

2018

# CENTRAL BANK OF NIGERIA (CBN)

ANTI- MONEY LAUNDERING/COMBATING  
THE FINANCING OF TERRORISM (AML/CFT)  
POLICY AND PROCEDURE MANUAL

AML/CFT Compliance Office  
Governors' Department  
Central Bank of Nigeria



23.0 _ Means of Identification .....	25
24.0 _ Sanction Screening.....	25
25.0 _ Whistle-Blower Protection.....	25
26.0 _ Periodic Customer Review.....	25
27.0 _ KYC Documentation Requirements .....	26
28.0 _ Record Keeping.....	26
29.0 _ Account Monitoring.....	27
30.0 _ Investigations (Alert Review and enquiry).....	28
31.0 _ Documentation of closed Alerts.....	29
32.0 _ Training.....	29
33.0 _ Internal Control and Independent Testing.....	30
34.0 _ APPENDICES:.....	31
36.0 _ APPROVALS.....	36

## Table of Contents

PART I: POLICY .....	7
i. Definition of Key terms.....	3
1.0 Background.....	7
2.0 Objective .....	7
3.0 Scope .....	8
4.0 Relevant Laws and Regulation.....	8
5.0 CBN AML/CFT Policy Statement .....	8
6.0 Overview of CBN Compliance Framework.....	9
7.0 AML/CFT Compliance Structure.....	10
8.0 Organogram.....	11
9.0 Compliance Responsibilities .....	12
10.0 AML/CFT Reporting Framework.....	14
11.0 Sanctions.....	15
12.0 Risk Assessment Framework.....	15
13.0 Customer Risk Assessment Process .....	15
14.0 High Risk Products and Services .....	17
15.0 Correspondent Banking Relationships.....	17
16.0 High Risk Geographic Locations .....	18
17.0 Customer Acceptance Policy .....	18
18.0 Customer Identification .....	18
19.0 Customer Due Diligence (CDD).....	19
20.0 Reporting .....	20
21.0 Other AML/CFT Reports to be rendered .....	20
PART 2: PROCEDURES.....	24
22.0 Nature and Level of the Business .....	24

## **I. Definition of key terms**

**Some key terms applicable in the implementation of this manual includes:**

- i. FATF- Financial Action Task Force**
- ii. ML- Money Laundering**
- iii. FT- Financing Terrorism**
- iv. AML- Anti-Money Laundering**
- v. CFT- Combating Financing of Terrorism**
- vi. CCO- Chief Compliance Officer**
- vii. KYC- Know Your Customer**
- viii. KYCB- Know Your Customers Business**
- ix. CDD- Customer Due Diligence**
- x. UNSCRs- United Nations Security Council Resolutions**
- xi. MDAs- Ministries, Departments and Agencies**

### **i. Financial Action Task Force (FATF)**

The FATF was established in July 1989 at the group of seven (G7) Summit in Paris, initially to examine and develop measures to combat money laundering. In October 2001, the FATF expanded its mandates to incorporate efforts to combat terrorism financing. The objectives of FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The FATF made 40 recommendations to raise the international standards of prevention of money laundering to a uniform level which set out basic framework for money laundering prevention efforts designed to be of universal application. (See appendix C).

## ii. Money laundering

Money Laundering is the act of directly or indirectly concealing or disguising any fund or property that is derived from the proceeds of an unlawful activity. Simply put, it is the process by which "dirty" money is made to look legitimate or "clean" so that the funds may be used freely without trace of its illicit source.

The Money Laundering Prohibition Act, 2011 (as amended) provides for procedures for customer due diligence, reporting requirements, offences and penalties. Section 15 (2) clearly stipulates the offence of money laundering as thus:

"Any person or body corporate, in or outside Nigeria, who directly or indirectly—

- (a) conceals or disguises the origin of;
  - (b) converts or transfers;
  - (c) removes from the jurisdiction; or
  - (d) acquires, uses, retains or takes possession or control of any fund or property, knowingly or reasonably ought to have known that such fund or property is, or forms part of the proceeds of an unlawful act;
- commits an offence of money laundering under this Act."

It also stipulates amongst others, the following penalty for contravention: "A person who contravenes the provisions of subsection (2) of this section is liable on conviction to a term of not less than 7 years but not more than 14 years imprisonment.

- a) A body corporate who contravenes the provisions of subsection (2) of this section is liable on conviction to a fine of not less than 100% of the funds and properties acquired as a result of the offence committed; and
- b) Withdrawal of license.
- c) Where the body corporate persists in the commission of the offence for which it was convicted in the first instance, the Regulators may withdraw or revoke the certificate or license of the body corporate."

Money laundering involves three independent stages namely Placement, Layering and Integration.

**Placement** – This is the stage where the funds from the illicit activities are physically placed into the economy. It may include the co-mingling of funds from legitimate sources and illegitimate sources. Examples of this stage include direct deposit of funds into Bank accounts, purchase of luxury goods such as cars and artworks, etc.

**Layering** – This involves the creation of complex transactions in order to distance the funds from the original source and also to obliterate the audit trail. (e.g. wire transfers, letter of credit, purchase of financial instruments, transfer to offshore accounts, re-sale of assets, etc.)

**Integration** – It is the stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all the other assets in the system. Integration of the ‘cleaned’ money into the economy is accomplished by the launderer making it appear to have been legally earned. At this stage, it is exceedingly difficult to distinguish legal and illegal wealth. e.g. Inflow from offshore for investments, funds from sale of real estate.

### iii. Terrorist Financing

This is defined in this manual to include both legitimate and illegitimate money characterized by concealment of the origin or intended criminal use of the funds. The techniques used to launder money are essentially the same as that used to disguise the origin of, and use, for terrorism financing.

Funds used to support terrorism may originate from legitimate sources, criminal activities or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin is key. Thus, if the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financed activity goes undetected.

Terrorism financing involves three stages namely Sourcing, Moving and Executing.

**Sourcing (raise)** - this stage involves raising funds by terrorists through donations, self-funding and criminal activities such as proceeds of drug trafficking, extortion, cheque fraud, credit card fraud, legitimate business, use of charitable organizations, sham charities, etc.

**Moving (transfer)** - this involves use of charities and non-profit organizations, use of Alternative Remittance Systems (ARS), use of cash couriers, use of gold to move value, wire transfers to move money across borders and the formal financial sector.

**Executing (use)** - in this stage funds are required to promote a militant ideology, pay operatives and their families, arrange for travel, train new members, forge documents, pay bribes, acquire weapons, and stage attacks.

### **iii. Predicate Offences**

Predicate offences are offences whose proceeds may become the subject of any of the money laundering offences established under the Act.

Designated Categories of Offences (DCOs) include:

- i. Participation in an organized criminal group and racketeering
- ii. Terrorism, including terrorism financing
- iii. Trafficking in human beings and migrant smuggling
- iv. Sexual exploitation, including sexual exploitation of children
- v. Illicit trafficking in narcotic drugs and psychotropic substances
- vi. Illicit arms trafficking
- vii. Illicit trafficking in stolen and other goods
- viii. Corruption and bribery
- ix. Fraud
- x. Counterfeiting currency
- xi. Counterfeiting and piracy of products
- xii. Environmental crime
- xiii. Murder, grievous bodily injury
- xiv. Kidnapping, illegal restraint and hostage-taking
- xv. Robbery or theft
- xvi. Smuggling
- xvii. Extortion
- xviii. Forgery
- xix. Piracy; and
- xx. Insider-trading and market manipulation
- xxi. Others

## **PART I: POLICY**

### **1.0 Background**

#### **Mandate of CBN**

**The Central Bank of Nigeria Act 2007 (as amended) enumerated the core functions of the Bank as follows;**

1. Ensure monetary and price stability;
2. Issue legal tender currency in Nigeria;
3. Maintain external reserves to safeguard the international value of the legal tender currency;
4. Promote a sound financial system in Nigeria and;
5. Act as Banker and provide economic and financial advice to the Federal Government.

In carrying out these core mandates, the CBN has over the years performed some major developmental functions, focused on all the key sectors of the Nigerian economy (financial, agricultural and industrial sectors, etc.) to promote sound financial system.

The role of the CBN as a Banker to the Federal Government entails offering financial advice and maintenance of accounts for Ministries, Departments and Agencies of government. The Bank also maintains accounts for financial institutions within Nigeria and with financial institutions outside Nigeria.

### **2.0 Objective**

The objective of this AML/CFT Manual is to set out policies and procedures to guide employees and the Bank to conduct business in accordance with applicable Anti-Money Laundering (AML) laws and regulations. The manual aims to establish procedures and minimum standards to protect the CBN from being used as a channel to launder money, finance terrorism and other forms of financial crimes.

### **3.0 Scope**

The CBN AML/CFT Manual sets minimum standards for employees of the Bank to comply with AML/CFT laws and regulations in the following broad areas:

- I. Conduct of financial services;
- II. Dealings with third party beneficiaries (such as consultants and contractors); and
- III. Employees conduct.

This manual is guided by the Money Laundering Prohibition Act 2011, Terrorism Prevention Act 2011 and other applicable relevant laws and regulations.

### **4.0 Applicable Relevant Laws and Regulation**

Other applicable laws and regulations include;

- i. Money Laundering (Prohibition) Act, 2011 (as amended)
- ii. Terrorism Prevention Act, 2012 (as amended)
- iii. Terrorism Prevention (Freezing of International Terrorist Funds and other Related Matters) Regulations, 2013
- iv. Economic and Financial Crime Commission (EFCC) (Establishment) Act 2004
- v. Banks and Other Financial Institutions Act (BOFIA) 1991
- vi. CBN AML/CFT Regulations, 2013
- vii. CBN Act 2007
- viii. CBN AML/CFT Risk-Based Supervision Framework, 2011
- ix. CBN Circulars and other communications by regulators
- x. National Drug Law Enforcement Act (1990)
- xi. Other international instruments ( such as FATF Recommendations, United Nations Security Council Resolutions)(UNSCR)

### **5.0 CBN AML/CFT Policy Statement**

The Central Bank of Nigeria provides banking services to the government and deposit money banks. Its primary function as a regulatory institution precludes it from most of

the provisions of the Money Laundering (Prohibition) Act, 2011 (MLPA), Terrorism Prevention Act, 2012 (TPA) and the Central Bank of Nigeria Anti-Money Laundering/Combating the Financing of Terrorism Regulations, 2013 (CBN AML/CFT Regulations). The Bank, however, ensures that its processes, policies and procedures conform to the spirit of the provisions of these laws, international protocols and agreements.

The Bank supports its staff to achieve the highest standards of compliance and integrity. Employees shall fully understand and be guided by these standards in the conduct of business and dealings with stakeholders. Protecting the good name and the reputation of the Bank shall be a primary consideration in all actions taken by employees.

The Bank therefore shall maintain the highest operating standards to ensure that its products and services were not used for the purpose of Money Laundering, Terrorism Financing or other crimes through investments in training, material resources, the use of appropriate technology and collaboration with other Regulators and Law Enforcement Agencies.

The AML/CFT operation in the Bank shall be reviewed by Internal Audit Department as well as External Auditors to ensure implementation of policies and procedures related to AML/CFT.

## **6.0 Overview of CBN Compliance Framework**

The AML/CFT Compliance function, domiciled in the Governors' Department of CBN, generally focuses on the identification of AML/CFT compliance responsibilities, assessment of risks, advice, monitoring, and reporting on the Bank's compliance with applicable laws, regulations and codes of conduct, and assist in the prevention of violations of the same in the Bank.

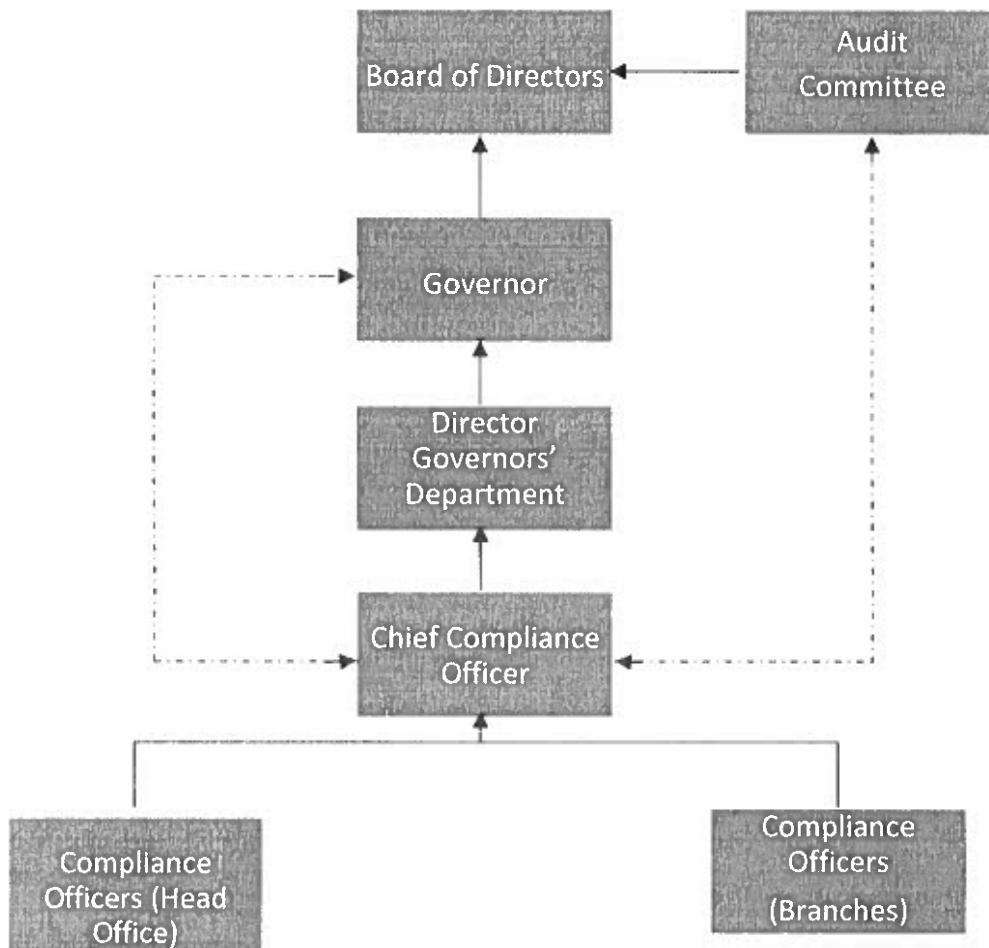
The AML/CFT Compliance Office develops the format for use by Strategic Business Units of the Bank to render periodic reports. It shall also assess the appropriateness of

the Bank's AML/CFT compliance procedures and guidelines, promptly follow up any identified deficiencies, and (where necessary) formulate proposals for improvement.

## **7.0 AML/CFT Compliance Structure**

- The Chief Compliance Officer (CCO) of the Bank (who is at the executive level) reports to the Board (Audit Committee) through the Director, Governors' Department. The administrators of the Departments and Head, Banking Office in the Branches shall be the Compliance Officer of their Strategic Business Units (SBUs). The Compliance Officers in the Departments and Branches shall report to the CCO through the head of their SBUs.

## 8.0 Organogram



## **9.0 Compliance Responsibilities**

### **Board**

The Board of Directors is responsible for providing leadership and direction in the management of the Bank's AML/CFT compliance risk. The Board will approve the Bank's AML/CFT Compliance Manual and it will periodically assess the extent to which the Bank manages its Money Laundering/ Financing Terrorism (ML/FT) risks. The Board will oversee the implementation of the policies contained in the compliance manual through its Audit Committee.

### **Committee of Governors' (COG)**

The Committee of Governors' is responsible for overseeing the management of the Bank's compliance risk and shall regularly be informed of the progress made in respect of AML/CFT compliance.

### **Director, Governors' Department**

The Director oversees AML/CFT compliance in the Bank and supervises the activities of the Office. The Chief Compliance Officer (CCO) reports all AML/CFT related issues to the management through the Director, Governors Department.

### **Chief Compliance Officer (CCO)**

The Head, Compliance Division in Governors' Department shall be the AML/CFT Chief Compliance Officer (CCO) of the Bank. The CCO is responsible for coordinating the identification, management of compliance risks and the supervision of other compliance functions of the Department. The CCO responsibilities amongst others include:

- Coordinate and implement the Bank's AML/CFT compliance initiatives.
- Develop the compliance strategy, policy, structure and processes.
- Report periodically on AML/CFT compliance related matter to the Management and Audit Committee of the Board.
- Report non-compliance and other potential exposures to the management immediately and establish prompt mechanisms for the resolution thereof.
- Collaborate with internal stakeholders and other Regulators.

- Ensure continuous training of AML/CFT compliance officers to ensure that they have required technical knowledge and regulatory framework that applies to the Bank.
- Establish and inculcate an AML/CFT compliance culture in the Bank through the development of an appropriate compliance awareness programme.
- Ensure that management incorporates AML/CFT regulatory requirements into operations manual.
- Collaborate with Capacity Development Department in the training of staff in AML/CFT awareness, detection methods and reporting requirements.
- Ensure that all new and old AML/CFT regulatory directives are communicated to staff.
- Assist Departments and Branches to identify and resolve issues related to AML/CFT non-compliance risk.
- Develop formal arrangements to help the CBN and its Officers to become more mindful, knowledgeable and capable of responding to those ML/FT risks that can affect the Bank's reputation and legal exposure.

## **Compliance Officers**

The specific duties of compliance officers are:

- Co-ordinate and monitor day to day compliance with applicable Money Laundering laws and regulations in their SBUs.
- Receive and vet suspicious transaction reports from staff.
- Assist the CCO in organizing AML/CFT programmes for employees of their SBU.
- Ensure timely rendition of AML/CFT regulatory reports.

## **Employees**

Employees are expected to be familiar and comply with applicable laws and regulations:

- Employees are to adhere to the AML/CFT compliance Policy Manual of the Bank;

- Employees should conduct business in accordance with applicable anti-money laundering, counter-terrorist financing laws and regulations, corporate policies, and maintain the highest ethical standards;
- Employees must not provide advice or other assistance to individuals or groups who attempt to violate or evade anti-money laundering, counter-terrorist financing laws and regulations or corporate policies;
- Employees should refrain from willfully ignoring indications that a customer seeks to engage in a relationship or transaction other than for a lawful purpose;
- Employees should avoid establishing relationships with individuals or entities who may pose undue reputational risk to the Bank; and
- Employees should protect the Bank's reputation for integrity and fair dealing, by ensuring that the Bank's customers and the transactions engaged in on its behalf are legitimate.

### **Stakeholder Departments**

These are key departments that due to their operational activities are involved with, or are to comply with relevant AML/CFT Laws and Regulations. The departments include:

- i. Banking and Payment Systems Department (BPSD)
- ii. Procurement and Support Services Department (PSSD)
- iii. Branch Operations Department (BOD)
- iv. Risk Management Department (RMD)
- v. Reserve Management Department (RED)
- vi. Human Resources Department (HRD)
- vii. Trade and Exchange Department (TED)
- viii. Financial Market Department (FMD)
- ix. All Branches

## **10.0 AML/CFT Reporting Framework**

### **Board Audit Committee**

The CCO shall periodically report to the Board of Directors through the Audit Committee of the Board on emerging issues on AML/CFT, status of the Bank on relevant, changes

in regulations. This will enable the Board to make informed decisions on whether the Bank is managing its ML/TF risk effectively.

### **Committee of Governors**

The CCO shall report quarterly to the COG on emerging issues on AML/CFT, status of the Bank on relevant changes in regulations.

### **11.0 Sanctions**

Non-compliance with the AML/CFT laws and regulations will be reported to Management for the appropriate sanctions.

### **12.0 Risk Assessment Framework**

CBN periodically conducts risk assessment to safeguard the Bank from being used to launder proceeds of crime or finance terrorism. This Risk Assessment will be conducted along the lines of our customers, products, geographic locations and delivery channels. It will ensure that identified lower and higher risks are properly mitigated. The Bank shall adopt risk-based approaches that are commensurate with the specific risks of money laundering and terrorist financing.

Higher money laundering risks demand stronger controls than warranted by individuals or countries deemed to be of lower risk. However, all categories of risks whether low or high must be mitigated by the application of appropriate controls as provided in this Manual, such as verification of customer identification, Know Your Customer (KYC) policies, and so on.

The following paragraphs provide a framework for identifying the degree of potential Money Laundering risks associated with specific customers and transactions in order to ensure focused monitoring of those customers and transactions that potentially pose the greatest risk of ML/TF.

### **13.0 Customer Risk Assessment Process**

The Bank assesses KYC risk by classifying accounts into different categories of Risk such as high, medium, and low.

The customer types are along the lines of financial institutions, Ministries, Departments and Agencies of government. Customer risk assessment is done at the point of account opening and as long as the business relationship continues.

**Higher risk customers-** Before establishing relationship with prospective customers, the various SBU's and Branches are responsible for carrying out formal assessment of risk on the accounts and classifying them as either high, medium or low risk. Accounts considered to be of higher risks will be monitored closely by SBUs and Branches. Any suspicion that accounts are being used to launder the proceeds of crime or to assist the financing of terrorism will be reported to the Chief Compliance Officer. Some potentially higher risk customers include:

- Politically Exposed Persons (PEPs): These are individuals who are or have been entrusted with prominent public functions in Nigeria or in foreign countries, and people or entities associated with them and include-
  - a) Heads of State or Government;
  - b) State Governors;
  - c) Local Government Chairmen;
  - d) Senior politicians;
  - e) Senior government officials;
  - f) Judicial or Military officials;
  - g) Senior executives of state owned corporations;
  - h) Important political party officials;
  - i) Family members or close associates of PEPs; and
  - j) Members of royal families.

PEPs also include persons who are or have been entrusted with a prominent function by an international organization; members of CBN senior management and this includes

directors and members of the board or equivalent functions other than middle ranking or more junior individuals.

The CBN does not maintain account relationships for those who fall into the above categories in their personal capacities. Rather, individuals listed above may represent some government institutions which maintain accounts with the Bank. The approval of the Accountant-General of the Federation or the State Accountant-General must be obtained before account relationships are established.

#### **14.0 High Risk Products and Services**

All Banking products that are used to convert cash to a monetary instrument and electronic products that permit rapid value movement (Wire Transfers, FX transactions followed by payment into an account in another jurisdiction) can be abused by criminals. For trade transactions, Export Letters of Credit have been ranked as high risk because of the possibility of presentation of false shipping documents when no goods are actually shipped. Another factor in this ranking is the possibility of over-inflated invoicing for low value or worthless merchandise. All other trade products have been risk ranked either as medium or low risk.

#### **15.0 Correspondent Banking Relationships**

Transactions conducted through Correspondent Banking relationships shall be managed in accordance with a risk-based approach; and Know Your Correspondent procedures shall be established to ascertain whether or not the correspondent Bank or the counter-party is itself regulated for money laundering prevention; and where regulated, the correspondent shall verify the identity of its customers in accordance with Financial Action Task Force (FATF) standards; and where this is not the case, additional due diligence shall be required to ascertain and assess the correspondent's internal policy on money laundering prevention and KYC procedures.

CBN shall guard against establishing correspondent Banking relationships with high risk foreign Banks such as shell Banks, with correspondent Banks that have historically allowed their institutions to be used for ML/FT.

## **16.0 High Risk Geographic Locations**

Care should also be taken when doing business with third parties located in Geographic locations with a history of supporting terrorism; bases for drug production/distribution; suffering from civil unrest/war.

These includes jurisdictions that have been identified as high risk countries by standard setting institutions such as FATF; countries on designated sanction Lists such as the United Nations Consolidated Lists and US Office of Foreign Asset Control (OFAC) List.

## **17.0 Customer Acceptance Policy**

Central Bank of Nigeria shall accept customers after due verification of customers' identities, address and/or place of business, after ascertaining their source of income / funds and after considering the level of risks they pose to the Bank, based on the kind of business under consideration (e.g. Bureau De Change Operators).

Care will be taken to apply appropriate level of due diligence, depending on customers' risk profiles. No account shall be opened for anonymous or fictitious customers.

The CBN should not enter into a relationship with a prospective customer until the person/entity has been duly identified and verified. The customer acceptance process also includes ensuring that the prospective customer is not on the 'watch list' which includes names of sanctioned persons as well as known fraudsters.

## **18.0 Customer Identification**

The Bank would identify and verify the identity of its customers and their beneficial owners. The Bank shall not consummate a business relationship until all relevant parties to the relationship have been identified and the nature of the business they intend to conduct ascertained.

Once an on-going business relationship is established, any inconsistent activity shall be examined to determine whether or not there is an element of money laundering.

Customer identification could be a major issue when establishing business relationship with a prospective customer and an on-going due diligence is necessary when the relationship has been fully consummated.

The Bank shall conduct a risk assessment of their customer base and in determining the risks, shall consider the following:

- a. The types of accounts offered
- b. The methods of opening accounts
- c. The types of identifying information available
- d. The institution's size, location, and customer base.

As a general rule, approval must be obtained from the Accountant General of the Federation before any SBU or Branch will open an account for all Ministries, Departments and Agencies of government.

#### **19.0 Customer Due Diligence (CDD)**

SBUs and Branches shall put in place Customer Due Diligence procedures which shall be monitored by the AML/CFT Compliance Office. Due Diligence shall be conducted for all customers in the following instances:

- When banking relationships are established;
- Where there is a suspicion of money laundering or terrorist financing;
- When the Bank has doubts about the validity or adequacy of previously obtained customer identification data.

As an Ordering or Intermediary financial institution when carrying out a wire transfer, the Bank will ensure that qualifying wire transfers contain and retain required and accurate originator and beneficiary information.

The Bank will conduct customer due diligence on a risk-sensitive basis to ensure our limited resources are focused on the higher risk accounts and/or transactions. The following category would be used:

- **Simplified Due Diligence**

Where an account is of inherently low risks, the Bank shall apply reduced or simplified measures. There are low risks in circumstances where the risk of money laundering or terrorism financing is lower, information on the identity of

the customer and the beneficial owner of an account is publicly available or where adequate checks and controls exist elsewhere in national systems, or where the volume transacted in the accounts is considered low.

In the event that the Bank applies Simplified or Reduced Customer Due Diligence measures to customers resident abroad, it shall be limited to customers in countries that have effectively implemented the FATF recommendations.

The Simplified CDD measures shall not apply to a customer whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios. In such a circumstance, enhanced due diligence shall become mandatory.

- **Enhanced Due Diligence (EDD)**

Enhanced Due Diligence is applied where the account/relationship is deemed to be high risk in nature. An increased level of monitoring of such account would be carried out. It goes as far as identifying the beneficial owners of entities and understanding their line of business.

The Bank shall perform enhanced due diligence for high risk categories of customer, business relationship or transaction.

## **20.0 Reporting**

The Chief Compliance Officer shall render reports on unusual funds transactions to the Committee of Governors' (COG).

## **21.0 Other AML/CFT Reports to be rendered**

The CCO shall collate and present the exceptions noted to the Bank's management and the audit committee of the Board.

Items	Description	Frequency
Special Reports on Funds Transactions (SRFT)	Reports of all customers' transaction above one	Monthly

	hundred million naira (₦100m)	
Swift Sanction Screening Reports	Reports of all customers' foreign transactions screened on the SWIFT sanction screening system.	Monthly
Testing for adequacy of AML/CFT Compliance	The CCO is required to test and determine the adequacy of the AML/CFT framework and identify areas of potential risks not covered by the AML/CFT Regulation.	Bi- annually (June and December)
New Areas of AML/CFT Risks	The CCO is required to review, identify and record other areas of potential money laundering risks not covered by the Regulation and report same to the Board Audit Committee.	Monthly

The following returns/actions are required to be provided by various SBUs and Branches under the regulation:

Items	Description	Frequency
Special Reports on Funds Transactions (SRFT)	Reports of all customers' transactions above one hundred million naira (₦100m). (See appendix B for report format)	Weekly
Employee Money Laundering Education and Training Programmes	Capacity Development Department shall develop an action plan for training in collaboration with AML/CFT Compliance Office of Governors' Department and other regulatory Departments.  Capacity Development Department is required to render quarterly returns on their level of compliance with the training plan to the Governors' Department.	Annually  Bi-Annually
Hiring of new employees	Human Resources Department should screen and obtain clarification from Banking Supervision Department that prospective employees had not been black listed from working in the banking industry.	Report to be part of documentation for approval to hire
Additional procedures and mitigants	Based on test of adequacy conducted, the CCO is required to design additional procedures and mitigants as contingency plan. These will provide how such potential risks will be appropriately managed if they crystallize. Details of the contingency plan are to be presented to the COG.	Bi-Annually (June and December)

Testing for the Adequacy of the AML/CFT Compliance Program every financial year.	The AML/CFT Compliance Program is to be independently tested by the Internal Audit Team to determine its adequacy, completeness and effectiveness. Report of compliance is required to be rendered to the COG.	Annually
Returns on United Nations Security Council Resolutions(UNSCRs) and other Terrorism Financing designated sanction lists	Information Technology Department to deploy appropriate software/ technology.	As the need arises

## **PART 2: PROCEDURES**

The general principles and means of obtaining satisfactory identification evidence are set out below:

### **22.0 Nature and Level of the Business**

The Bank shall obtain sufficient information on the nature of the business that the prospective customer intends to undertake, including the expected or predictable pattern of transactions. The information collected at the outset for this purpose shall include:

- a. Purpose and reason for opening the account or establishing the relationship
- b. Nature of the activity that is to be undertaken
- c. Expected origin of the funds to be used during the relationship
- d. Details of occupation/employment/business activities and sources of income.

The Bank shall keep the information up to date as the opportunities arise, such as when an existing customer opens a new account or when there are changes to the mandate of the account.

Information obtained during any meeting, discussion or other communication with the customer shall be recorded and kept in the customer's mandate file to ensure that current customer information is readily accessible to the Anti-Money Laundering Compliance Office.

Particular attention should be made to these customers when conducting due diligence:

#### **Politically Exposed Persons (PEPs)**

- b. Non-face to face relationship.
- c. Non-Governmental Organizations (NGOs)
- d. Off-shore Correspondence Accounts
- e. Ministries, Departments and Agencies (MDAs)

## **23.0 Means of Identification**

All institutions wishing to establish account or business relationship with the Bank shall provide proof of address, while operators of the account shall be required to provide other forms of identification, such as international passport/driver's license/national identity card and Bank Verification Number (BVN).

## **24.0 Sanction Screening**

All transfers to third parties are to be screened against the sanction lists. The sanction lists will be updated periodically by the Administrator in line with releases by relevant service providers.

## **25.0 Whistle-Blower Protection**

Employees play an important role in raising issues and concerns which help the Bank better identify, address and deter money laundering and terrorism financing. The Bank has adopted whistle-blower protection to ensure that it provides a safe environment for reporting and addressing suspected non-conformity with the provisions of this manual.

Reports of violations or suspected violations shall be kept confidential and consistent with the need to conduct an adequate and independent investigation and protect the identity of the whistle blower at all times.

Whistle blowers shall be protected by the Bank if they are threatened or likely to be exposed to risk as a result of reporting any unethical conduct. An employee who harasses or threatens a whistle blower shall be disciplined in line with the provisions of the *Human Resources Policy and Procedure Manual (HRPPM)*.

## **26.0 Periodic Customer Review**

Risk management is an ongoing process throughout the life of the relationship and as such reassessments must be carried out on a periodic basis. The period is determined by the initial risk assessment given to the customer at account opening. The customer's information should be updated as follows:

- High risk clients 2 year cycle.
- Medium risk clients 4 year cycle

- Low risk clients 5 year cycle.

However, it is to be noted that an event can trigger a risk re-assessment review outside the aforementioned cycle i.e. "Event Driven Review" e.g. where there is a sudden change in the leadership or account signatories of the MDA or financial institution.

## **27.0 KYC Documentation Requirements**

The Bank shall obtain from the prospective customers the minimum KYC documentation as stated in appendix A in this manual for all MDAs.

For other business relationships, the affected SBUs and Branches shall obtain the minimum KYC requirements.

## **28.0 Record Keeping**

The law requires that records of customers' transactions be kept for a minimum period of five (5) years after the transaction has been consummated. For the purpose of this Manual, customers' transactions records shall be kept for a minimum of five (5) years, whether or not the customer has ceased business relationship with the Bank.

The Bank shall maintain customers' records of identification, account files and business correspondence for as long as the relationship subsists and at least five (5) years following the termination of an account or business relationship and shall make available such records as may be required by the AML/CFT Compliance Office from time to time.

SBUs and Branches would retain records of customer identification and transactions. This is both for internal audit purposes and in order to enable the authorities to investigate and trace laundered money when necessary.

The Bank will maintain records of all suspicious or large transactions identified and what decision was reached.

Records are kept for a minimum period of five (5) years as may be required by the Law from the date of the last transaction.

## **29.0 Account Monitoring**

Occasionally customers may seek to deliberately build up a degree of trust before they use their account for criminal or/and terrorist financing purposes. Customers may be involved in money laundering and terrorist financing, therefore any product or service offered by the Bank is a potential medium for either activity.

The nature of business must be recorded when the account is opened and that is the initial yardstick by which staff will measure whether the account is being conducted in line with the expectations or whether suspicious transactions are being passed through. It is the early period of a new customer relationship that represents the greatest vulnerability and warrants close attention.

It is also vital that the Bank accepts every opportunity to update information on customers in order to maintain a high standard of monitoring. Attention should also be given to ensuring that documentation is reviewed on a regular basis and is automatically updated when events such as change of address or change of signatories occurs.

Identification of any of the types of transaction does not automatically establish suspicion, but should arouse prompt enquiry and consideration of the circumstance. Hence, there is need for good Know Your Customer (KYC)/Know Your Customer's Business (KYCB) knowledge and records.

Whereas the primary responsibility for identifying suspicious transactions lies with the staff processing or checking items. The Bank, as an additional safeguard, shall deploy appropriate software/technology that will generate report for suspicious transactions that are scrutinized by the Chief Compliance Officer.

On risk assessment basis, customer information must be updated during general communication with customers. This information must include but is not limited to the names of current directors (if applicable), type of business and volume to be expected

over the account. It also gives the customer the opportunity to inform the Bank of any new areas of business intended.

Consequently, the Bank will be able to see if there are any material changes to the organization. Such information is an integral part of the KYC process and must be kept up to date.

### **Special Reports On Funds Transactions (SRFT)**

#### **Identification**

When a transaction or suspicious transaction whether or not it relates to the laundering of the proceeds of a crime or an illegal act –

- Involves a frequency which is unjustifiable or unreasonable,
- Is surrounded by conditions of unusual or unjustified complexity; or
- Appears to have no economic justification or lawful objective,

The Bank shall obtain information from the customer as to the origin and destination of the funds, the aim of the transaction and the identity of the beneficiary. All transactions falling into this category shall be reported to the AML/CFT Office within 7 days after the occurrence of the transaction using the template provided.

The Bank will acquire an AML Software, for the purpose of identifying potential suspicion in customers' activities and for filtering transactions.

Notwithstanding the software in place at the Bank, it is still the responsibility of every branch operatives to file any unusual transaction that may be grounds for suspicion of Money Laundering and Terrorist Financing which might not adequately be captured by the software.

### **30.0 Investigations (Alert Review and enquiry)**

When a transaction falls within the definition covered by this Compliance Manual, the authorized Staff of the Branch where the transaction occurs shall immediately follow the procedure below:

- Seek information from the customer as to the source of the funds, the purpose of the transaction and the identity of the beneficiary.

- The Branch Controller/Head of SBUs shall make a formal report to the AML/CFT Compliance Office within 2 days of the determination of the occurrence of the suspicious transaction.
- Upon receipt of the report, the AML/CFT Compliance Office shall carry out a careful check on the transaction to enable it form an opinion whether it falls within the definition given above.
- The CCO shall designate an Officer to promptly review account/transactions in conjunction with the compliance officer in the SBU or Branch. Every action taken shall be recorded.
- The CCO shall carry out further evaluation and form final opinion on whether the transaction qualifies to be lodged as SRFT or not.
- Once this is established, the CCO will cause a detailed report on the matter containing all relevant information on the matter.
- The Chief Compliance Officer (CCO) shall promptly process the reports and escalate those that are deemed questionable to COG for prompt approval for actions.

### **31.0 Documentation of closed Alerts**

All alerts reviewed and found not to be suspicious will be filed and closed.

### **32.0 Training**

The CCO shall ensure adequate training of staff on AML/CFT compliance issues and act as a contact point within the Bank to provide answers to compliance queries from respondent Banks and staff members. The Office shall also help in establishing written guidance for staff on the appropriate compliance with laws, rules and standards through policies and procedures and other documents such as compliance manuals, codes of conduct and practice guidelines.

At a minimum, all new employees must receive formal training within 60 days of their joining the Bank. This training should cover local anti-money laundering laws, Anti-Money Laundering Policy and Procedures, and recognizing and reporting Suspicious

Transactions (employee responsibilities and examples of suspicious activity, "red flags").

AML/CFT Compliance Office must maintain a record of all formal training, to include the names and positions of the participants, for at least 5 years.

Annually all staff are targeted to attend AML refresher training to update them of all new developments including information on current Money Laundering ML/ FT techniques, methods and trends; ML red flags; KYC requirements; customer transaction monitoring and suspicious transaction reporting; new changes in the Global AML world and local regulations.

### **33.0 Internal Control and Independent Testing**

#### **Independent Testing**

An important component of an AML Program is an independent test or audit of the program. The independent test requirement must be performed, either internally or externally, by parties independent of the creation of the business' AML procedures. In most cases, this testing is performed by Internal Audit Department. To supplement this independent test, there are several other internal controls to be performed by AML/CFT Compliance Office.

#### **Internal Audit Department**

The scope and breadth of the activities of the AML/CFT compliance function shall be subject to periodic review by the internal audit function. An audit programme which covers the adequacy and effectiveness of the Bank's compliance function should be established, including testing of controls commensurate with the perceived level of risk.

### **34.0 APPENDICES:**

- A. KYC Requirements for opening Government Accounts - Federal, State and Local Governments and their Parastatals Documentation

Documents	Waiver	Deferral	Approving Authority	Period of Deferral
Duly Completed Account Opening Form	Not Allowed	Not Allowed	D/G (Operations)	N/A
Completed KYC Form for each of the signatories	Not Allowed	Not Allowed	D/G (Operations)	N/A
Completed individual Signatory customer's personal information form.	Not Allowed	Not Allowed	D/G (Operations)	N/A
Two (2) Recent Passport Photographs of each of the Signatories	Not Allowed	Not Allowed	D/G (Operations)	N/A
Two Completed Mandate Cards	Not Allowed	Not Allowed	D/G (Operations)	N/A
Certified copy of official gazette establishing the Ministry/Government /Agency or Parastatal	Not Allowed	Not Allowed	D/G (Operations)	N/A
Letter of authority from the Accountant General of the Federation or State Government as the case may be. For Local Government, the letter should be signed by Council Manager, Treasurer, Chairman and Accountant General for Local Government.	Not Allowed	Not Allowed	D/G (Operations)	N/A
Application letter from the Head Ministry/Agency/Parastatal with details of signatories to the account.	Not Allowed	Not Allowed	D/G (Operations)	N/A
Acceptable Means of Identification for each of	Not Allowed	Not Allowed	D/G (Operations)	N/A

the Signatories				
<ul style="list-style-type: none"> <li>- National ID</li> <li>- Resident's Permit</li> <li>- Bank Verification Number (BVN)</li> <li>- International Passport</li> <li>- Driver's License</li> </ul>				
Report of verification/confirmation done at the office of the Accountant General/ Chairman of Local Government conducted by a designated staff of the Bank	Not Allowed	Not Allowed	D/G (Operations)	N/A
Duly Completed Address Verification Form of the MDA's address	Not Allowed	Not Allowed	D/G (Operations)	N/A

B. Reporting Format for Special Report on Funds Transactions (SRFT)

<b>DEPT./BRANCH:</b>		<b>CENTRAL BANK OF NIGERIA</b>												
<b>SPECIAL REPORTS ON FUNDS TRANSACTIONS (SRFT)</b>														
<b>Special Transactions Reporting Form:</b>														
S/No	Report Date	Reference No	Name Of Customer	Customer Address	Telephone	Acc t Ty pe	Ac ct No	Acco unt Statis	Transac tion Date	Transac tion Type	Transact ion Details	Amo unt	Purpose Of Transaction	Source Origin Of Funds

**Notes:**

**Value of transactions to be reported should be from N100 million Naira and above**

**Transaction Type should be either INFLOW or OUTFLOW**

**Reporting Officer:**

Name of Reporting Officer:	
Status:	
Signature:	

**Approving Officer:**

Name of Approving Officer:	
Status:	
Signature:	

## C. The FATF Recommendations

### INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION

#### A – AML/CFT POLICIES AND COORDINATION

- 1 - Assessing risks & applying a risk-based approach
- 2 - National cooperation and coordination

#### B – MONEY LAUNDERING AND CONFISCATION

- 3 - Money laundering offence
- 4 - Confiscation and provisional measures

#### C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION

- 5 - Terrorist financing offence
- 6 - Targeted financial sanctions related to terrorism & terrorist financing
- 7 - Targeted financial sanctions related to proliferation
- 8 - Non-profit organisations

#### D – PREVENTIVE MEASURES

- 9 - Financial institution secrecy laws

#### *Customer due diligence and record keeping*

- 10 - Customer due diligence
- 11 - Record keeping

#### *Additional measures for specific customers and activities*

- 12 - Politically exposed persons
- 13 - Correspondent banking
- 14 - Money or value transfer services
- 15 - New technologies
- 16 - Wire transfers

#### *Reliance, Controls and Financial Groups*

- 17 - Reliance on third parties
- 18 - Internal controls and foreign branches and subsidiaries
- 19 - Higher-risk countries

#### *Reporting of suspicious transactions*

- 20 - Reporting of suspicious transactions
- 21 - Tipping-off and confidentiality

#### *Designated non-financial Businesses and Professions (DNFBPs)*

- 22 - DNFBPs: Customer due diligence
- 23 - DNFBPs: Other measures

## **E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS**

- 24 - Transparency and beneficial ownership of legal persons**
- 25 - Transparency and beneficial ownership of legal arrangements**

## **F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES**

### ***Regulation and Supervision***

- 26 -Regulation and supervision of financial institutions**
- 27 - Powers of supervisors**
- 28 - Regulation and supervision of DNFBPs**

### ***Operational and Law Enforcement***

- 29 - Financial intelligence units**
- 30 - Responsibilities of law enforcement and investigative authorities**
- 31 - Powers of law enforcement and investigative authorities**
- 32 - Cash couriers**

### ***General Requirements***

- 33 - Statistics**
- 34 - Guidance and feedback**

### ***Sanctions***

- 35 – Sanctions**

## **G – INTERNATIONAL COOPERATION**

- 36 - International instruments**
- 37 - SRV Mutual legal assistance**
- 38 - Mutual legal assistance: freezing and confiscation**
- 39 - Extradition**
- 40 - Other forms of international cooperation**

### 35.0 APPROVALS

S/N	AUTHORIZING OFFICER	DESIGNATION	SIGNATURE AND DATE
1.	ADEMOSU, Moses A	Asst. Director, GVD	Moses A. Ademosu
2.	Ogeado, S-N.	Deputy Director, GVD	S-N. Ogeado
3.	Ifechukwu Anthony	Director, GVD	Anthony Ife
4.	O. J. Nnanna, Ph.D	Deputy Governor, FSS	O. J. Nnanna
5.	EMEFIELE, GI	Governor, CBN	Emefiele