FCMB Enterprise Risk Management

(Compliance Risk Management)

Know Your Customer

Anti-Money Laundering

&

Countering Financing of Terrorism and Proliferation Manual

Table of Contents

1. INTRODUCTION.

1.1 POLICY STATEMENT

First City Monument Bank (**FCMB**) is committed to:

a. Implementing sound anti-money laundering and countering financing of terrorism & proliferation policies and procedures which will ensure that it is not used as a conduit for money laundering or financing of other illicit businesses;

b. Implementing policies, procedures, guidelines and provisions of manuals emanating from relevant regulatory bodies towards ensuring compliance with all domestic and international laws and regulations on money laundering and countering financing of terrorism and proliferation in order to mitigate AML/CFT risks it is exposed to;

c. Full compliance with both the letter and the spirit of all regulatory requirements and high standard of market conduct;

d. Conducting all banking and investment business in accordance with all regulatory policies and guidelines governing its operating environment;

e. Giving full cooperation to law enforcement authorities within the limits of the rules governing confidentiality;

f. Effective communication of these policies towards raising the level of staff awareness on AML/CFT issues;

g. Retention and preservation of records of customers' transactions for a minimum of five years or as may be prescribed by various regulatory bodies;

h. Exiting relationships which pose heightened money laundering risks to the bank and reporting same to the relevant regulatory agencies.

Drawing significantly from recommendations of the *Basel Committee* on Banking Regulations and Supervisory Practices, the *Wolfsberg* Group principles, Financial Action Task Force recommendations, provisions of the Money Laundering (Prohibition) Act as amended and CBN AML/CFT Regulations, the Bank has put in place the following measures in the attainment of its objective of ensuring full compliance with the letter and the spirit of all applicable laws and regulations.

The Bank

i. has established sound internal policies, controls, procedures to mitigate money laundering and financing of terrorism risks.

ii. regularly trains its staff to identify suspicious activities/transactions and to take appropriate actions.

iii. has in place and updates the AML/CFT employee training programmes for new hires and regular refresher trainings for existing staff.

iv. has internal referral process and procedures for compliance matters.

v. ensures implementation of policies and procedures and internal controls to correct/enhance and/or adapt to regulatory changes / deficiencies.

vi. has designated a senior management staff as its Chief Compliance Officer to oversee its AML/CFT program

1.2 PURPOSE

This manual forms an integral part of the bank's Compliance Risk Management Framework.

The essence of this AML/CFT Manual is to:

a. Document the comprehensive and constantly evolving policies, procedures and processes deployed by First City Monument Bank to assure adherence to the provisions of AML/CFT legislations and guidelines in Nigeria and all jurisdictions where our businesses are located.

b. Create a framework for managing AML/CFT compliance risks in the bank.

c. Ensure that the bank does not fall victim of illegal activities perpetrated by its customers.

d. Specify basic expectations of all staff with as regards their obligations for the management of AML/CFT risks.

It should be noted that this Manual is not a static document; it will continue to

change to reflect changes in both the laws and regulations themselves and in best practice, and staff should expect to receive regular updates. The regulations embody good business practice and reflect the high level principles for businesses laid down by the CBN. It is essential for FCMB to maintain a high reputation for professionalism and for acting in accordance with best practice.

1.3 ROLES AND RESPONSIBILITIES

The Board

The roles and responsibilities of the Board of Directors with respect to AML/CFT Compliance Risk Management include (but shall not be limited to):

Assume overall accountability for Compliance performance

i. Ensure that appropriate AML/CFT Compliance Risk Management framework is established and is in operation;
ii. Approve the AML/CFT Compliance Risk Management program and policies;
iii. Provide guidelines regarding the management of AML/CFT Compliance risks;
iv. Appoint and designate a Chief Compliance Officer (in line with CBN guidelines) to coordinate and monitor AML/CFT Compliance by the bank.

Management

Management is responsible for the business and Compliance as part of their business activities. Management's responsibilities would include the following:

(i) Lead by example in enforcing integrity and in fostering an open and receptive attitude towards Compliance;

(ii) Ensure that each employee's job description and employment letter state that he or she is responsible for compliance in his or her area of work;

(iii) Ensure that each employee under their charge is aware of, understand and adhere to the Manual and all applicable laws, regulations and standards (through for example ensuring sufficient training for new employees, and periodic refresher training for existing employees);

(iv) Ensure that the unit conducts periodic assessment of its compliance risks;

(v) Ensure that adequate controls are in place to mitigate the identified compliance risks;

(vi) Ensure that compliance issues and potential issues are handled promptly and effectively; Report all material compliance issues and potential issues to next level Management and Compliance Unit, and seek appropriate guidance when in doubt;

(vii) Deal with all instances of non-compliance promptly and fairly, including dealing with violators in a way that emphasizes the importance that FCMB attaches to compliance matters;

(viii) Encourage active cooperation and feedback among all FCMB employees by creating open lines of communication with Compliance, Internal Audit and other control functions;

(ix) Cooperate fully with any inspection, audit, testing and query from regulators, Compliance, Internal Audit and other control functions;

(x) Follow up actively on all recommendations from regulators, Compliance, Internal Audit and other control functions; and

(xi) Ensure sufficient resources, Management's support and access for the unit to carry out (i) – (x) in a timely and effective fashion.

Chief Compliance Officer

i. Coordinate and monitor AML/CFT Compliance by the bank;

ii. Inform Board and Management of AML/CFT Compliance efforts, compliance failures and the status of corrective actions;

iii. Monitor implementation of the code of corporate governance;

iv. Ensure implementation of Board decisions on compliance matters;

v. Ensure that regulatory changes are effectively implemented in the bank;

vi. Direct prompt investigation of any unusual or suspicious transaction and reports to the Regulatory body;

vii. Ensure that compliance requirements are integrated into the day to day activities of the bank and that processes are efficient and in accordance with applicable laws and policies.

AML/CFT Compliance Officer

i. Coordinate and monitor day to day compliance with applicable money laundering laws and regulations;

ii. Monitor transactions to detect any unusual or suspicious transactions.

iii. Conduct Preliminary investigation on any unusual or suspicious transaction.

iv. Prompt preparation and delivery of all relevant returns to the regulatory bodies in line with the MPLA 2011 (as amended) and CBN AML/CFT Regulation (2013)

v. Communicate AML/CFT issues to all stakeholders

Branch/Zonal Compliance Officers

Zonal Compliance Officers shall be appointed and designated as compliance officers in charge of branches under them and shall perform the following functions:

i. Monitor money laundering activities in the branch

ii. Ensure adherence to KYC and KYCB principles.

iii. Coordinate submission of suspicious transactions report to the Chief Compliance Officer

iv. Coordinate collation of documents as may be requested from time to time.

v. Ensure full implementation of the Bank's policy and statutory regulations on compliance and money laundering activities.

vi. Ensure swift resolution of corrective action grid on all inspection reports i.e. statutory / Group reports, e.g. CBN, NFIU, NDIC, Group Internal Audit Reports, Control reports, etc

vii. Create awareness among branch staff on Compliance and anti-money laundering activities.

Group Internal Audit

i. Incorporate compliance testing in their normal audit program.

ii. Report on results of the independent testing to the Board through the GMD/CEO

All Employees:

i. Familiarize themselves with guidelines, manuals, handbooks and best practices relating to their respective areas of responsibility and implementing the measures and approaches prescribed diligently and to the best of their ability;

ii. Report any legal violations or other forms of misconduct in accordance with FCMB policies and procedures so that any such issues can be duly addressed;

iii. Report suspected money laundering activities to the Chief Compliance Officer

1.4. SCOPE

This manual is applicable to FCMB and its subsidiaries.

2. COMPANY BACKGROUND

2.1 BRIEF HISTORY

First City Monument Bank (FCMB) is a full service banking group, headquartered in Lagos, Nigeria

FCMB is the flagship company of the First City Group, one of Nigeria's leading comprehensive financial services providers. From its early origins in investment banking as City Securities Limited in 1977, FCMB (established in 1982) has emerged as one of the leading financial services institutions in Nigeria, a top 10 bank with subsidiaries that are market leaders in their respective segments.

First City Monument Bank ('the Bank'/'FCMB') was incorporated as a private limited liability company on 20 April 1982 and granted a banking licence on 11 August 1983. On 15 July 2004, the Bank changed its status from a private limited liability company to a public limited liability company and was listed on the Nigerian Stock Exchange by introduction on 21 December 2004.

The Bank completed the acquisition of FinBank in February 2012 and subsequently merged with FinBank in October 2012. Following the merger, the FCMB Group now has 2 million customers, 233 branches and cash-centres spread across every state of the Federal Republic of Nigeria and a presence in the United Kingdom (through its FSA-authorised investment banking subsidiary, FCMB UK)

Over the years, the bank has received several awards for outstanding financial performance, superior management and dedication to excellence. Some of these awards include:

- The prestigious *ThisDay* Award for the "Stock Offer of The Year" in 2005, an acknowledgement of the success of our capital raising activities in a highly competitive period in the industry
- In 2000 and 2001, FCMB Capital Markets won the Reuters/SBA Research Mergers & Acquisition Award as the leader in Mergers & Acquisition in Nigeria
- Between 1993 and 1998, FCMB won the coveted trophy for the most consistent issuing house in Nigeria.

2.2 OPERATIONAL PERFORMACE

We currently operate in over 233 branches with a strategic nationwide spread. We have deployed a robust and scalable banking technology application to offer seamless service delivery through various electronic channels.

Having successfully transformed to a retail and commercial banking-led group, the Bank expects to continue to distinguish itself by delivering exceptional service and taking its unique brand of supportive banking to every household in Nigeria.

2.3 OUR VISION, MISSION AND BEHAVIOURAL ATTITUDE

Our Vision

To be the Premier Financial Services Group of African Origin.

Our Mission

To attain the highest levels of customer advocacy, be a great place to work, and deliver superior and sustainable returns to our shareholders

Our Core Values

Professionalism - Ensuring we play by the rules

Sustainability - Ensuring we develop capacity to endure

Customer Focus - Advancing customer advocacy

Excellence - Aiming for the highest operating standards.

3.0 DEFINITIONS OF ACRONYMS AND TERMS

3.1 ACRONYMS

- **AML - Anti Money Laundering:** Refers to policies, procedures and controls which are instituted to prevent, detect and report money laundering activities.
- **CBN - Central Bank of Nigeria:** The apex bank of Nigeria and a regulator to all banks in Nigeria. It supervises all Banking practices and operations as it relates to Banks and the public or bank and another Bank or between a Bank and itself.
- **CCO - Chief Compliance Officer:** A senior official who is a Statutory Officer by virtue of Section 9(1a) of MLPA 2011, who interfaces between Management and Staff, Organizations, Regulatory and Law Enforcement Agencies on all issues pertaining to money laundering and financing of terrorism.
- **CO – Compliance Officer:** A statutory official of a financial institution by virtue of Section 9(1a) of MLPA 2011, who interfaces with staff and Organizations, Regulators and Law Enforcement Agencies on all issues pertaining to money laundering and reports to the CCO.
- **CDD – Customer Due Diligence**: This means taking steps to identify your customer and checking that they are who they say they are. In practice this means obtaining the following from a customer:
    - name
    - photograph on an official document which confirms his identity
    - residential address
- **CTRs – Currency Transaction Reports:** This is made by financial institutions and designated non-financial institutions regarding any transaction, lodgment or transfer of funds in excess of N5,000,000 or its equivalent, in the case of an individual, or N10,000,000 in the case of a

corporate body pursuant to Section 10 of the ML(P)A, 2011.

- **EFCC- Economic and Financial Crimes Commission**: A Federal Government agency which is charged with the responsibility of coordinating the various Institutions involved in the fight against money laundering and enforcement of all laws dealing with economic and financial crime.

- **FATF – Financial Action Task Force:** FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. It was established in 1989 by the G-7 Summit that was held in Paris. As a "policy making body" it works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. It is known for its 46 recommendations which establish an AML framework for its member countries. (See Appendix 1 for FATF 40 Recommendations)

- **FCMB – First City Monument Bank**

- **KYC – Know Your Customer:** Entails obtaining and verifying customer identity, Preservation of records of customers, mandatory disclosure of transactions to authorized statutory bodies.

- **KYCB – Know Your Customer's Business**: Another offshoot from the KYC where financial institutions are enjoined to know the line of business of their customers such that transactions by the customers are fairly predictable. This will assist in the identification of unusual transactions or activities that may appear inconsistent with the customer's known business.

- **MLPA** – **Money Laundering (Prohibition) Act.** A Federal legislation which deals on the policies, framework and sanctions on Money laundering for both Financial Institutions and Designated Non-Financial Persons and Businesses (DNFPBs)

- **NDLEA – National Drug Law Enforcement Agency**

- **NFIU – Nigeria Financial Intelligence Unit:** The Nigerian arm of the global Financial Intelligence Unit (FIU). It is domiciled within the Economic and Financial Crimes Commission (EFCC) as an autonomous unit. The activities of the NFIU are covered under the EFCC Act 2004 and MLPA 2011. Its core role is that it serves as the country's central agency for the intelligence information gathering, collection, analysis and dissemination of financial

information regarding money laundering and the financing of terrorism.

- **PEPs – Politically Exposed Persons:** This involves individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of Government, Politicians, Senior Government Official, Judicial or Military Officials, Senior Executives of State Owned Corporations, important Political Party Officials and any "close associate" of a senior political figure (local/foreign) all fall into this category.

- **STRs – Suspicious Transaction Reports**: This is made by financial institutions and designated non-financial institutions or made voluntarily by any person irrespective of the amount involved pursuant to **Section 6** of the MLPA, 2011.

  It is a transaction, which is inconsistent with a customer's known legitimate business or personal activities. The first key to the recognition of a suspicious transaction is in knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

3.2 TERMS

- **Management –** this refers to the Group Managing Director, Deputy Managing Director, Executive Directors, General Managers, Deputy General Managers, Assistant General Managers and Senior Managers
- **Executive Management** – this refers to the Group Managing Director, Deputy Managing Director, Executive Directors and General Managers
- **Staff** – This includes all employees of the Bank.
- **Shell Bank** – Any financial institution or bank with no fixed (physical) and registered address.

4.0 ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM POLICIES

4.1 MONEY LAUNDERING

Money Laundering is the process by which monies or assets derived from criminal activities are converted into funds or assets which appear to have a legitimate origin. It involves taking criminal proceeds and disguising their illegal sources in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities.

Money Laundering empowers corruption and organized crime where corrupt public officials and criminals are able to launder proceeds from crimes, bribes, kick-backs, public funds and on some occasion, even development loans from international financial institutions. Organized criminal groups want to be able to launder the proceeds of drug trafficking and commodity smuggling through the financial systems without a trace. In the modern day definition, Money Laundering now covers various predicate offences including child trafficking, prostitution, etc

Money Laundering Predicate Offence

Money laundering predicate offence is the underlying criminal activity that generates proceeds, which when laundered, results in the offence of money laundering. These include kidnapping, illegal restraint and hostage taking, insider trading and market manipulation, embezzlement & fraud, bribery and corruption, robbery, drug trafficking, environmental crimes, terrorism, counterfeiting currency, counterfeiting and piracy of products, smuggling, extortion, forgery, sexual exploitation, etc

Stages of Money Laundering

Placement

The physical disposal of cash/property derived from criminal activity. The purpose of this stage is to introduce proceeds into the traditional or non –traditional financial system without attracting attention e.g. purchase of artwork, cash deposits, casinos etc.

Layering

This involves separating source of proceeds from ownership by changing the form. This is designed to hamper audit trail e.g. Complex wire transfers, resell of assets/properties, opening of several accounts to disguise origin of funds etc

Integration

Re – channeling the laundered funds back to the financial system as legitimate funds.

Money Laundering laws apply not only to criminals who try to launder their ill- gotten gains, but also to financial institutions and their Employees who participate in those transactions, if the employees know that the property is criminally derived. "Knowledge" includes the concepts of "willful blindness" and "conscious avoidance of knowledge". Thus, employees of a financial institution whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, may be considered under the law to have the requisite "knowledge"

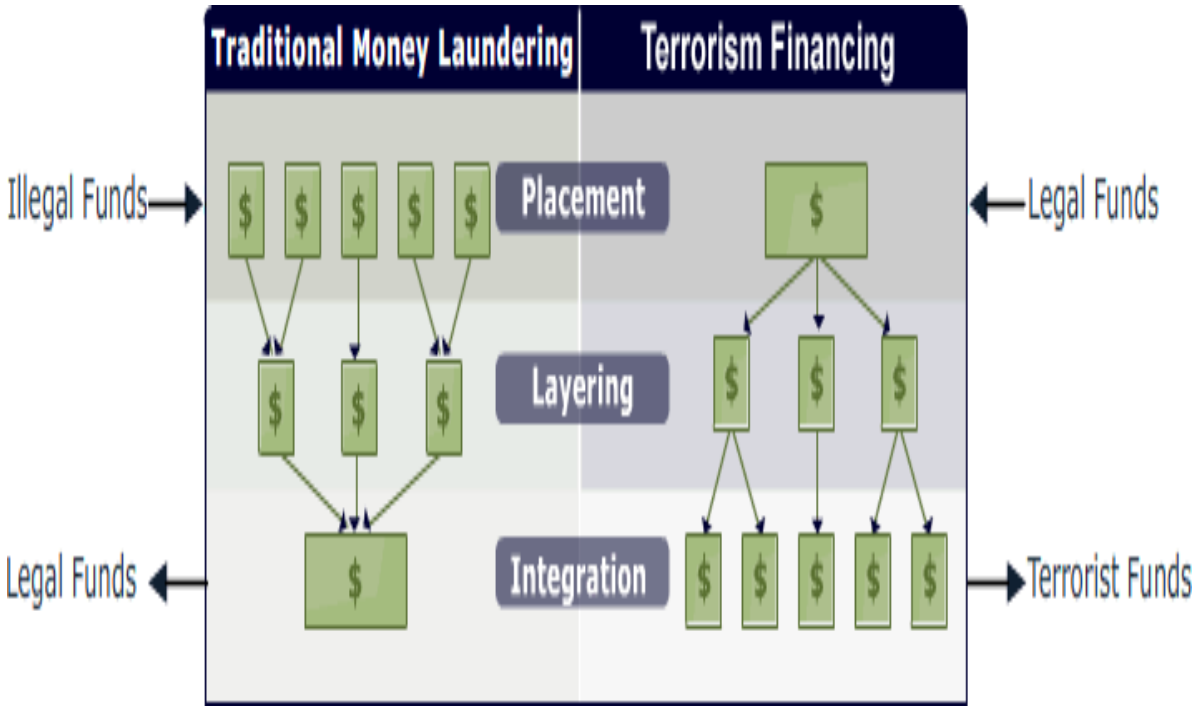
4.2 TERRORISM AND TERRORISM FINANCING

Terrorist act – any act intended to cause death or serious bodily injury to a civilian or any other person not taking an active part in the hostilities. Usually, the purpose is to intimidate a population or to compel a government or society to do or abstain from doing any act

Terrorism financing (TF) occurs when a person by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such the funds will be used or in the knowledge that the funds will be used in full or in part, in order to carry out a terrorist act.

Terrorist activities are sometimes funded from the proceeds of illegal activities. Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

Difference between Money Laundering and Terrorism Financing



4.3 REGULATORY AND LEGAL FRAMEWORK

Nigerian financial institutions are monitored for money laundering by some organisations/agencies and under the provisions of the regulations specified below:

Institutional Framework - Local

- *Economic and Financial Crimes Commission (EFCC)*
- *Nigeria Financial Intelligence Unit (NFIU)*
- *National Drug Law Enforcement Agency (NDLEA)*
- *Central Bank of Nigeria (CBN)*
- *Federal Ministry of Commerce (FMC)*
- *Independent Corrupt Practices Commission (ICPC)*
- *Federal Inland Revenue Services (FIRS)*
- *National Insurance Commission (NAICOM)*
- *Nigeria Customs Service (NCS)*
- *Nigeria Immigration Services (NIS)*
- *Nigeria Deposit Insurance Corporation (NDIC)*
- *Securities and Exchange Commission (SEC)*

Institutional Framework – International

- *Basel Committee on Banking Supervision*
- *Financial Action Task Force (FATF)*
- *Inter-Governmental Group Against Money Laundering (GIABA)*
- *Egmont Group (of Financial Intelligence Units)*
- *Wolfsberg Group*
- *United Nations Office of Drugs and Crime (UNODC)*
- *The World Bank*
- *European Union*
- *Interpol*

- *The Joint Money Laundering Steering Group*

Legal Framework – Local

- *Money Laundering (Prohibition) Act 2011*
- *Terrorism (Prevention) Act 2011*
- *CBN AML/CFT Regulations 2013*
- *SEC Rules and Regulations 2011*
- *Advanced Fee Fraud Act 2006*
- *Bank's (recovery of Debt) and Financial Malpractices in Banks in Nigeria Act (as amended)*
- *Banks and other Financial Institutions Act 1991*
- *ICPC (Establishment) Act*
- *EFCC (Establishment) Act 2004*
- *NDLEA Act*
- *Dishonored Cheques Act, etc*

Legal Framework – International

- *Directive 2005/60/EC of the European Parliament and of the Council.*
- *Office of Foreign Asset Control (OFAC)*
- *USA PATRIOT Act : Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*
- *Sarbanes-Oxley Act*
- *FATF 40 Recommendation*

4.4 CUSTOMER IDENTIFICATION PROGRAM (CIP)

The Customer Identification Program is intended to enable the bank form a reasonable belief that it knows the true identity of each customer.

As a general rule, a business relationship with FCMB will NOT be established until the identity of a potential customer is satisfactorily established. Where a potential customer declines to provide any account initiation information, the relationship will not be established. Furthermore, if follow-up information is not forthcoming, any relationship already established will be terminated.

The Bank's account opening procedures which also specify the identification documents and information required from each customer are contained in the bank's Operations Policy Manual

KNOW YOUR CUSTOMER (KYC)

KYC is the due diligence that financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information before doing financial business with them.

A customer for the purpose of our **KYC** policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the Bank.
- One on whose behalf the account is maintained (i.e. the beneficiaries).
- Beneficiaries of transactions conducted by professional intermediaries (3rd Party Account) such as Lawyers, stockbrokers etc.
- Any person or entity connected with a financial transaction, which can pose significant reputational or other risks to **FCMB**. An example is a wire transfer or issue of high value demand draft as a single transaction.

Our approach to KYC is from a wider prudential, not just anti-money laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

To this end, the Bank's KYC policies and procedures emphasize the following:

i. Obtaining the necessary documents and information from every customer as specified in the Bank's Operations Policy manual

ii. Prohibition of opening numbered or anonymous accounts or accounts in fictitious names

iii. Minimum acceptable identification evidence for low risk and low value accounts

iv. Independent verification of the legal status of incorporated entities and sole proprietorships with the Corporate Affairs Commission in writing

v. Screening of customer information against database of individuals and entities subject to sanction (watch-list check) at on-boarding stage and quarterly customer database scan as required by the AML/CFT regulations

vi. Identifying the customer as well as the beneficial owners and verifying that customer's identity using reliable, independent source documents, data or information

vii. Profiling of customers such that transactions by our customers are fairly predictable.

viii. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

ix. Customer information update whenever the need arises

x. Obligation to report to the regulatory authorities suspicious transactions, which may ultimately have a bearing with money laundering activities

The Bank as a matter of policy does not transact business with "shell corporations" as described under the International Conventions.

The bank applies each of the CDD measures under but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

The measures to be taken shall be consistent with any guidelines issued by competent authorities.

The bank shall perform enhanced due diligence for higher risk customers, business,

relationships or transactions including-

a. Non-resident customers;

b. Private banking customers;

c. Legal persons or legal arrangements such as trusts that are personal-assets-holding vehicles;

d. Companies that have nominee-shareholders or shares in bearer form;

e. Politically Exposed Persons, cross border banking and business relationships amongst others

f. Any other businesses, activities or professions as may be prescribed by regulatory, supervisory and competent authorities

4.5 FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)

The main objective of the Act is to counter offshore tax avoidance by US persons with money invested outside the US and ensuring that US persons with financial assets outside the US are paying the correct amount of US tax, e.g. US persons living outside the US, US persons hiding behind non-US companies, etc

FATCA regime is to be administered by US financial institutions and **foreign (non-US) financial institutions (FFIs)**

FATCA regulations incorporate a targeted, risk-based approach aimed at:

- Maintaining the policy objective of improved information reporting on US taxpayers with assets invested in non-US jurisdictions
- Limiting the scope of entities, obligations and accounts affected by FATCA
- Reducing due diligence and compliance burdens
- Aligning with FATCA Intergovernmental Agreements (IGAs)

Refusal by a FFI to comply may result in application of 30% withholding tax on:

- US sourced fixed or determinable annual or periodic (FDAP) income payments made to the FFI;

- US sourced gross proceeds received by the FFI

Refusal by a participating FFI's accountholders to comply with information and reporting requests may result in the FFI having to apply 30% withholding tax on withholdable payments made to their accountholders

FFIs may mitigate adverse FATCA compliance issues – e.g., obtaining deemed compliant status or qualifying for exemptions under FATCA or IGAs

4.6 THREE TIERED KYC

FCMB as a responsive institution fully supports CBN initiatives and has put measures in place to achieve financial inclusion that this initiative is meant to achieve. The bank utilises flexible account opening requirements for low value and medium value accounts which are subject to caps and restrictions as the amount of transactions increase.

Features of Low-Valued (Tier 1) Accounts:

- They are strictly savings accounts
- It allows maximum single deposit amount of N20,000.00
- It allows maximum cumulative balance of N200,000.00 at any point in time
- The basic information required for the account opening are name, place/date of birth, photograph, gender, address and telephone number
- Mobile banking allowed subject to a maximum transaction limit of N3,000 daily limit of N30,000.00

Features of Medium-Valued (Tier 2) Accounts:

- They are strictly savings accounts
- It allows maximum single deposit of N50,000.00
- It allows maximum cumulative balance of N400,000.00 at any point in time
- The basic information required for the account opening are name, place/date of birth, photograph, gender, address and telephone number
- Address verification is a requirement

- The customer information for account opening may be sent on- line (electronically)
- Allows for the use of mobile banking products, e-channels and issuance of ATM cards to customers
- Mobile banking is allowed subject to a maximum transaction limit of N10,000 and daily limit of N100,000

Characteristics of High-Valued (Tier 3) Accounts:

- It has both savings and current account features
- The Bank is required to obtain full account opening documentation requirement in line with the CBN AML/CFT Regulations 2013

Record Keeping and Retention requirements

Section 7 of Money Laundering (Prohibition) Act 2011 (as amended) states that:

A Financial Institution shall:

- preserve and keep records of a customer's identification of a customer for a period of at least five (5) years after the closure of the accounts or the severance of relations with the customer;

- preserve and keep records and related information of a transaction carried out by a customer and the report provided for in section 6 of the Act for a period of at least five (5) years after carrying out the transaction or making of the report as the case may be.

The bank shall maintain all necessary records of transactions, both domestic and international for at least five years after completion of the transaction or such longer period as may be required by the CBN or NFIU. (For more details see the bank's Records Management Policy).

Records of all suspicious transactions shall be kept for the same period.

Requests for AML records by Regulatory and Law Enforcement Agencies

Upon request by a regulatory or law enforcement agency, the bank shall make available records related to its AML/CFT Compliance or its customers as soon as possible from the date of the request.

4.7 REPORTING SUSPICIOUS TRANSACTIONS

A. Identification of Suspicious Transactions

The bank shall exercise due diligence in identifying and reporting of suspicious transaction.

Suspicious transactions shall include:

1. Transaction involving a frequency which is unjustifiable or unreasonable, unusual or has unjustified complexity.

2. Transaction which appears to have no economic justification or lawful objectives.

3. Transactions which are structured to avoid reporting and record keeping requirements.

4. Transfers of foreign currency transactions which are recalled twice from the account of a customer by correspondent bank. (Note that a first recall could be due to error.)

5. If the circumstances surrounding the first recall of a foreign currency transactions from the account of a customer by correspondence bank appeared suspicious.

6. Altered or false identification or inconsistent information or any transaction involving criminal activity in the view of the bank

Under the Terrorism (Prevention) Act 2011, banks are required to make report to the NFIU, within a period not more than 24 hours, on suspicious transactions relating to terrorism, where they have sufficient evidence to suspect that the funds:

a. are derived from legal or illegal sources but are intended to be used for any act of terrorism or;
b. are proceeds of crime related to terrorist financing; or
c. belong to a person, entity or organisation considered as terrorist

B. Procedures for Disclosure of Suspicious Transactions

1. Any Officer of the bank who suspects any transaction to be suspicious shall make an immediate report to the Chief Compliance Officer. If it occurred at the branches, it shall be drawn to the attention of the Compliance Officer of the branch/zone and then to the Chief Compliance Officer through the AML/CFT Compliance Officer in Head Office (See Appendix 2 for **STR Form**)

2. The bank has also established procedures whereby such reports are coordinated through a central point Money Laundering Reporting Officer domiciled in the Head Office for onward reporting to the NFIU/EFCC

3. In the event that urgent disclosure is required in a 'live' situation, particularly when the account concerned is part of an on-going investigation, an initial notification shall be made by telephone to the Commission

4. Staff must not disclose to customers or anyone else that they are subject to money laundering investigation. (Tipping off). FCMB, its directors, officers and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed with the competent authorities.

All suspicious transactions including attempted transactions are to be reported regardless of the amount involved. The requirement to file STRs applies regardless of whether the transactions are considered to involve tax matters or other matters

The Bank has also deployed an Anti-Money Laundering solution (SAS Money Laundering Detection application) which is a rules based application to monitor customers' transactions and flags potential suspicious transactions for monitoring by analysts. Alerts generated are reviewed and decisions to file STRs or not are documented.

C. Compilation of Reports and Returns to Regulatory Authorities

The bank shall ensure timely and accurate rendition of all AML/CFT returns as specified in the CBN AML/CFT Regulations 2009 (as amended), the Money

Laundering (Prohibition) Act 2011, the SEC Rules and Regulations as well as other relevant Regulations/Acts/Guidelines/Circulars that may be issued from time to time by various government agencies. (See the bank's Regulatory Returns Universe)

4.8 Awareness and Training

The Money Laundering (Prohibition) Act 2011 requires financial institutions to ensure, first, that its employees are made aware of the provisions of the relevant legislation and the obligations imposed on staff and financial institutions. Secondly, staff shall be given training on how to recognize and deal with transactions which may be related to money laundering or terrorist financing.

The bank's AML/CFT training program is a mix of e-learning and instructor-led training modules. The trainings incorporate current developments and changes to the MLPA 2011 and CBN AML/CFT Regulations 2009 and other related guideline. Changes to internal policies, procedures, processes and monitoring systems are also covered during the trainings

All staff are required to complete the AML/CFT training at least once in every financial year as this forms an integral part of the bank's employee appraisal system. Evidence of completion and records of attendance shall be kept by the Training Academy and shall be made available to Compliance unit on request.

The bank shall also utilize other avenues such as e-mails, compliance newsletters to disseminate compliance issues arising from new rules and regulations to all staff.

4.9 Correspondent Banking Relationship

The bank shall ensure that Correspondent-banking relationships are carefully selected. The bank shall not establish correspondent relationships with high risk foreign banks, including shell banks [1]with no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks.

4.10 Politically Exposed Persons

"Politically Exposed Persons" (PEPs) are individuals who are or have been

[1] **Shell bank is a bank that has no physical presence in any country or is not regulated*

entrusted with prominent public functions in any country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and any "close associate" of a senior political figure (local/foreign).

Business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves.

- *A senior political figure:* This includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior political figure (local/foreign).

- *Immediate Family:* The "immediate family" of a senior political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.

- *Close Associate:* A "close associate" of a senior political figure is a person who is widely publicly known to maintain an unusually close relationship with the senior political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior political figure. Although close associates are more difficult for banks to identify, they include individuals who, due to the nature of their relationship with the PEP, are in a position to conduct significant domestic and international financial transactions on behalf of the PEP.

The term PEP includes persons whose current or former position can attract publicity beyond the borders of a country and whose financial circumstances may be the subject of additional public interest.

Examples of PEPS includes, but not limited to the following:

- Heads of State or Government and Cabinet Ministers

- Governors

- Local Government Chairmen
- Senior Politicians
- Senior Government Officials
- Judicial or Military Officials
- Senior Executives of State owned Corporations
- Important Political Party officials
- Family members or close associates of PEPS
- Members of Royal Families.

PEP also include persons who are or have been entrusted with a prominent function

by an international organization, including members of senior management including directors, deputy directors and members of the board or equivalent functions other than middle ranking or more junior individuals

What is the risk in doing business with PEP?

Accepting and managing funds from corrupt PEPs can severely damage the bank's own reputation and can undermine public confidence in the ethical standards of the bank, since such cases usually receive extensive media attention and strong political reaction. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

Where to begin

As with most aspects of compliance, the place to begin is with a risk assessment. The bank conducts a risk assessment of its products/services, customers, and geographies where business is conducted. The outcome of this assessment forms the basis of a PEP/KYC compliance program.

PEP Risk Assessment

The Bank assesses the risks posed to its banking activities on the basis of the scope of operations and the complexity of the bank's customer relationships. Management establishes a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities.

The following factors are considered when identifying risk characteristics of Politically Exposed Persons:

1. Nature of the customer and the customer's business. The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor is considered for private banking accounts opened for PEPs.

2. Purpose and activity. The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account.

3. Relationship. The nature and duration of the bank's relationship (including relationships with affiliates) with the private banking customer.

4. Customer's corporate structure. Type of corporate structure.

5. Location and jurisdiction. The location of the private banking customer's domicile and business (domestic or foreign). The review considers the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or, conversely, is considered to have robust AML standards.

6. Public information. Information known or reasonably available to the bank about the private banking customer. The scope and depth of this review depends on the nature of this relationship and the risks involved

Risk Minimisation

a. Conducting detailed due diligence at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a "politically exposed person". The bank assesses the countries with which it has financial relationships.
b. Where the bank has business in countries vulnerable to corruption, it

would establish who the senior political figures in that country are and seek to determine whether or not their customer has any connections with such individuals (for example if they are immediate family or close associates).

c. The bank is more vigilant where its customers are involved in those businesses which appear to be most vulnerable to corruption.

d. Every effort is made to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

e. The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile would be regularly reviewed and updated.

f. A review at senior management or board level of the decision to commence the business relationship and regular review, on at least and annual basis of the development of the relationship.

g. Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

h. Full documentation of the information collected in line with the above. If the risks are understood and properly addressed then the acceptance of such persons becomes a commercial decision as with all other types of customers.

The Bank's obligations and position on PEP accounts

Before any account is opened for any PEP, Senior Management approval must be obtained. For this purpose, Senior Management approval must be obtained from the line Executive Director and the Chief Compliance Officer. This will be done as part of account opening formalities. No account would be opened for any PEP without the approval being in place.

The customers due diligence efforts do not end at account opening; ongoing account monitoring is expected. Activities on PEP accounts will be reviewed on a monthly basis with a view to identifying unusual and potentially suspicious

transactions related to them and filing, as appropriate, STRs related to them.

Monthly returns will be sent to the CBN and NFIU on PEP transactions. This is to assist the regulators in monitoring the activities of PEPS.

The Bank will take reasonable steps to ascertain the source of wealth and the source of funds of PEPS and report all anomalies to the CBN and other relevant authorities.

Periodic Enhanced Due Diligence and monitoring must be carried out on all PEPS by the RM and or AO concerned. On an annual basis, the relationship managers shall certify that none of the accounts reporting to them became PEP in the course of the year. In the event that any transaction is noted to be abnormal, such must be immediately flagged and reported to the Compliance unit immediately.

While circumstances will vary, certain transactions by PEPs are considered potentially suspicious and may be indicative of illegal activity.

The following guidance provides a non-exhaustive list of red flags that includes, among other things:

- Requests to establish relationships with or route transactions through an institution that is unaccustomed to doing business with foreign persons and that has not sought out business of that type.
- A request to associate any form of secrecy with a transaction, such as booking the transaction in the name of another person or business entity.
- The routing of a transaction through several jurisdictions without any apparent purpose other than to disguise the nature, source, or ownership of funds.
- The rapid increase or decrease in the funds or asset value in an account that is not attributable to market conditions.
- Frequent or excessive use of funds transfers or wire transfers either into

or out of an account.

- Large currency or bearer instrument transactions in or out of an account.

- The frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account.

Any situation falling into one of the above descriptions shall not automatically be treated as problematic until further investigation is done. If the facts point to a suspicious transaction, then procedures for filing a Suspicious Activity Report shall be followed and Senior Management notified of the situation.

4.11 Designated Non-Financial Businesses and Professions (DNFBPs)

Financial institutions are required, prior to establishing business relationship with designated non-financial businesses and Professions, to obtain evidence of registration (e.g. certificate of registration showing registration number) with the Special Control Unit on Money Laundering (**SCUML**) of Federal Ministry of Trade and Investments.

DNFBPs refer to dealers in jewelries, precious metals and precious stones, cars and luxury goods, audit firms, tax consultants, clearing and settlement companies, lawyers, notaries, other independent legal practitioners and chartered accountants, trusts and company service providers, hotels, casinos, supermarkets, real estate agents, non-governmental organizations (NGOs), religious and charitable organizations, etc.

The above DNFBPs customers include sole practitioners, partners and employed professionals within professional firms. They do not refer to "internal" professionals that are employees of other types of businesses nor to professionals working for government agencies who may already be subject to AML/CFT measures.

5.0 WHISTLE BLOWING

The Management of the bank has a duty to conduct the bank's affairs in a responsible and transparent manner and to take into account legal and regulatory requirements under which the bank operates. The Board of the bank is also committed to the principle of sound corporate governance and behavior as enunciated in the CBN Code of Corporate Governance for banks in Nigeria. One of the several ways a breach of regulatory requirements and staff misconduct can be addressed is through a whistle blowing programme.

As such, the whistle-blowing policy and procedures of the bank are designed to encourage stakeholders to bring unethical conduct and illegal violations to the attention of an internal and or external authority so that action can be taken to resolve the problem.

5.1 WHISTLE-BLOWING MATTERS

As a matter of policy, whistle-blowing is encouraged within the bank at every stakeholder levels. Any of the following matters against the bank or its officers can be brought up for investigation:

- All forms of financial malpractices and impropriety or fraud;
- Improper conduct or unethical behavior;
- Any form of criminal activity;
- Failure to comply with regulatory directive, legal obligations or statutes;
- Rendition of false returns;
- Falsification of records;
- Forgery (use of false certificates, false declaration of age, etc) ;
- Actions detrimental to Health and Safety or the environment (SEMS regulations and policies);
- Commission of offence by FCMB, officers/staff;
- Obstruction of internal/external regulators & auditors;
- Leakage of confidential data;
- Bribery and corruption;
- Abuse of authority;

- Sexual harassment;
- Insider Abuse;
- Non-disclosure of interest;
- Connected transactions;
- Concealment (including attempted concealment) of any malpractice;
- Other forms of corporate governance breaches.

5.2 WHISTLE-BLOWING PROCEDURES

1. All stakeholders will be provided with details of KPMG Ethics Line facilities via the bank's website. The KPMG Ethics Line facilities provide avenues for employees and any other person to confidentially and anonymously report all incidents relating to various categories of unethical and criminal conduct including cases relating to social and environmental risk crystallization associated with projects the bank has financed.

2. A disclosure is deemed to have been made through the KPMG Ethics Line facilities or to the CBN and/or any other Government agency provided that such disclosure is true and reasonable.

3. The Bank shall not subject a Whistle-blower to any detriment whatsoever on the grounds that s/he has made a disclosure in accordance with the provisions of this policy.

4. An employee who has suffered any detriment by reason of disclosure made pursuant to the provision of these guidelines shall be entitled to compensation and/or reinstatement provided that in the case of compensation, the employee's entitlement shall be computed as if he had attained the maximum age of retirement or had completed the maximum period of service, in accordance with his condition of service. For stakeholders, the whistle- blower shall be adequately compensated.

5. Whistle-blowers are encouraged but not required or obliged to disclose their identities to FCMB and/or KPMG when reporting incidents through KPMG Ethics Line facilities. In the event of the whistle-blower willfully disclosing his/her identity, it shall remain undisclosed to FCMB until the complainant provides written consent to KPMG. These measures are necessary in order to

maintain the confidentiality and anonymity of the whistle-blowers.

6. All reports received via the KPMG Ethics Line facilities will be transcribed unto call sheet memoranda and transmitted to designated officers within FCMB for further action.

7. Reports of any allegation relating to fraud, theft of company asset and human resource related matters (e.g. sexual harassment) shall be submitted to the Managing Director, Company Secretary/ Group Legal Counsel, Chief Compliance Officer and Chief Inspector/ Head of Internal Audit

8. Whistle blowing matters relating to breach of the Code of Corporate Governance for Banks in Nigeria and other types of unethical conducts shall be reported to the Chairman of the Board, Managing Director, Group Head, Enterprise Management and Chief Compliance Officer.

9. Where the matter relates to a report against a Director (excluding the Managing Director), irrespective of the type of incident, it shall be reported to the Chairman of the Board, Managing Director and Company Secretary/ Group Legal Counsel.

10. If the allegation is against the Managing Director, irrespective of the type of incident, it shall be conveyed to the Chairman of the Board and the Company Secretary/ Group Legal Counsel.

11. In general, every call sheet memorandum is copied to the Chief Compliance Officer and Head of Internal Audit /Chief Inspector for report rendition purposes.

12. The Head of Internal Audit shall provide the Chairman of the Board Audit and Risk Management Committee with a summary of cases reported and the result of the investigation. Provided the allegation has been made lawfully without malice, the employment position of the person making it will not be adversely affected. It is the responsibility of Executive Management to ensure that Whistle blowers are protected from victimisation.

13. The person or persons against whom the allegation is made shall be informed of the allegation and the evidence supporting it and must be allowed to comment in writing before investigation is concluded.

14. If on preliminary investigation, the allegation is judged to be wholly without substance or merit, the allegation may be dismissed and the person making the allegation will be so informed through the Ethics Line service.

15. Where an allegation is found to be valid, Executive management shall constitute Disciplinary Committee to review the matter and apply appropriate sanctions on the erring staff.

16. As may be required by extant regulations and guidelines, whistleblowing incidences shall be reported to Law Enforcement Agencies or appropriate Regulatory Bodies for any further action or prosecution.

17. All allegations, including those dismissed after preliminary examination, and the results of their investigation must be reported to the Board Audit and Risk Management Committee.

18. If someone who has made a whistle blowing allegation remains dissatisfied with the outcome of the investigation, the issue should be escalated to the Chairman of the Board of Directors who shall constitute a special panel to review the allegation.

19. Where a Whistle-blower believes that s/he has been subjected to any detriment in contravention of the above, s/he may present a complaint to the Central Bank of Nigeria.

6.0 Audit of AML/CFT

The Group Internal Audit (GIA) shall be responsible for review of the bank processes and transactions to ensure that they comply with CBN, NFIU/EFCC requirements on Anti-Money Laundering and Countering Financing of Terrorism

7.0 Review of Policy

This Policy is subject to further review every 12 months or less depending on changes in the Law.

This document was last reviewed in January 2015.

Appendix 1 : FATF Recommendations 2012 (*www.fatf-gafi.org*)

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 - SRII Terrorist financing offence
6 - SRIII 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 - Mutual legal assistance
38 - Mutual legal assistance: freezing and confiscation
39 - Extradition
40 - Other forms of international cooperation

Appendix 2: Suspicious Transactions Form

SUSPICIOUS TRANSACTION REPORT

Date: **No of Pages:** (including this page)

To: **Telephone No:**
Mobile Phone No:
Facsimile No:

REPORTING OFFICER

Name Tel Fax
Position Branch/Dept

CUSTOMER/CLIENT DETAILS AND BACKGROUND

Customer Name ID/Passport No.
Nationality Address
Telephone No Occupation
Employer's Name Employer's Address/Tel No

Existing Accounts (Nos)	Type of Accounts	Credit Balance	Date	Date Account Opened

BRIEF DESCRIPTION OF CUSTOMER'S RELATIONSHIP WITH BANK (PRESENT AND PAST)

NATURE OF TRANSACTION

- ☐ Reactivated dormant account
- ☐ Large/unusual cash deposits/withdrawals
- ☐ Activity inconsistent with customer
- ☐ Regular/unusual off-shore activity
- ☐ Large/unusual inwards/outwards remittances
- ☐ Other

DETAILS OF TRANSACTIONS AROUSING SUSPICION

Amount (Dr/Cr)	Amount No(S)	Details of Remitting Bank(Incoming funds)/Destination (outgoing funds)

CONFIDENTIAL
Facsimile

SUSPICIOUS TRANSACTION REPORT

REASONS FOR SUSPICION
REASONS GIVEN BY CUSTOMER FOR TRANSACTIONS/ON MAKING FURTHER ENQUIRIES
OTHER RELEVANT INFORMATION
IMPORTANT: Please attach copies of (1) Account opening form (2) Recent account history (3) Suspicious transaction documents AND (4) Customer identification documents.
NOTE: *You should not inform customer/client of your suspicion and report.*

REPORTER'S SIGNATURE	
MANAGER'S/HEAD OF DEPARTMENT'S SIGNATURE	

Potential Transactions Perceived or Identified as Suspicious

- Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.
- Transactions involving shell companies.
- Transactions with correspondents that have been identified as higher risk.
- Large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered.
- Transaction with correspondents that have been identified as higher risk.
- Transaction activity involving amounts that are just below the stipulated reporting threshold or enquires that appear to test an institution's own internal monitoring threshold or controls.

Money laundering using cash transactions

- Significant increases in cash deposits of an individual or corporate entity without apparent cause. Particularly if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer.
- Unusually large deposits made by individual or a corporate entity whose normal business is transacted by cheques and other non-cash instruments.
- Frequent exchange of cash into other currencies.
- Customers who deposits cash through many deposits slips such that the amount of each deposit is relatively small, that overall total is quite significant.
- Customer whose deposits contain forged currency notes or instruments
- Customer whose deposit cash to cover applications for bank drafts.
- Customer who regularly deposit cash to cover applications for bank drafts
- Customers making large and frequent cash deposits but with cheques always drawn in favour of persons not unusually associated with their type of business.
- Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.
- Branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors.
- Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

Money laundering using deposit accounts

- The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business;
- Minimal, vague or fictitious information provided by a customer that the deposit money bank is not in position to verify.

- Lack of reference or identification in support of an account opening application by a person who is unable or unwilling to provide the required documentation.
- A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening a bank account.

- Customer maintaining multiple accounts at a bank or different banks for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.
- Customers depositing or withdrawing large amounts of cash with no apparent business source or in a manner inconsistent with the nature and volume of the business.
- Accounts with large volumes of activity but low balances or frequently overdrawn positions.
- Customers making large deposits and maintaining large balances with no apparent rationale.
- Customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances, typically, these transactions are not consistent with the customer's legitimate business needs.
- Sudden and unexpected increase in account activity or balance arising from deposit of cash non-cash items. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly.
- Accounts that are used as temporary repositories for funds that are subsequently transferred outside the bank to foreign accounts. Such accounts often have low activity.
- Customer requests for early redemption of certificate of deposit or other investment soon after the purchase, with the customer being willing to suffer loss of interest or incur penalties for premature realization of investment.
- Customer requests for disbursement of the proceeds of certificates of deposits or other investments by multiple cheques each below the stipulated reporting threshold.
- Retails business which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs.
- Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks.
- Substantial cash deposits by professional customers into client, trust or escrow accounts.
- Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation

process from such accounts prior to a request for onward transmission of the funds.

- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- Greater use of safe deposit facilities by individual, particularly the use of sealed packets which are deposited and soon withdrawn.

- Substantial increase in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other clients company and trust accounts.

- Large number of individuals making payments into the same account without an adequate explanation.
- High velocity of funds that reflects the large volume of money flowing through an account.
- An account opened in the name of name of a money changer that receives deposits.
- An account operated in the name of an off-shore company with structured movement of funds

Trade Based Money Laundering

- Over and under-invoicing of goods.
- Multiple involving of goods and services
- Over and under-invoicing of goods and services
- Falsely described goods and services and "phantom" shipments where by the exporter does not ship any goods at all after payments and been made, particularly under confirmed letters of credit.
- Transfer pricing
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Items shipped are inconsistent with the nature of the customer's normal business and the transaction lacks an obvious economics rationale.
- Customer requests payment of proceeds to an unrelated third party.
- Significantly amended letters of credits without reasonable justification or changes to the beneficiary or location of payment.

Lending Activities

- Customers who repay problem loans unexpectedly.
- A customer who is reluctant or refuses to state the purpose of a loan or the source of repayment or repayment or provides a questionable purpose and/or source of repayment.
- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loans secured by deposits or other readily marketable assets, such as securities ,
- Particularly when owned by apparently unrelated third parties.
- Loans are made for, or are paid on behalf of a third party with no reasonable explanation.
- Loans lack a legitimate business purpose, provide the bank with significant fees for assuming minimal risk, or tend to obscure the movement of funds (e.g. loans made to a borrower and immediately sold to an entity-related to borrower).

Terrorist Financing Red Flags

- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seems to corresponds to the stated occupation (e.g. student, unemployed, or self-employed).
- Financial transaction by a nonprofit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
- Large number of incoming or outgoing funds transfers takes place through a business account and there appears to be logical business or other economic purpose for the transfers, particularly when this activity involved designed high-risk locations.
- The stated occupation of the customer is inconsistent with the type and level of account activity.
- Funds transfer does not include information on the originator or the person on whose behalf the transaction is conducted the inclusion of which should ordinarily be expected.

- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
- Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

Other Unusual or Suspicious Activities

- Employee exhibits a lavish lifestyles that cannot be justified by his/her salary
- Employee fails to comply with approved operating guidelines particularly in private banking
- Employee fails to comply with approved operating guidelines particularly in private banking
- Employee is reluctant to make vacation.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside work in the institution's service area despite the availability of such services at an institution closer to them.

- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high value assets awaiting conversion to currency, for placement in the banking system.
- Customer uses a personal account for business purpose.
- Official Embassy business is conducted through personal accounts
- Embassy accounts are funded through substantial currency transactions.
- Embassy accounts directly funds personal expenses of foreign nationals.

Bribery and Corruption indicators

The following is a list of possible scenarios that may arise during the course of employee or director working for the bank and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only to help you in your compliance with this policy.

i. If an employee or director encounters any of these scenarios in the course of his/her work, he/she must report them promptly to the Chief Compliance Officer or use the Whistleblower platform:

ii. He/she becomes aware that a third party engages in, or has been accused of engaging in, improper business practices;

iii. He/she learns that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a "special relationship" with foreign government officials;

iv. a third party insists on receiving a commission or fee payment before committing to sign up to a contract with us, or carrying out a government function or process for the Bank;

v. a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

vi. a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

vii. a third party requests an unexpected additional fee or commission to "facilitate" a service;

viii. a third party demands entertainment or gifts before commencing or continuing contractual negotiations or provision of services;

ix. a third party requests that a payment is made to "overlook" potential legal violations;

x. an invoice from a third party that appears to be non-standard or customized;

xi. a third party refuses to put contractual terms agreed in writing;

xii. he/she notices that the Bank has been invoiced for a commission or fee payment that appears large given the service stated to have been provided;

xiii. he/she is offered an unusually generous gift or offered lavish hospitality by a third party;

xiv. He/she is asked to give hospitality to persons who are not associated with the organization (for example family members)

xv. or is offered hospitality which extends to persons beyond our business (for example family members)

Appendix 3 : AML/CFT Returns [CBN AML/CFT Regulations 2009 (As amended)]

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
B1396 Section 1.1.1	Proceeds of Crimes	This section requires FIs to identify and report to the CBN and NFIU the proceeds of crimes derived from: terrorism, including terrorist financing; corruption and bribery; fraud; grievous bodily injury; piracy; extortion etc	NFIU / CBN	As may occur
B1400 Section 1.6.4	Level of Risk of Customers, Transactions or Products	FIs are required to adopt CDD measures on a risk sensitive basis and to have regard to the risk involved in the type of customer, product, transaction or the location of the customer. Where there is doubt, they are directed to clarify with the CBN	CBN	As may occur
B1402 Section 1.10.3	Politically Exposed Persons	Senior management approval must be obtained by financial institutions before they establish any business relationship with a PEP and must render monthly returns	NFIU / CBN	Monthly
B1404 Section 1.14.1	Record maintenance on transactions	This section requires FIs to maintain all necessary record, in respect of domestic or international transactions for a minimum of 5years following completion of the transaction. Such record will be kept longer if requested by the CBN and NFIU in specific cases.	NFIU / CBN	As may occur
B1405 Section 1.16.2.5	Complex, Unusual (Large) and	Fis are required to examine as far as possible the background and purpose of	NFIU/ CBN	As may occur

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
	suspicious transaction	suspicious transactions and make available their findings to the CBN and NFIU and other competent authorities and auditors		
1.18.3.	Currency Transaction Report	Report all transactions in any currency above a threshold of N5m and N10m for individual and corporate bodies respectively	NFIU	Weekly
		Reports on transfer to or from a foreign country of funds or securities by a person or body corporate including Money Service Business of a sum exceeding US$10,000 or its equivalent	CBN /SEC/ NFIU	Weekly
B1409 Section 1.18.5.3	Foreign branches and subsidiaries	FIs are required to inform the CBN in writing when their foreign branches or subsidiaries are unable to observe the appropriate AML/CFT measure because they are prohibited by the host country's laws, regulations or other measures.	CBN	as may occur
B1410 Section 1.18.6.1.2	Employee Education and Training Programme	FI's are required to design a comprehensive training programme for employees and to render quarterly returns on their level of compliance to the CBN and NFIU	CBN & NFIU	Quarterly
B1410 Section 1.18.6.1.3		FIs are required to submit their annual AML/CFT employee training program	CBN & NFIU	Annually (31st December)

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
		to CBN and NFIU not later than 31st December every financial year		
B1411 Section 1.18.7.1.	Monitoring of Employee Conduct	FIs are required to monitor employee as well as customers' account for potential sign of money laundering. This should be done under the supervision CCO	CBN & NFIU	Bi-annually (June and December)
	Additional Areas of Potential Money Laundering Risks	FIs are required to review, identify and record other areas of potential money laundering risks not covered by the AML/CFT regulations 2009 and report to the CBN/NFIU	CBN & NFIU	Quarterly
B1411 Section 1.20.	Additional procedures and mitigants (AML/CFT)	FIs are required to review the AML/CFT framework and identify new areas of potential money laundering risks. They are required to design additional procedures and mitigants as contingency plan in their AML/CFT operational manual and render returns to the CBN & NFIU as at 31st December of every year	CBN & NFIU	As at 31st December of every financial year
B1411 Section 1.21.	Testing the adequacy of the AML/CFT compliance	Report on independent testing of AML/CFT Compliance program	CBN & NFIU	As at 31st December of every financial year

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
B1412 Section 1.22.	Formulation of AML/CFT Regulations	Approved copies of AML/CFT Regulations formulated by management should be forwarded to the CBN & NFIU	CBN & NFIU	Within six months of release of the CBN AML/CFT Regulation
B1412 Section 1.25.2	Money or Value transfer (MVT) services	MVTs operators are to maintain a current list of its agents and render quarterly returns to the CBN	CBN	Quarterly
B1413 Section 1.25.3	New (MVT) relationships	before establishing new correspondent relationships, MVT operators are required to obtain approval from the CBN and also to document/maintain a checklist of the respective AML/CFT responsibilities	CBN	as may occur
B1427 Section 2.6.1.5.9	Financially Excluded Persons	Report on customers treated as being financially excluded	CBN & NFIU	Quarterly
B 1448 Section 2.8.8.3	Linked Transactions	where returns rendered to the NFIU after suspicion of money laundering arising from linked transaction, FI is required to maintain copies of supporting cheques, forms and other relevant record until the records are of no further interest.	NFIU & CBN	as may occur
B 1401 Section 1.8.2	Failure to complete CDD	Any FI that has already commenced business relationship and later comes to realize lapses in the completion of CDD is	NFIU	as may occur

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
		required to terminate such relationship and render STR to NFIU		
B 1403 Section 1.10.5	PEP	Where a FI is in a relationship with a PEP and notices any abnormal transaction, it is required to flag the account and report same immediately	NFIU	as may occur
B1405 Section 1.16.2.5	Suspicious Transactions	A financial institution that suspects that funds are the proceeds of a criminal activity or is related to terrorist financing is required to promptly report to NFIU	NFIU	When identified
B1414 Section 1.26.9	Wire Transfers	FIs are required to report any wire transfer that lacks complete originator information	NFIU	as may occur
B1419 Section 2.4.8.5	Time Frame for Identification Requirements	where an applicant refuses to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation, the FI is required to make a STR based on the information in its possession before the funds involved are returned to the potential client or where they came from	NFIU	as may occur

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
B1419 Section 2.4.9	Cancellation and Cooling-Off Rights	Where an abnormal exercise from cancellation and cooling-off rights by an investor becomes apparent, FI are required to treat the matter as suspicious and report same	NFIU	as may occur
B1430 Section 2.6.1.8.5	Non face to face Identification	where a FI 's business is operated electronically, computerized monitoring systems/solutions should be put in place to recognise suspicious transactions	NFIU	Quarterly
B 1432 Section 2.6.2.2.6	Offshore Trusts	Any application to open an account or undertake a transaction on behalf of another without the applicant identifying their Trust or Nominee capacity should be regarded as suspicious and should lead to further enquiries and rendition of report to the NFIU.	NFIU	as may occur
B1434 Section 2.6.2.6.4	Executorship Accounts	Where suspicions are aroused concerning the nature or origin of assets comprising an estate that is being wound up, the reports of the suspicions are to be rendered.	NFIU	as may occur
B1435 Section 2.6.2.7.4	"Client Accounts" opened by professional intermediaries	FIs are required to make reasonable enquiries about transactions passing through this type of account and any cause for concern should be	NFIU	as may occur

Section	Type of Report	Basis/Purpose	Recipient of Report	Frequency
		reported		
B1435 Section 2.8.6.3	Linked Transactions	Where transactions are believed to be linked and money laundering is suspected, the FI should investigate and render returns on same together with documentary evidence	NFIU	as may occur