investigation revealed that Mrs T facilitated loan application for eleven customers by providing acceptable third-party collaterals at a fee which is paid upon disbursement of the loan to the farmers. Investigations also revealed that all the collateral documents supplied were fake and did not emanate from the Land Authority. A compromised staff of the land authority enabled the shenanigan while the bank relied on all the fake documents and search reports to disburse loans to (11) customers.

Investigation further revealed that Mrs T purchased three-bedroom terrace costing **N79,769,000.00 (approx. $105,371.96),** purchased stocks costing **N95,000,000.00 (approx. $125,491.56)** with her commission from the transactions that she facilitated. The younger brother of Mrs T also enabled the laundering of proceeds of this crime as he utilised some proceeds for renovation and furnishing of Mrs T's home property in Abuja while another sibling invested a portion of the proceed, using his own investment company. Proceeds of crime were also laundered using various corporate bodies home and abroad i.e., Dubai, Grenada. The suspect also used some corporate bodies, using the

proceeds of her crime, to acquire Grenada Citizenship[23] for herself and her son, having invested in the Country.

All funds linked to the suspect were traced and recovery of the proceeds of crime is ongoing. Interim Forfeiture Court Order has been gotten for one of the properties in Abuja as well as her Shares and Dividends. Monetary recoveries of **$100,000** have also been made and the case is being prepared for prosecution.

Indicators/techniques/methods

- ❖ Connivance of a bank staff in falsifying documents.
- ❖ Connivance with a staff of the land authority to produce forged land documents.
- ❖ Use of third parties to launder funds (investment)
- ❖ Use of corporate entities to launder funds.
- ❖ Purchase of citizenship by investment
- ❖ Utilisation of proceeds of crime for purchase of assets (real estate and shares)

Jurisdictions Involved

Nigeria, Grenada, Dubai

Source: EFCC

CASE STUDY 38 – USE OF LEGAL PERSONS TO LAUNDER PROCEEDS FROM PROCUREMENT FRAUD

This case is based on a tip made to the EFCC by a concerned citizen on criminal activities of some government officials of a Federal Agency within the Federal Capital Territory Abuja, Nigeria.

On receipt of the intelligence, investigators commenced investigation immediately and gathered intelligence from bank accounts linked to the suspects. Intelligence was also requested from competent authorities including Corporate Affairs Commission and a Federal Agency.

Financial investigations conducted revealed government officials and their proxies were using multiple companies to fraudulently obtain government funds, receive multiple payments for some of the contracts, which strongly suggest bid rigging, conflict of interest in handling government official business, misappropriation of public funds in the execution or non-execution of contracts, bribery of government officials and money laundering amongst others.

[23] The FATF and OECD published a report in November 2023 that holistically examines money laundering and financial crime risks associated with investment migration programmes, including risks related to foreign bribery, fraud and corruption, alongside other policy considerations related to public integrity, tax and migration. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Misuse-CBI-RBI-Programmes.pdf.coredownload.pdf

Analysis also revealed that the officers conspired with contractors to violate procurement procedures and pay funds to the tune of **N11,000,000,000.00 (approx. $14,530,602.10)** to the contractors and their proxy companies. These officials also forged documents and made payments to their cronies under the guise of the Agency's personnel enumeration, after which these proceeds were shared among them.

Funds and Properties linked to the suspects so far have been traced and recoveries are ongoing. Processes to forfeit the properties to the Federal Government are also underway through the Economic and Financial Crimes Proceeds of Crime Management Department, while the Legal and Prosecution Department are drafting up Charges against the suspects for possible prosecution.

Indicators/techniques/methods

- The Contravention of the Procurement Act (2007) by forging Documents, Vouchers to the tune of **N11,000,000,000.00**. **(approx. $14,530,602.10)**
- Sharing of the proceeds by the conspirators (Government Appointees, Officials of the Agency, Contractors and Proxies)
- Use of middle men to front as Company owners while in actual fact serve the interest of the officials.

Jurisdiction Involved

Abuja, Nigeria

Source: EFCC

CASE STUDY 39 – CASE OF CRIMINAL CONSPIRACY, ABUSE OF OFFICE, RECEIPT OF GRATIFICATION, CRIMINAL MISSAPPROPRIATION OF PUBLIC FUNDS, PROCUREMENT FRAUD AND MONEY LAUNDERING INVOLVING A DIRECTOR OF PROCUREMENT OF A GOVERNMET AGENCY AND LEGAL PERSONS

This deals with an Intelligence Report generated within the EFCC by the Directorate of Intelligence against the Director of Procurement of a Government Institution in charge of Rural Electrification.

On receipt of the intelligence, investigators commenced investigation immediately and gathered relevant information from competent authorities as well as the Corporate Affairs Commission on the suspect and various legal persons that featured to identify the directors, promoters and shareholders of all identified companies. Additionally, letters of investigation were dispatched to all contractors of the Electrification Agency who paid procurement kickbacks to the suspect.

Investigations conducted revealed that the director established various companies which he utilized for the receipt of kickbacks from contractors whom he awarded contracts to as the director of procurement, while also utilizing the companies for the award of various contracts from the Electrification Agency and other government institutions. He was also the signatory of the corporate bodies for a period before 2018 when he excused himself as the signatory. Investigation revealed that the suspect co-opted his friend who owns other companies with whom proceeds of their crime were laundered. The suspect through one of his registered companies also received various kickbacks from several companies.

The sum of **N42,220,000.00 (approx. $55,771.09)** was traced to the suspect as gratification and he has undertaken to refund the said monies. Recoveries are gradually being made by the suspect while investigation continues.

Indicators/techniques/methods

- The Contravention of the Procurement Act (2007) through influencing contract award to allies and cronies
- Laundering of proceeds of crime using legal persons and cronies
- Sharing of the proceeds by the conspirators (The Suspect and Contractors)

Jurisdiction Involved

Abuja, Nigeria

Source: EFCC

CASE STUDY 40 – LAUNDERING OF PROCEEDS FROM CRIMINAL CONSPIRACY, ABUSE OF OFFICE AND CRIMINAL MISSAPPROPRIATION OF PUBLIC FUNDS & PROCUREMENT FRAUD THROUGH LEGAL PERSONS

This deals with an Intelligence Report sent to the EFCC by the Nigerian Financial Intelligence Unit on the activities of some officials of a Federal Ministry within the Federal Capital Territory Abuja, Nigeria.

Investigations revealed top officials of a federal ministry and their proxies were using multiple companies to obtain government contracts and receive multiple payments for some of the contracts, which strongly suggest bid rigging, conflict of interest in handling government official business, misappropriation of public funds in the execution or non-execution of contracts, bribery of government officials and money laundering amongst others.

Analysis of bank accounts of the ministry, its officials, contractors and their proxies. shows the officials conspired with contractors, violate procurement procedures and pay funds to the tune of **N5,259,669,662.75 (approx. $6,947,833.37)** and $200,000.00 to the contractors and their proxy companies which the proceeds were shared among them.

All funds linked to the suspects were traced and fully recovered through the Economic and Financial Crimes Recovery Account domiciled in Central Bank of Nigeria. The case has been sent to the Legal and Prosecution Department, Charges against the suspects have been filed and awaiting prosecution through the Abuja Federal High Court.

Indicators/techniques/methods

- The Contravention of the Procurement Act (2007) by forging Ministerial Tenders Boards, Award Letters to the tune of N5,259,669,662.75 **(approx. $6,947,833.37)** and $200,000.00.
- Sharing of the proceeds by the conspirators (The Officials and Contractors)
- Use of legal persons by government officials.

Jurisdiction Involved:

Abuja, Nigeria

Source: EFCC

CASE STUDY 41 - LAUNDERING OF PROCEEDS FROM PROCUREMENT FRAUD THROUGH LEGAL PERSONS

This case was reported to the office of the Acting Executive Chairman of the EFCC on 6th February, 2017 against one Mr. Vin and others of a Government Agency on Education.

The petitioner alleged that for many years, Mr. Vin has been the Head of Procurement in the Government Agency and had engaged in several forms of fraudulent activities in the Government Agency's Procurement Unit. That as a result of his obvious contravention of the Public Procurement Act 2007, the Government Agency had little to show for the over **N130,000,000,000 (approx. $171,725,297.64)** that has been appropriated to it for projects by the Federal Government. That in 2014, the verification reports on contracts worth **N8,000,000,000 (approx. $10,567,710.62**) for the supply of science equipment to some government schools showed that most of the materials were either substandard or not delivered at all. That another MDG contracts worth **N9,000,000.000**

(approx. $11,888,674.45) for supply of textbooks to schools were either not executed or substandard products were supplied even though payments were made without verification.

Parallel Financial Investigation was carried out with relevant information received from various competent authorities and financial institutions. Assets purchased with the proceeds of crime were traced.

Investigation revealed that 8 companies owned by one Mr P were fraudulently selected by the Government Agency as against the selective bidding approved by Bureau for Public Procurement and out of **N7,000,000,000 (approx. $9,246,746.79)** that the contractor received from the Government Agency, a total sum of **N4,478,682,300.00 (approx. $ 5,916,177.31)** was diverted to various companies and individuals linked to the contractor and cronies of the then Minister of Education.

The entire sum has now been fully recovered in favour of EFCC Recovered Funds domiciled with the Central Bank of Nigeria

Indicators/techniques/methods

- Abuse of selective bidding process
- Transactions using companies that was not engaged by Government
- Use of commercial banks to move the laundered money
- Use of middle man and shell companies to launder the money

Jurisdiction Involved

Nigeria

Source: EFCC

Typology 12 Laundering of Proceeds of Employment Fraud

CASE STUDY 42 – SELF-LAUNDERING OF PROCEEDS DERVIVED FROM EMPLOYMENT SCAM

This deals with a written Petition by SMA against MSV where the complainant approached the suspect to help him secure employment for his friend CBD at a Government Agency.

Investigation revealed that the complainant paid the sum of Nine Hundred Thousand Naira **₦900,000.00 (approx. $1,188)** to an account belonging to the suspect as processing fee for the employment of CBD at the Government Agency. The said Nine Hundred Thousand Naira (**₦900,000.00**) was utilised for personal use by the suspect. Response from the Government Agency revealed that the Council did not embark on any recruitment exercise in 2021.

The suspect warehoused the proceeds of crime in his personal account and utilised it for personal purposes.

In summary, investigation has been concluded and the casefile has been forwarded to Legal and Prosecution Department for vetting and advice.

Indicators/techniques/methods

- Proceeds of crime warehoused in the suspect's account and same was utilized for personal purposes (self-laundering)

Jurisdiction Involved
Abuja, Nigeria

Source: EFCC

CASE STUDY 43: LAUNDERING OF PROCEEDS FROM EMPLOYMENT SCAM THROUGH BANK ACCOUNTS

This deals with a written petition by **Mr B** against **Ms. V** wherein the suspect received the total sum of **N3,700,000.00 (approx. $4,887)** for job slots in two government agencies.

Investigation revealed that the suspect, a civil servant, was paid the total sum **N3,700,000.00 (approx. $4,887)** by the complainant and his brother for jobs slots with two government agencies. The said sum was paid in three tranches between July, 2020 and November, 2020 into accounts with two commercial banks belonging to the suspect.

Investigation also revealed that the suspect was in no position to employ the complainant nor influence his employment into the above-mentioned Agencies. Investigation also confirmed that **Ms. V** withdrew the money in cash for her personal use. Proceeds of crime has been recovered from the suspect

Indicators/techniques/methods

-

Jurisdiction Involved
Abuja, Nigeria

Source: EFCC

CHAPTER FIVE: JURISDICTIONS OF CONCERN

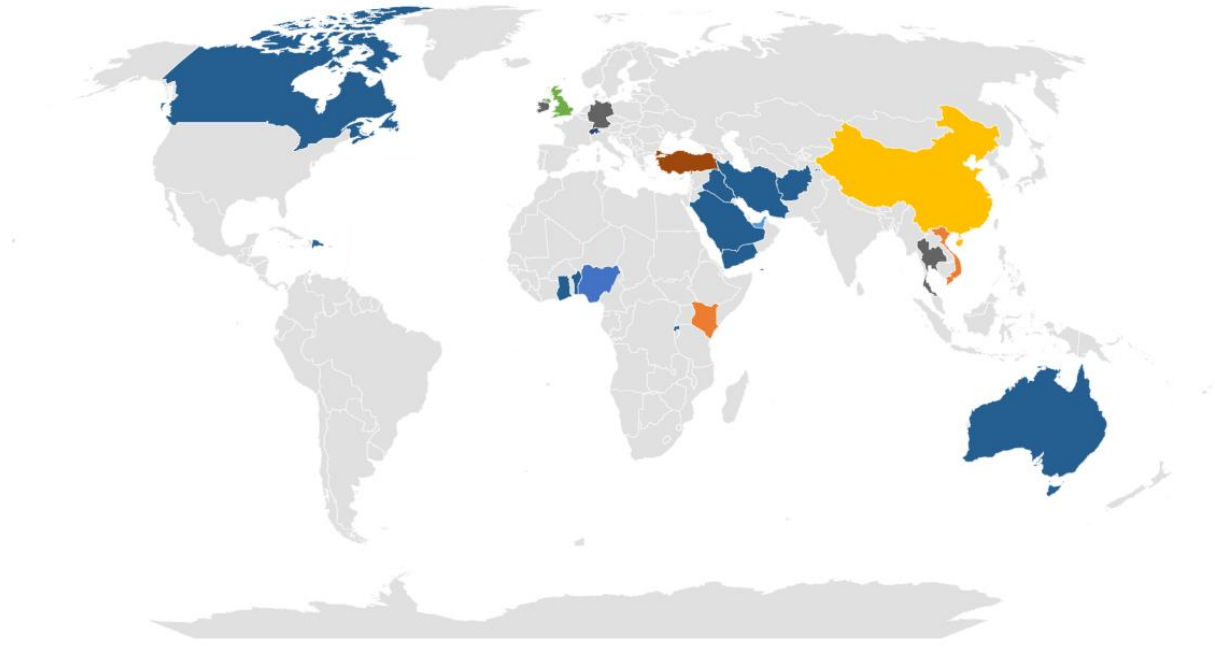
We explore the crucial topic of jurisdictions of concern with respect to money laundering in the context of fraud in this chapter. These jurisdictions were identified after a review of case studies included in this report and information obtained from questionnaires sent to reporting entities and investigative authorities. Through a thorough analysis of actual cases and the collection of viewpoints from relevant parties, the objective is to highlight the various types of money laundering schemes that are connected to fraud in various jurisdictions in relation to Nigeria. This approach ensures a robust foundation for evaluating the multifaceted challenges posed by money laundering activities in specific geographic areas, contributing to a more informed and focused international cooperation plan informed by risk.

The table below summarises jurisdictions that have been identified as well as their associated typologies based on case studies and responses received from questionnaires:

SN	JURISDICTION	ASSOCIATED MONEY LAUNDERING TYPOLOGY
1	Nigeria	1. Laundering of Proceeds of Fraud through Cryptocurrency Platforms 2. Use of Ponzi Schemes 3. Use of Bureau De Change Operators 4. Use of Bank Accounts to Launder Proceeds of Fraud 5. Laundering of Funds from Chargeback Fraud 6. Laundering Proceeds from Business Email Compromise (BEC) Fraud 7. Fraud in Relation to Trade Based Money Laundering 8. Fraud in Pension Funds Administration 9. Money Laundering by Organised Criminal Groups 10. Laundering the Proceeds of Capital Market Fraud 11. Laundering the Proceeds of Procurement Fraud 12. Laundering of Proceeds of Employment Fraud
2	Kenya	Laundering of Proceeds of Fraud through Cryptocurrency Platforms
3	Vietnam	Laundering of Proceeds of Fraud through Cryptocurrency Platforms
4	Unites States of America	1. Laundering of Proceeds of Fraud through Cryptocurrency Platforms 2. Use of Bank Accounts to Launder Proceeds of Fraud 3. Laundering Proceeds from Business Email Compromise (BEC) Fraud 4. Money Laundering by Organised Criminal Groups
5	China	1. Laundering of Proceeds of Fraud through Cryptocurrency Platforms 2. Money Laundering by Organised Criminal Groups

SN	JURISDICTION	ASSOCIATED MONEY LAUNDERING TYPOLOGY
6	United Arab Emirates	1. Use of Bureau De Change Operators, Laundering Proceeds from Business Email Compromise (BEC) Fraud 2. Fraud in Relation to Trade Based Money Laundering 3. Laundering the Proceeds of Procurement Fraud
7	United Kingdom	1. Use of Bureau De Change Operators 2. Money Laundering by Organised Criminal Groups
8	Switzerland	Use of Bureau De Change Operators
9	Turkey	Use of Bank Accounts to Launder Proceeds of Fraud
10	Thailand	Money Laundering by Organised Criminal Groups
11	Germany	Money Laundering by Organised Criminal Groups
12	Ireland	Money Laundering by Organised Criminal Groups
13	Grenada	Laundering the Proceeds of Procurement Fraud
14	Australia	Based on Questionnaire response
15	Canada	Based on Questionnaire response
16	Ghana	Based on Questionnaire response
17	Benin Republic	Based on Questionnaire response
18	Cayman Islands	Based on Questionnaire response
19	Dominican Republic	Based on Questionnaire response
20	Afghanistan	Based on Questionnaire response
21	Iraq	Based on Questionnaire response
22	Saudi Arabia	Based on Questionnaire response
23	Yemen	Based on Questionnaire response
24	Rwanda	Based on Questionnaire response

CHART DEPICTING JURISDICTIONS OF CONCERN



CHAPTER SIX: ANALYSIS OF QUESTIONAIRE RESPONSES

This chapter delves into money laundering typologies associated with fraud within Nigeria, as perceived by financial institutions, DNFBPs, supervisory authorities and the law enforcement agencies. A questionnaire was developed to and circulated to the stakeholders and their responses analysed to provide valuable insights based on their experience.

It's important to note that the views expressed herein are the individual perspectives of the respondents and do not necessarily reflect the official stance of their respective institutions.

This differentiation establishes the foundation for an examination of the challenges related to money laundering in Nigeria and the varied strategies implemented for its prevention and detection.

The questionnaire responses were received from a variety of sources, with the highest number coming from Bureau de Change Operators, totalling 534 responses and 62 from capital market operators. Others include 8 responses from Casino Operators, 6 from International Money Transfer Operators, 5 from Deposit Money Banks, and 4 each from the Central Bank of Nigeria and Payment Service Providers. The Car Dealers, Real Estate Agents, the Securities and Exchange Commission (SEC), National Insurance Commission (NAICOM), Economic and Financial Crimes Commission (EFCC), and INTERPOL - National Central Bureau all had one submission each.

Some responses were provided at an institutional level hence the single questionnaire submissions.

LAW ENFORCEMENT AUTHORITIES

Economic and Financial Crimes Commission (EFCC)

The Economic and Financial Crimes Commission (EFCC), Nigeria's foremost authority in the investigation and prosecution of economic and financial crimes, expressed its insights into the complex realm of money laundering typologies through fraud within the nation. As a fully autonomous institution vested with the authority to apprehend, detain, and prosecute those involved in various financial crimes, including advance fee fraud and futures market fraud, they mentioned their accumulated wealth of experience in combating these illicit activities.

The individuals elaborated on their experiences with the proceeds of these crimes, revealing insights into widespread patterns and sectors exploited by fraudsters to launder unlawfully obtained gains. Significantly, sectors such as real estate, banking, bureau de change services, virtual assets (particularly cryptocurrency), and the acquisition of high-value goods have surfaced as the favored channels for money laundering through fraudulent means. Common indicators observe through high scrutiny include lavish lifestyles, unexplained inflows into bank accounts, illicit financial flows, and the acquisition of assets or properties that significantly surpass reported incomes, considering them as potential red flags for such activities.

Regarding the ascent of cryptocurrency, or virtual assets, it was observed as an emerging trend in the landscape of money laundering through fraud. The responder pointed out that the EFCC collaborates extensively with other law enforcement agencies, financial institutions, and regulatory bodies.

To ensure their investigative and enforcement capabilities remain at the forefront, the responder noted that the EFCC prioritizes continuous staff training, as officers undergo rigorous programs, including certifications such as the ACAMS and CFE examinations, globally recognized credentials in anti-money laundering and fraud examination. Moreover, the EFCC has established dedicated resources such as the Chairman's Monitoring Units 1 and 2, Economic Governance Sections 1 and 2, and Special Duty Units to address the proceeds of fraud effectively.

The responder noted that Nigeria boasts robust provisions for prosecuting money laundering cases associated with fraud. They explained that the Money Laundering (Prevention and Prohibition) Act 2022 (MLPPA 2022) and the Proceeds of Crime (Recovery and Management) Act 2022 provide comprehensive measures to facilitate the prosecution and recovery of proceeds of crime.

INTERPOL – National Central Bureau (NCB)

The response received from the INTERPOL National Central Bureau in Nigeria reaffirmed its overarching global mission, which involves offering investigative support and training to law enforcement agencies worldwide. This mission includes tackling various crimes, notably

fraud, explaining the agency's familiarity with money laundering cases associated with fraud, a situation frequently encountered in the proceeds of these crimes.

The agency noted that a common trend in laundering the proceeds of fraud involves the use of third parties, such as banks, Bureau de Change (BDCs), payment processors, and companies. In this emerging technique, some foreign nationals residing in Nigeria open fraudulent accounts using the identities of vulnerable Nigerians, often conniving with bank account officers. These accounts are controlled by these foreign nationals, allowing them to access and transfer funds.

On the effectiveness of its international cooperation, INTERPOL-Nigeria maintains extensive collaboration with its 194 member countries, citing achievements such as the recent extradition of a Nigerian individual arrested on an Italian warrant and the apprehension of a Chinese national in Niamey, Niger Republic, over a fraud case investigated by INTERPOL Abuja.

The bureau highlighted the involvement of INTERPOL-Nigeria detectives in money laundering-related courses and programs conducted by INTERPOL's General Secretariat in Lyon, France, and other relevant bodies. These training initiatives contribute to enhancing their capabilities in addressing money laundering issues.

SUPERVISORY AUTHORITIES

Central Bank of Nigeria (CBN)

The responses received from AML/CFT staff of the Central Bank of Nigeria (CBN) indicated that there are regulatory frameworks in place to address money laundering activities associated with fraud. These include the Cyber Security Framework and Guidelines designated for Banks and Payment Services Providers and Operational Guidelines for Blacklisting. The CBN ensures compliance with these regulations and guidelines by creating awareness, conducting training and inspections, and assessing the effectiveness of reporting entities' anti money laundering (AML) measures related to fraud in both banks and other financial institutions.

When there are instances of fraud by the staff of the CBN, they are summarily dismissed. Furthermore, the CBN maintains a database of ex-staff who are blacklisted and disengaged

from the financial services sector for fraud or any act of dishonesty. The purpose is to ensure that such persons are not employed in the banking sector or any other sector.

The CBN collaborates with INTERPOL and the FBI in combating money laundering through fraud, as there is a need for effective industry collaboration and cooperation from law enforcement agents to detect, identify, apprehend, and prosecute fraudsters.

Securities and Exchange Commission (SEC)

To safeguard investors and maintain market integrity, the SEC employs various tools, including registering securities and market intermediaries, conducting inspections, and surveilling exchanges. They investigate potential breaches of market laws and regulations and, when necessary, take enforcement actions against errant market operators.

The MLPPA 2022 and SEC AML Regulation 2022 are the regulatory frameworks for addressing money laundering activities associated with fraud in Nigeria. The SEC ensures compliance with these regulations and guidelines through off-site transaction monitoring and on-site inspections to assess the effectiveness of the reporting entities.

When instances of money laundering through fraud occur, the regulatory agency enforces the penalties contained in the laws and regulations. The SEC collaborates with the International Organization of Securities Commissions (IOSCO), the NFIU, the NPF, and the EFCC in combating money laundering through fraud. There are some mechanisms and platforms for information sharing among regulatory authorities specifically focused on money laundering through fraud, such as CRIMS via the NFIU. Also, there are specific technological advancements and innovative approaches that the regulatory authority is exploring to address money laundering through fraud, such as automation within the capital space.

National Insurance Commission (NAICOM)

The regulatory framework addressing money laundering activities associated with fraud in the insurance sector is governed by the NAICOM AML/CFT/CPF Regulations, 2022. To ensure compliance, the regulatory authority employs offsite supervision through regulatory returns and onsite examination of regulating entities. Regular inspections or audits occur, with routine onsite examinations conducted once every two years.

In case of detecting money laundering through fraud, the regulatory authority initiates regulatory investigations, occasionally escalating matters to relevant law enforcement agencies for further action and potential prosecution. Collaboration is a key strategy, with existing Memoranda of Understanding (MOUs) between the commission and regulatory authorities domestically and internationally.

Information sharing is facilitated through platforms such as the Regulatory Coordination Sub-Committee of the Inter-Ministerial Committee on AML/CFT/CPF. The regulatory authority supports reporting entities in preventing, detecting, and reporting money laundering tied to fraud through various means, including training sessions, workshops, seminars, and regulatory returns.

Emerging trends and challenges in combating money laundering through fraud highlight insurance-related fraud, particularly in fraudulent claims on both life and general insurance products. Instances of fraudulent premium collection and remittance, often involving insurance agents, pose additional challenges.

Special Control Unit against Money Laundering (SCUML).

A total of seven responses were received from the Special Control Unit against Money Laundering (SCUML).

Based on the responses, the regulatory frameworks being put in place to address the proceeds of fraudulent activities are the Money Laundering (Prevention and Prohibition) Act, 2022, the use of government issued identification (e.g National Identity Management Initiatives), effective market entry controls and sensitization through public companies.

The regulations and guidelines that focus on combating money laundering through fraud are the Cybercrime (Prevention and Prohibition), Act 2015, the Framework and Guidelines for Public Internet Access (PIA), the National Data Protection and Regulation 2019, and the Advance Fee Fraud Act, 2005. The SCUML ensures compliance with the existing laws, regulations and guidelines through public engagement outreach (on-site and off-site) and conducts frequent inspections and audits to assess the effectiveness of AML related to fraud. When there is an instance of money laundering through fraud, the SCUML withdraws the certificates issued to the affected designated operator and escalates the case to law enforcement agencies.

The regulatory authority collaborates and shares information with NFIU, NDLEA, NPF, INTERPOL, EFCC, ICPC, and the FBI for further investigation and prosecution. The cooperation of the FBI and other foreign agencies has helped with the arrest and prosecution of fraudsters in Nigeria. Also, it supports the reporting entities in preventing, detecting, and reporting money laundering activities tied to fraud through ongoing sensitization before the issuance of certificates and assists them in the development of guidance on beneficial ownership by identifying proprietors and categorizing their risk.

The challenges of combating money laundering through fraud are based on experience. The use of cryptocurrencies, forgery of SCUML certificates, and use of casinos and gaming by high-profile people suggest money laundering through fraud. The SCUML is exploring ways to address money laundering through fraud based on the availability of specific technological advancements and innovative approaches. Likewise, the Application Programming Interface (API) that connects to other regulatory systems (CAC, NIMC), automation of business account registration, and procedures to reduce certificate forgery and authentication of certificates by banks via QR codes.

REPORTING ENTITIES

Deposit Money Banks. (DMBs)

Responses received from DMBs indicate that the most prevalent money laundering trends involving fraudulent activities are the frequent use of accounts opened with incomplete KYC, which eventually were used by pickers. A picker work on behalf of criminal groups to recruit money mules to move illicit funds through their bank accounts[24].The funds are then transferred from pickers' accounts to a cryptocurrency exchange that runs their accounts like a business account while ensuring that words like "crypto" are not used during transactions. Also, the use of government identification documents to give credence to stolen identities and the movement of funds from a victim account to the Bureau de Change in order to hide the identities of the actors are some of the common patterns observed. Other trends include romance scams, trade-based money laundering, cryptocurrency, cyber fraud et al.

The specific fraud patterns involve the use of digital assets to obfuscate the origin and destination of funds through cryptocurrency exchanges.

[24] https://www.skopenow.com/news/money-mules-how-organized-crime-groups-recruit-via-social-

Emerging fraud trends observed are the use of tier-one bank accounts to defraud customers (victims) in that category due to their literacy level. Also, the increased grant to Fintechs to carry out money transfers across international borders without enhanced KYC procedures for their customers or users of their service.

Measures in place to prevent and detect ML activities related to fraud, according to the respondents, include the implementation of the transaction monitoring system, red flag triggers set up in the monitoring system, a multi-factor authentication system, restrictions on new accounts pending verification, thresholds set on accounts based on account opening dates and transaction counts, and changes in personally identifiable information. The assessment of money laundering through fraudulent activities is done by assessing the product using customer profiles, transaction volumes, geographic location, products and services, and customer due diligence. Know your customer, know your customer's business, and enhance due diligence, among others.

The legal and regulatory requirements for reporting suspected cases of money laundering through fraudulent activities are Section 7 of the Money Laundering (Prevention and Prohibition) Act, 2022 and the Central Bank of Nigeria AML/CFT/CPF Regulations 2022.

Ensuring compliance with the reporting requirements, this is done by monitoring the reporting timelines and submission through compliance officers as well as ensuring acknowledged copies of the submitted reports are uploaded onto the report compliance portal. Likewise, filing STRs, SARs, and CTRs within 24 hours of their occurrence.

Trainings are organized based on the potential cases of money laundering through fraudulent activities, such as red flags for identifying ML, ultimate beneficial ownership, customer due diligence, and stages of money laundering, which are conducted quarterly, half-yearly, and sometimes yearly. Employees are encouraged to report suspicious activities internally, and there are whistle-blowing channels for reporting such activities.

The DMBs collaborate with other financial institutions and law enforcement including the EFCC and NPF to combat money laundering through fraud, this is done through a Fraud Desk that receives fraud intelligence and also shares it with other financial institutions. The law enforcement agencies instruct the banks to apprehend some customers who are accused of fraudulent activities, and they also share information with networks and organizations specifically focused on combating money laundering through fraud.

The challenges observed from the responses are the use of multiple transaction channels and the multiplicity of stakeholders involved in the transaction processing cycle. The introduction of Fintechs into the banking space and non-face-to-face transactions makes it difficult to verify the identity of the person conducting a transaction. Challenges in detecting money laundering through fraud include the malfunctions of the system causing system glitches, an unintelligent transaction monitoring tool, and delayed responses by counterparties. Other signs are layering and complex transaction structures, a lack of international coordination, and a high level of technological know-how among fraudsters.

Payment Service Providers (PSPs)

The most prevalent money laundering trends involving fraudulent activities identified within the sector by the four (4) respondents are impersonation, credit card fraud, internet fraud, and fraudulent transfers of funds. According to the respondents, the specific fraud patterns observed that are commonly linked to money laundering activities include card theft, card testing and chargeback fraud.

The PSPs uses Forter (which is a machine learning algorithm used to analyze every transaction in real-time) to assist in detecting and preventing fraud as it happens. This helps online retailers minimize losses and avoid chargebacks. Other measures include the implementation of tools for transaction monitoring and fraud engines, the implementation of two-factor authentication (2FA) and three domains secure (3DS), and the training of staff on anti-money laundering. The PSPs assess fraudulent activity through an AML Product Risk Assessment for new and upgraded products, which includes annual risk assessments, robust customer onboarding processes, and online real-time monitoring.

On legal and regulatory requirements for reporting fraudulent activities, the PSPs filed STRs and SARs to the NFIU via the goAML portal within 24 hours. The information in the STRs includes KYC and customer records such as BVN, biodata information and other relevant information.

In the opinion of respondents, the jurisdictions identified as being associated with money laundering through fraud are the USA, UK and Nigeria.

The PSPs provide quarterly training on AML/CFT, anti-fraud, and new ML trends to their staff on recognizing and reporting potential cases of money laundering through fraudulent activities. They participate in information sharing with networks and organizations specifically

focused on combating money laundering through fraud. Most of the challenges highlighted are the complexity involved in "following the money" for cases involving complex layering, the cost of technology, and the unavailability of local AI solutions for ML prevention.

International Money Transfer Operators (IMTOs)

A total of six responses were received from the IMTO sector. According to the respondents, the prevalent ML trends involving fraudulent activities are card fraud, identity theft, proceeds of consumer frauds and scams, advance fee fraud, romance scams, business email compromise, and employment scams. On-specific fraud patterns, card theft, card testing, internet fraud, BIN attacks, phishing scams, one-to-many transactions, and financial mules were observed.

The emerging fraud trends identified are preference for remote transactions, misrepresentation of both sources of funds and usage, and use of cryptocurrencies to conceal the source of funds or the person behind the transaction. Strict compliance monitoring with a two-layered check on a transaction and third-party testing to ascertain the robustness of the program and controls were the measures put in place to detect the fraudulent activities.

The IMTOs assess the risk of money laundering through fraudulent activities associated with products and services through an AML product risk assessment for new and upgraded products. The risk is assessed according to regions, demographics, GDP income, and purchasing power. They filed STRs and SARs with NFIU via the goAML portal within 24 hours of the transactions. The STRs contained information relating to the transaction and the customers involved. In ensuring compliance with reporting requirements, the IMTOs operate in line with regulatory requirements registered with the NFIU goAML portal, with 33.33% reporting very frequently. The jurisdictions associated with fraudulent activities are the USA, the UK, Australia, Canada, Ghana, and Benin Republic, as well as some countries in Asia. Also, trainings are conducted for the staff of the institutions on recognizing and reporting cases of fraudulent activity.

Bureau De Change Operators (BDCs)

A total of Five Hundred and Thirty-Five (535) respondents completed the questionnaire, with 29% belonging to the compliance department. Based on the questionnaire responses received, it was observed that the most prevalent money laundering trends involving

fraudulent activities are the unusual source of funds and using BDC companies as a front company to launder fraud proceed by corrupt government officials, secretive new clients who avoid personal contact, embezzlement, fake bank credit alerts and identity theft. Another trend is structuring of transactions, which involves splitting large amounts of cash into multiple small deposits and often spreading them to avoid detection.

The methods used in laundering the proceeds of fraud were the change of a hefty amount of Naira currency into USD and Hawala transactions, third-party money laundering using illicit or informal BDCs, concealment of true sources, trade-based money laundering and overbuying crypto currency, credit card fraud, Ponzi schemes, investment fraud, bank fraud, mortgage fraud, tax fraud and online fraud.

The most recent evolving trends of laundering proceeds of fraud are the mobile payment and e-wallets. The widespread use of mobile payment services and e-wallets have created new avenues for money laundering. Criminals exploit vulnerabilities in these systems, mainly the lack of transaction monitoring. Respondents further identified illegal transactions of foreign currency without licenses, export of foreign currency, huge amounts of money transferred from foreign jurisdictions into dormant bank accounts, frequent cash payments into special accounts as evolving trends in laundering proceeds of fraud.

The measures put in place to prevent and detect the proceeds of fraud are developing a framework that guides and enables staff to monitor, recognize and respond appropriately to suspicious transactions in addition to the guidelines issued by competent authorities. Also appointing Chief Compliance Officers, keeping proper sales records of customers and conducting proper CDD and KYC.

Likewise, reviewing all the existing policies to ensure check and balance on the mandate of the Central Bank of Nigeria and stiffen penalties on foreign exchange operators, creating awareness and alerting customers to the vulnerabilities of money laundering.

The methodologies used to measure the risk of ML through fraudulent activities related to products and services are by conducting regular audits and identifying the risk and reviewing each of the risk factors, which is done by assessing the risk associated with various types of consumers based on traits such as industry, geographical location and reputation. High-risk customers, such as politically exposed persons (PEPs), foreign shell companies, or those operating in high-risk jurisdictions, may require enhanced due diligence (EDD). Employees are placed on consistent trainings and seminars that educate them on AML /CFT knowledge.

The legal and regulatory requirements for reporting the proceeds of fraud are complying with all existing rules and regulations prescribed by the CBN AML/CFT/CPF Regulations 2022. Likewise, implementing a procedure to enable the reporting of suspicious activities. Involvement of competent authorities and other relevant authorities and registration of the company on the NFIU goAML platform and filing of all suspicious transactions irrespective of the amount involved, likewise those that exceeded reporting threshold. The respondents indicate that the Money Laundering (Prohibition and Prevention) Act 2022 and the Economic and Financial Crimes Commission (Establishment) Act, 2004 provide the legal framework for their compliance.

The BDCs ensure compliance with reporting requirements by employing a compliance officer whose duty is to ensure that CDD is duly carried out and PEP requirements are duly followed by initiating a risk management system. Likewise, getting approval from management to establish business relationships, proper record-keeping and internal control, monitoring and reporting suspicious transactions, and the implementation of targeted financial sanctions. Also, adherence to all guidelines as stipulated by the CBN, NFIU, ABCON and other regulatory bodies and working with the institutions in developing a training calendar for periodic sensitization on AML/CFT/CPF obligations.

The frequencies observed in reporting suspicious transaction to NFIU revealed that 29.6% accounted for frequently followed by 29.2% very frequently, 17% never, 12.7% occasionally and 11.4% rarely respectively.

The information and documents contained in reporting suspicious transactions involving the proceeds of fraud are identification of individuals or legal entities involved, originator and beneficiaries, and brief details of the initial investigation conducted. The customer's name, address, contact information, date of birth, identification documents, and transaction details, which include the date, time, and location of transactions, are among the information provided, along with any explanation given by the customer about the transaction and details of the suspicious financial activity. Other information contained in STRs include the clients' BVN, phone number, passport page and verified address.

The jurisdictions with a high risk of fraud are Cayman Islands and the Dominican Republic. Any domiciliary bank outflows to these countries are highly suspicious of romance/dating, crypto currency, identity theft, and direct investment fraud.

The types of training provided to staff members in spotting and reporting the occurrences of ML through fraudulent activities are training on concepts and mitigations of money laundering, sensitization on AML/CFT organized by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) for Foreign Exchange Bureau which seeks to enlighten the BDC operators on current global best practices is on AML/CFT. According to the responses on training timelines, 35% indicated quarterly, 34% indicated twice a year, and 32% indicated yearly. The programmes are designed primarily for compliance officers and directors of BDCs.

The channels and procedures set up for reporting the proceeds of fraud internally are through the compliance officer, who reports to the operation manager in writing with clear details of the activities. The operation manager reports to the director, the director reports to the managing director, and the managing director reports to the board of directors and makes copies for the legal team. The procedures were escalated to the risk department for onward reporting on the goAML website.

According to 84.4% of the responses, the BDCs collaborate with ABCON, EFCC, NFIU, and CBN. They exchange ideas on a regular basis during joint seminars and interactions. Similarly, 55.7% of responses indicate that their engagement in information sharing is based on the new framework for conducting and examining KYC and reporting trends.

The challenges encountered by the BDCs is that customers do not comply with the KYC procedure and they are unwilling to provide adequate personal background information. Also, they are usually reluctant to provide complete information pertaining to business purpose and location. Other challenges include a rapidly changing regulatory landscape, privacy concerns and data protection and sophisticated techniques.

The challenges encountered in detecting the proceeds of fraud are evolving tactics, absence of risk based approach in profiling customers, products, services and delivery channels. Other challenges faced in reporting the proceeds of fraud is the network challenges, resources constraints and data analysis tools.

Capital Market Operators

A total of 62 responses were received from the capital market operators.

Based on the questionnaire responses received, the most prevalent money laundering trends involving fraudulent activities are identity fraud, capital market fraud, investment deposit

fraud, the use of multiple accounts, and third-party transactions. Others include the use of wire transfers, placement through the deposit of purchase for shares, real estate fraud, the use of nominee and estate accounts, and use of third party and crypto currency trading.

The recent evolving trends in laundering proceeds of fraud are the wise Yahoo boys pretending to be bank officers, multi-customer cross-wallet activities (where a customer has the ability to have opaque fiat and crypto wallets with several financial institutions). Likewise, in the sale of shares shortly after purchase and the request for withdrawal of all or part of the funds deposited, sometimes the client gives flimsy excuses as a reason for their action, and in some cases, he may request payments of such funds to third parties. Also noticed is the terrorist funding raised from ransom activities that needs to be injected back into the system.

The measures put in place to prevent and detect the proceeds of fraud are AML/CFT/CPF policies and procedures, constant monitoring and surveillance, and non-acceptance of third-party funding or liquidation.

The methodologies used to measure the risk of fraudulent activities related to products and services are filing of reports to relevant agencies, training of staff, and regular management meetings, also maintaining client risk profiling and operational ability to track activities in the services provided, and complying with regulations guiding the operations of the institution in order to mitigate any form of risk associated with fraud.

The capital market operators (CMOs) reported STRs and SARs to the NFIU and ensured compliance with reporting requirements by reporting very frequently, which accounts for 77% of the responses. The STRs and SARs contained information about customers' BVN, account opening form, customer name, transaction details, address, and bank details.

The jurisdictions associated with money laundering through fraud are the south-west and south-east of Nigeria, with 46% admitting to not knowing any jurisdiction. The CMOs provide training to their staff in line with SEC policy and encourages them to report suspicious activities through their internal control and compliance officers.

The CMOs collaborate with the SEC, NFIU, EFCC, other regulatory authorities and also share information on combating the proceeds of fraud. Ideas are exchanged on a regular basis during joint seminars and interactive sessions.

Insurance Operators

13 respondents, primarily from the risk management and compliance units of insurance operators, responded to the questionnaire on money laundering associated with fraud within the insurance sector. The identified prevailing trends encompass a variety of fraudulent activities, including clients paying premiums for insurance policies and subsequently requesting refunds without reasonable explanations. Other trends involve policy fronting, where fraudsters purchase policies using illicit funds under legitimate entities to legitimize the source of funds, as well as premium evasion, false claims, identity theft, shell companies, and terrorist financing.

Additional trends reported involve requisitions for refunds after surrenders, cancellations, terminations, overpayments, and sometimes maturity. Respondents also highlighted instances of overpayment of premiums with requests to return the excess to a different account. Specific fraud patterns commonly linked to money laundering activities included structuring, identity theft through the use of stolen identities, and false claims submitted by fraudsters posing as policyholders.

Regarding emerging fraud trends, 50% of respondents reported no new trends, while the rest noted the use of shell companies, terrorist financing, the purchase of life insurance with investment elements, connivance between insurers and intermediaries to defraud companies, traditional refund requests, and third-party claiming requests.

Respondents indicated that insurance institutions assess the risk of money laundering through fraudulent activities related to products and services using specified risk ratings and due diligence on business relationships. Enhanced due diligence is applied to high-risk clients. Transaction scrutiny, internal and external ML/FT/PF risk assessments, and product feature reviews are conducted. Some institutions employ a comprehensive risk assessment framework involving customer due diligence, monitoring, regular audits, and ongoing monitoring.

Legal and regulatory requirements for reporting suspected cases of money laundering through fraudulent activities include the NAICOM regulations 2022, the Money Laundering (Prohibition and Prevention) Act 2022, Nigerian Financial Intelligence Unit STR filing guidelines, and knowing your customer requirements.

To ensure compliance with reporting requirements, institutions adhere to regulatory authorities' requirements, monitor client behaviour and transactions, and report illicit activities to competent authorities. Other methods include timely notices, dashboard reporting, auto-trigger alerts, monthly performance reviews, zero tolerance for non-compliance, and filing STR and CTR reports within stipulated time frames.

In terms of reporting suspicious transactions related to money laundering through fraud to the NFIU, 28.6% indicate frequent reporting, 28.4% very frequent reporting, and 57% report occasionally, frequently, or never. Information in suspicious transaction reports includes personal customer information, beneficiary details, sources of livelihood, transaction patterns, findings from CDD reports, and KYC forms.

Jurisdictions associated with money laundering through fraud include Afghanistan, Iraq, Saudi Arabia, Yemen, Rwanda, and Iran as foreign jurisdictions, while south-south and south-west are identified as domestic jurisdictions, with 30% having no knowledge.

90% of respondents indicate that their institutions provide quarterly AML/CFT/CPF training to all staff and agents, with topics tailored to observed knowledge gaps, while fraud detection training is conducted for audit staff. Training is also extended to the board and executive management, and new staff receive training during onboarding, with an e-learning module deployed to all staff categories.

Casino Operators

Eight (8) casino companies responded to the questionnaire and identified the most prevalent trends associated with fraudulent activities as funding the betting wallets with illegal funds from the payment of ransom, withdrawing funds from wallets without staking, or cashing out a game before the commencement of the game.

The emerging and evolving trends in money laundering associated with fraudulent activities are cryptocurrencies. Fraudulent initial coin offerings (ICOs) are raised. An ICO is a way of raising money. The funds are raised by the sale of a brand-new coin, typically digital money.

The measures that have been put in place to prevent and detect money laundering activities related to fraud are: no betting wallet can be funded with a third-party account or debit card. Establishing KYC policies and procedures to ensure that relevant customers' information is

obtained and updated regularly and that staff are mandated to flag suspicious transactions and escalate them to the floor manager, who then escalates them to the compliance department for reporting to the NFIU.

Respondents averred that casino companies assess the risk of money laundering through fraudulent activities by carrying out enhanced due diligence on their customers and establishing robust customer due diligence procedures for them.

The legal and regulatory requirements for reporting suspected cases of money laundering through fraudulent activities are the SCUML laws and regulations. Likewise, any cash-based transaction (CBT) of $10,000 or its naira equivalent is reported as a cash-based transaction report (CBTR) to SCUML, and cases of suspicious transactions are also frequently filed with the NFIU within 24 hours of occurrence and contain the name of the punter[25], address of the punter, telephone number of the punter, mode of the transactions, amongst other relevant information.

In order to ensure compliance with reporting requirements, the casino companies designate some dedicated staff for the schedule who are under the supervision of the Head of Operations. They keep thorough records of all reports submitted to the SCUML, and regular audits are conducted by the regulators. Trainings on cyber security and ML vulnerabilities are conducted on a yearly basis and are mandatory for compliance officers. Also, the Association of Casino and Gaming Operators organized an external training on new trends in ML associated with fraud.

The casino partners collaborate and share information with relevant financial institutions, regulators, and LEAs, such as the Lagos State Lotteries Board and Association, among others. The challenges faced are due to the absence of cooperation from the competitors. With the rapid advancement of technology, criminals exploit digital platforms, online marketplaces, and emerging payment methods to facilitate fraudulent activities and evade detection.

Real Estate Sector

The most prevalent money laundering trend associated with fraud is the purchase of high-profile properties with the use of a third party to buy the property. The measure put in place in order to prevent and detect fraudulent activities is to ensure due diligence in the screening

[25] A punter is a speculator who makes large bets on unlikely outcomes with the hopes of beating the odds for large payoffs. (Investopedia)

of clients and assess the risk of fraudulent activities through a proper background check on clients.

In order to ensure compliance with regulatory reporting requirements in the sector, currency transaction reports (CTRs) are being filed and reported to the regulatory authority. Likewise, STRs are filed and reported occasionally to the NFIU and contain the name and address of the client, and employees are encouraged to report suspicious activities internally to the principal partner.

There is no jurisdiction that was identified as being associated with money laundering through fraud. Training is conducted for real estate officers. However, there is no clear information on the frequency and cadre of staff trained based on functions**.**

Car Dealers Sector

The most prevalent money laundering trend and pattern associated with fraud is the use of cash in response to the payment and buying high-quality cars at a cheaper rate. The emerging fraud trends associated with money laundering in recent years are fake alerts, payments made with a company or organization account, and invoice receipts bearing a personal name. Creating awareness among the members is the measure put in place to prevent and detect money laundering activities related to fraud.

Employees are not encouraged to report suspicious activities internally, and the sector hasn't shared information with other relevant authorities.

There is no jurisdiction identified as being associated with money laundering through fraud. Training is conducted for car dealer associations twice a year, with 90% of attendees absent. However, there is no clear information on the frequency and cadre of staff trained based on functions.

The sector collaborates and shares with other financial institutions and law enforcement agencies to combat money laundering through fraud by reporting monthly transactions and providing seminars to its members. The challenge indicated is related to the illiteracy (at least 90%) of the operators, who need to be vigorously trained.

CHAPTER SEVEN CHALLENGES AND RECOMMENDATIONS

The prevalence of fraud in Nigeria, encompassing a wide array of forms from mail fraud to cryptocurrency fraud, presents a significant challenge to the country's financial and economic stability. Fraud not only inflicts personal losses on vulnerable individuals but also jeopardizes the operations of businesses and leads to substantial revenue losses. It has deep historical roots, with fraudsters adapting to new technologies and tactics over time.

The typologies of fraud identified in international investigations, including corporate fraud, cryptocurrency-related fraud, social engineering, and various online scams, illustrate the evolving nature of fraudulent activities. These typologies are often fuelled by enabling risk factors such as economic distress, which create motivation for fraudsters to exploit.

The challenges below are identified following a review of responses to the questionnaires by reporting entities and the competent authorities vis-à-vis industry knowledge provided by the project team.

REPORTING ENTITIES

1. Uneven understanding of money laundering through fraud evidenced by the responses to the questionnaire and engagements with reporting entities.
2. Uneven understanding of fraud types resulting in an inadequate risk assessment conducted by reporting entities.
3. Institutional policies and procedures are insufficient to identify and escalate suspected fraud.
4. Most institutional risk assessments do not assess the risk of money laundering through fraudulent activities associated with products and services. A review of responses indicates reporting entities do not fully grasp the correlation between fraud and money laundering.
5. Inadequate measures for screening employees.
6. Bureau de Change Operators conducting transactions that are out of scope of approved operations by the CBN
7. Challenges in tracking and identifying individuals involved in fraud due to the anonymous nature of certain transactions, particularly crypto-related.

COMPETENT AUTHORITIES

1. Absence of disaggregated statistics on investigations, prosecutions and convictions for predominant fraud types in Nigeria.
2. Inadequate sensitization of reporting entities of fraud types predominant in Nigeria.
3. Escalation channels for fraud cases from supervisory authorities need to be improved upon.
4. Inadequate collaboration between supervisory authorities and law enforcement agencies on escalated fraud

NATIONAL POLICIES AND LEGISLATION

1. Inadequate sensitization of the public on fraud types
2. Inadequate automation of procurement processes in Ministries, Departments and parastatals resulting in exploitation of systems to commit procurement fraud.
3. Absence of a national policy and framework to regulate and monitor cryptocurrency transactions.
4. Inadequate transparency in the recruitment process for MDAs

To combat money laundering associated with fraud in Nigeria, it is imperative that both regulatory authorities and businesses adopt proactive measures. These may include enhanced cybersecurity practices, stricter identity verification procedures, and greater awareness campaigns to educate individuals and organizations about the risks of fraud. Additionally, international collaboration and information sharing are crucial to stay ahead of evolving fraud typologies.

In summary, addressing the issue of money laundering through fraud in Nigeria requires a multi-faceted approach that encompasses prevention, detection, and mitigation efforts, along with a commitment to ongoing research and collaboration to ensure understanding of the emerging threats in the ever-evolving landscape of financial fraud.

Recommendation for Reporting Entities

1. Implement robust customer verification procedures to ensure the legitimacy of individuals and businesses.
2. Regularly update customer profiles, monitor high-risk online transaction channels, products, geographic locations and conduct risk assessments, especially for high-risk customers.
3. Establish sophisticated or AI (Artificial Intelligence) driven system to monitor fraudulent transaction patterns on online transactions channels/platforms and employ Transaction monitoring systems to detect unusual or suspicious activities for prompt filing to the NFIU.
4. Train staff on recognizing and reporting suspicious transactions or behaviour
5. Establish clear channels for employees and stakeholders to report suspicious activities anonymously.
6. Tailor AML/CFT efforts based on the assessed risk of customers, products, channels and geographical locations in line with the sectoral and National Risk Assessment.
7. Maintain a transparent and cooperative relationship with supervisors.
8. Develop and adopt measures to ascertain and sustain employee integrity.
9. Implementation of measures that will expose fraudulent staff and prosecuting them to deter others.
10. Stay updated on the latest fraud and AML/CFT techniques by regularly referring to guidance by the NFIU and supervisory authorities.
11. Educate customers on ways to avoid falling victim to fraud.
12. Individuals and entities should have hotlines or easy channels for reporting fraud to law enforcement and regulators.

Regulatory Authority/Supervisory Authorities

1. Every other regulatory agency should have a black book for keeping records of frauds in their industry like the CBN. The black book/database for fraud should be shared with investigative authorities and NFIU subject to a request for information during investigations.
2. Adopt a risk-based approach to supervising reporting entities, allocating resources and attention based on the assessed risk levels.

3. Provide reporting entities with clear guidance on fraud prevention and detection measures.
4. Take swift and decisive enforcement actions against entities found to be involved in fraudulent activities by imposing appropriate penalties to deter future misconduct.
5. Provide legal protections and incentives to encourage individuals to come forward with information about fraudulent activities.
6. Strengthening Judicial Processes: Improve the efficiency and effectiveness of the judicial system by establishing specialized fraud courts, providing specialized training for judges, and implementing technology-enabled solutions for case management.

Recommendation for Law Enforcement Agencies

1. To increase trust in the banking industry and prevent future fraud, Nigerian banks must employ the Cybercrime Act to punish perpetrators.
2. Provide specialized training to law enforcement agencies, such as the Economic and Financial Crimes Commission (EFCC), and Nigeria Police Force (NPF) to improve their capacity in investigating and prosecuting fraud cases.
3. Enhancing International Cooperation: Strengthen collaboration with international organizations, law enforcement agencies of other countries, and financial institutions to share intelligence, best practices, and strategies for combating cross-border fraud. Sign and enforce mutual legal assistance treaties to facilitate information sharing and extradition of offenders.
4. Prioritise financial intelligence received on fraud and request for financial intelligence when investigating fraud cases to assist parallel money laundering investigation.
5. Leverage on the provisions of the Proceeds of Crime (Recovery and Management) Act, 2022 to prevent fraudsters from enjoying their proceeds of crime.
6. Law enforcement agencies should strengthen cooperation with other nations by establishing mechanisms for swift information exchange and joint investigations to address challenges arising from the global nature of citizenship by investment programs.