FCMB Enterprise Risk Management

(Compliance Risk Management)

Know Your Customer

Anti-Money Laundering

&

Countering Financing of Terrorism and

Proliferation Manual

INTRODUCTION.

POLICY STATEMENT

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

i. 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;

ii. 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;

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

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

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

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

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

viii. 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, procedures and internal controls to correct/enhance and/or adapt to regulatory changes / deficiencies.

vi. has designated an Executive Director as the Bank's Executive Compliance Officer in line with CBN's directive and has also designated a senior management staff as its Chief Compliance Officer to oversee its AML/CFT program.

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):

i. Assume overall accountability for Compliance performance;

ii. Ensure that appropriate AML/CFT Compliance Risk Management framework is established and is in operation;

iii. Approve the AML/CFT Compliance Risk Management program and policies;

iv. Provide guidelines regarding the management of AML/CFT Compliance risks;

v. Appoint and designate an Executive Compliance Officer and Chief Compliance Officer (in line with CBN guidelines) to coordinate and monitor AML/CFT Compliance by the Bank.

EXECUTIVE COMPLIANCE OFFICER

i. Report to the Board on all compliance related matters.

ii. Ensure there is no breach of extant regulations in the Bank.

iii. Answer to regulators on compliance failures within 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.

ZONAL COMPLIANCE OFFICERS

i. Monitor money laundering activities in the branch.

ii. Ensure adherence to KYC and KYCB principles.

iii. Coordinate submission of suspicious transactions report to 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.

SCOPE

This manual is applicable to FCMB and its subsidiaries.

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).*
- *Nigerian 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 (as amended).*
- *Terrorism (Prevention) Act, 2011 (as amended).*
- *CBN AML/CFT Regulations, 2013.*
- *SEC Rules and Regulations, 2013.*
- *SEC AML/CFT Regulations, 2013.*
- *Terrorism Prevention (Freezing of International Terrorists Funds and Other Related Measures) Regulations, 2011.*
- *Cybercrimes (Prohibition, Prevention, etc) Act, 2015.*
- *Special Control Unit against Money Laundering AML/CFT Regulations for Designated Non-Financial Businesses and Professions in Nigeria, 2013.*
- *Advance Fee Fraud and other Fraud Related Offences 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 (Offences) 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.*
- *FATF 40 Recommendations.*

MONEY LAUNDERING/TERRORISM FINANCING RISK ASSESSMENT PROCESS

FCMB adopts risk-based approach that are commensurate with the specific risks of money laundering and terrorist financing. Higher money laundering risks demand stronger controls. However, all categories of risk — whether low, medium or high — must be mitigated by the application of applicable controls as provided in this Manual, such as verification of customer identification, Know Your Customer (KYC) policies, and so on.

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

IDENTIFYING SPECIFIC RISK CATEGORIES

Attempts to conduct illegal activities through the Bank may come from many different sources throughout the system. Certain products, services, customers, and geographic locations in which the Bank operates may be particularly vulnerable or may have been historically used by criminals for *ML/TF* activities.

The following specific products, services, customers, entities and geographic locations are identified as having *ML/TF* risk to the Bank.

PRODUCTS AND SERVICES

In evaluating the ML/TF risk with respect to products and services, the following become relevant: 'Does a particular product or service, new or current:

- Have an especially high transactions or investment value or involves international transaction?
- Allow payments to third parties?
- Have unusual complexity?
- Require government verification of customer eligibility?
- Allow the customer to be treated anonymously?

These categories can include the following:

- Electronic funds payment services: electronic cash such as stored value cards, domestic and international funds transfers and third party payment processor; remittance activity; automated clearing house (ACH) transactions, automated teller machines (ATMs); and Mobile Phones Financial Services.
- Electronic Banking.
- Foreign exchange and funds transfers.
- Domestic and international private banking.
- Trust and asset management services.
- Monetary instruments.
- Foreign correspondent accounts, such as payable through accounts (PTA); foreign currency denominated accounts.
- Trade finance or letters of credit.
- Special use, or concentration (suspense) accounts.
- Lending activities, particularly loans secured by cash collateral and marketable securities.

INDIVIDUAL CUSTOMERS AND ENTITIES

Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, or the nature of anticipated transaction activity into their account. An assessment of the risk level of various types of clients such as individuals, listed companies, private companies, joint ventures, partnerships, financial institutions and others who want to establish a relationship with the Bank should be conducted to determine and define the level of risk for each individual customer.

For instance, in the case of individual customer, those who have a history of involvement in criminal activities should receive the highest ratings.

Political figures or those in political organizations should score toward the top of the scale, higher than officials of multinational corporations. In the case of corporate customers, for example, when the Bank is approached by a private company, the risk is higher than it would be with a larger corporation because the due diligence that can be conducted is more limited.

Access to a considerable amount of publicly available information could result in a lower risk than with a small company that is not listed and for which public information is not available.

The following list, though not exhaustive, indicates the customers and entities that are likely to pose a higher level of risk to the Bank:

- Foreign financial institutions, including banks and foreign money services providers such as bureau de change, currency exchanges, and money transmitters.
- Foreign corporations and domestic business entities, particularly offshore corporations such as domestic 'shell' companies, private investment companies (PICs) and international business corporations (IBCs) located in high-risk geographic locations and tax havens.
- *Politically Exposed Persons (PEPs)* as defined in this Manual.
- Non-resident aliens and accounts held by foreign individuals.

- Cash intensive businesses, including, for example, restaurants and fast food businesses, liquor stores, large merchandise distributors, privately owned vending machines operators, car dealers, etc.
- Foreign and domestic *Non-Governmental Organizations (NGOs)* and charities.
- Professional service providers such as attorneys, accountants, or real estate brokers.
- Casinos.
- Travel agencies.
- Leather goods stores.
- Jewel, gem and precious metals dealers.
- Brokers/dealers in securities.
- Import/ export companies.
- Money Transfer Agent (MTA).

GEOGRAPHIC LOCATIONS

In assessing customers' jurisdiction risk, customer service officers and relationship managers must be aware of the vulnerability of jurisdiction where customers reside. Some might be located in countries with higher risk of money laundering.

When looking specifically at money laundering risk with respect to customers' location of business or residents, the following should be considered amongst other factors:

- Terrorism and sanctions lists published by governments and international organizations that include legal prohibitions and designations published by the United Kingdom's Financial Services Authority, U.S. Office of Foreign Assets Control, the U.S. Financial Crimes Enforcement Network, the European Union, World Bank, the United Nations Security Council Committee, The Central Bank of Nigeria (CBN) sanction list, etc.

- Whether the country is or has been on the *Financial Action Task Force's (FATF)* list, whether it is a member of the *FATF*, whether it operates *Anti-Money Laundering (AML)* controls equivalent to international best practices or has deficient standards.

- The overall reputation of the countries in question. In some, cash may be a standard medium of exchange. Others may have politically unstable regimes and high levels of public or private sector corruption. Still, others may be widely known to have internal drug production or to be in drug transit regions.

  It should however be noted that geographic risk alone does not necessarily mean a customer's or transaction's risk level is high or low. Cases should be evaluated individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations. **When in doubt, contact the Chief Compliance Officer.**

ANALYSIS OF SPECIFIC RISK CATEGORIES

The next stage of the risk assessment process is the analysis of data obtained during the risk identification stage so as to accurately assess ML/TF risk more accurately. Evaluation and analysis of data pertaining to the Bank's activities should be considered in relation both to FCMB's Customer Identification Program (CIP) and to Customer Due Diligence (CDD) information.

For the purpose of this Manual, analysis of customers' data and account profile should specifically take into account, the following:

- Purpose of the account.
- Actual or anticipated activity in the account (i.e. turnover).
- Nature of the customer's business.
- Customer's location/ Source of funds.
- Type of products or services a customer uses.
- Structure of business.

Others include:

- Method of opening account.
- Identification used.

- Nationality.
- Customer address information.
- Residency status.
- Beneficiary owner.

CUSTOMER RISK ASSESSMENT MATRIX

In order to improve the monitoring and control process of our client base, ***FCMB*** shall categorise its customers by their perceived risk rating – either: HIGH, MEDIUM or LOW risk using the designated risk assessment matrix.

UPDATING THE RISK ASSESSMENT

HIGH: Half Yearly;

MEDIUM: Yearly;

LOW: Every two Years.

Should circumstances however dictate a review of an account in any of the categories, this can be conducted at any time more frequently than as set out above.

The Bank will take a risk based approach to the rating of each customer and this will in turn affect the level of KYC information collected. This would include not only the level of documentation held but also the number and content of additional checks performed over the Internet or by obtaining media information. These factors may alter the bank's perceived rating and the risk level altered accordingly.

The reviews will be carried out by the Customer Service Manager in conjunction with the zonal Compliance Officer.

The review will consist of taking into account the criteria as set out above and will include an examination of the statement of the account showing entries since the last review. The Zonal Compliance Officer may decide to request a full evaluation to be conducted by an Account Officer if it is felt the circumstances warrant it.

Accounts will not be allowed to move from one category to a lower category without the written approval of the Branch Compliance Officer after advice and clearance by the Bank's Chief Compliance Officer. Accounts may be moved to a higher category at the written request of any one member of senior management as set out above or on the instruction of the CCO.

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:

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

- Prohibition of opening numbered or anonymous accounts or accounts in fictitious or pseudo names.

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

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

- 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.

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

- Profiling of customers and risk rating such that transactions by our customers are fairly predictable.

- 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.

- Customer information update whenever the need arises.

- 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. Charitable organisations, Non-Governmental Organisations, Money Services Businesses, Bitcoin exchangers, Casinos, dealers in precious stones, and any other businesses, activities or professions as may be prescribed by regulatory, supervisory and competent authorities.

CUSTOMER DUE DILIGENCE AND ACCOUNT OPENING PROCEDURES

This section sets out the *Customer Due Diligence (CDD)* procedures and highlights information and documentation requirements for account opening with respect to various categories of customers/accounts type.

Staff are expected to conform with the Bank's policy on account opening and ensure appropriate documentation when establishing account relationship with customers.

PRIVATE INDIVIDUALS RESIDENT IN NIGERIA INDIVIDIAL (ORDINARY ACCOUNTS)

- Duly completed account opening form.
- Valid means of identification (ID) of signatory or person introducing another customer.
- Residence permit (for expatriates).
- Passport photographs.
- Birth certificate of a minor and 2 passport photographs of the trustee (applicable to savings account for children).
- Tax Identification Number (applicable to residents of Abuja).
- Proof of residence.

- Duly registered Power of Attorney, where an individual appoints another person to be a signatory to his personal account.
- Bank Verification Number.

INDIVIDIAL (TIER 1 ACCOUNTS)
These accounts can only permit single deposit amount of N50,000 and a maximum cumulative balance of N300,000.

- Duly completed account opening form.
- Bank verification Number
- One passport photograph.

PRIVATE INDIVIDUAL NOT RESIDENT IN NIGERIA

For these category of customers who cannot make face-to- face contact, any of the following would suffice as evidence of the name of the customer:

- Notarized International passports;
- Notarized National identity cards; or
- Notarized International driver's license.

Reference numbers, date and country of issue should be obtained and the information recorded in the customer's file as part of the identification evidence.

Separate evidence is required to be obtained with respect to the applicant's permanent residential address from the best available evidence, preferably from an official source. The address must be verifiable by way of a recorded description or other means. "P.O. Box number" alone should not be accepted as evidence of address.

The above should be verified through a reputable credit or financial institution in the applicant's home country or country of residence. However, particular care must be taken when relying on

identification evidence provided from other countries, such evidence must be duly confirmed.

SALARY SAVINGS ACCOUNT

- Duly completed account opening form.
- Letter of introduction from the company/appropriate authority (for individual current and savings salary account holders who do not have acceptable means of identification.
- Means of ID (secondary IDs approved by the bank).
- Bank Verification Number.

CORPORATE

- Duly completed account opening form.
- CTC of Form CAC 2/ CAC1.1.
- CTC of Form CAC7/CAC 1.1.
- Certificate of incorporation.
- CTC of Memorandum and Articles of Association.
- Tax Identification Number (TIN).
- Valid means of ID of each signatory and Directors.
- Residence Permit (foreigners).
- Passport photograph of each signatory.
- Nigeria Investment Promotion Commission (NIPC) certificate (for corporate entities incorporated in Nigeria with foreign ownership).
- Executed and sealed Board resolution.
- Current proof of residence/address.
- Bank Verification Number.
- ***** *CBN licence for finance companies and international money transfer operators as well as SCUML certificate for designated non-financial businesses and professions.*

ENTERPRISE ACCOUNT

- Duly completed account opening form.
- Certificate of registration of business name.
- Form of application of registration of business name.
- Tax Identification Number (TIN).
- Passport photographs of each signatory.
- Valid means of ID of each signatory.

- Current proof of residence/address.
- Residence permit (foreigners).
- Bank Verification Number.
- SCUML certificate as applicable.

PARTNERSHIP ACCOUNT

- Duly completed account opening form.
- Partnership resolution.
- Certificate of registration of business name.
- Form of application of registration of business name.
- Tax Identification Number (TIN).
- Letter of appointment as bankers.
- Residence Permit (foreigners).
- Valid means of ID of each signatory.
- Proof of address.
- Partnership deed or agreement.
- Passport photographs of each signatory.
- Bank Verification Number.

MICROFINANCE BANK

- Duly completed account opening package.
- All the documents for corporate accounts plus CBN operating licence/Approval-In-Principle.
- Bank Verification Number.

CLUBS /SOCIETIES/ASSOCIATION/UNINCORPORATED SOCIETIES

- Duly completed account opening package.
- Constitution, rules and regulations.
- CTC of certificate of registration.
- Passport photograph for each signatory.
- Society/Club/Association's resolution to open account.
- Form of identification for each signatory.
- Tax Identification Number (TIN).
- Residence permit (foreigners).
- Utility receipt.
- Bank Verification Number.

MINISTRIES, PARASTATALS AND OTHER GOVERNMENT BODIES

- Duly completed account opening form.
- Copy of gazette or Act establishing the parastatal (if applicable).
- Board resolution authorizing the opening of the account (if incorporated or has a duly constituted Board).
- Copy of certificate of incorporation (if an incorporated parastatal).
- Copy of MEMART (if incorporated or has a duly constituted Board).
- Valid means of ID of each signatory.
- Authorisation of Accountant General of the Federation/State or relevant Local Government Council.

BUREAU DE CHANGE (BDC)

- Duly completed account opening form.
- All documents for corporate accounts plus the following:
    - CBN licence.
    - Bank Verification Number.

EXECUTORS/ADMINISTRATORS

- Duly completed account opening form.
- Passport photograph.
- Letter of Administration or Probate.
- Valid ID for each signatory.
- Current proof of residence/address for each signatory.
- Banker's confirmation and letter of indemnity
- Bank Verification Number.

NGOs AND MULTILATERAL AGENCIES

- Duly completed account opening form.
- Passport photograph for each signatory.
- Valid Id for each signatory.
- References (two) for each signatory.
- Valid ID for each signatory.
- Registration certificate (If applicable).
- Tax Identification Number (TIN).
- Passport photographs for each signatory.
- Proof of address.
- Copy of Rules/Constitution.
- Bank Verification Number.
- SCUML certificate where applicable.

TRUSTEES

- Duly completed account opening form.
- Passport photograph for each signatory.
- Valid Id for each signatory.
- References (two) for each signatory.
- Registration certificate (If applicable).
- Proof of residence/ address.
- Deed of appointment as trustees.
- Executed and sealed Board resolution.
- Bank Verification Number.

RELIGIOUS BODIES/ORGANISATIONS

- Duly completed account opening form.
- Certified True Copy of registration certificate or document establishing the organization.
- Constitution/document guiding their operations.
- Letter of introduction of the signatories to the account.
- Valid means of identification of the signatory(ies).
- Two (2) references.

EMBASSIES, CONSULATES & HIGH COMMISSIONS OF FOREIGN COUNTRIIES

- Duly completed account opening form.
- Letter of credence of the ambassador from the home country.
- Copy of current international passport of signatories.
- Letter of reference from the Ministry of External Affairs.
- Official document from home country establishing the authority of the embassy to open the account and how the account is to be operated.

PARTNERSHIP ACCOUNTS

- Duly completed account opening form.
- Partnership resolution.
- Certificate of registration of business name.
- Form of Application for registration of business name.
- Tax Identification Number (TIN).
- Letter of appointment as bankers.
- Residence permit (foreigners).
- Valid ID of each of the signatories.
- Proof of address.
- Partnership deed.

STAFF ACCOUNTS

- Two recent passport photographs.
- Valid ID.
- Bank Verification Number.

CUSTOMER DUE DILIGENCE INFORMATION VERIFICATION

The above listed customer due diligence information should be verified by at least one of the following methods:

- For established corporate entities - reviewing a copy of the latest report and accounts (audited, if available);

- Conducting an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;

- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated;

- Utilizing an independent information verification process, such as accessing public and private databases;

- Obtaining satisfactory prior bank references;

- Physical visitation to the corporate entity place of business; and
- Contacting the corporate entity by telephone, mail or e-mail.

POLITICALLY EXPOSED PERSONS

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

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

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.

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:

- **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.

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

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

- **Customer's corporate structure-** Type of corporate structure.

- **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.

- **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 Minimization

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 an 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.

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 or Regional 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 customer due diligence efforts do not end at account opening; ongoing account monitoring is expected. Activities on PEP accounts will be reviewed on 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 Department immediately.

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

The following guidance provide 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 transfer or wire transfer 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.

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 against Money Laundering (**SCUML**) of the 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.

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 with no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks.

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.

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 utilizes 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 N50,000.00.
- It allows maximum cumulative balance of N300,000.00 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 N100,000.00.
- It allows maximum cumulative balance of N500,000.00 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

RETENTION OF RECORDS

The Money Laundering and Terrorist Financing Regulations require financial institutions to maintain adequate records which are appropriate to the nature of the business and which can be used as evidence in any subsequent investigation.

WHY RETAIN RECORD?

Records must be retained, not only because regulations demand record retention but also to ensure that:

- Any legislation and KYC rules are met.
- Third parties i.e. external auditors, can assess the effectiveness of the Bank's observance of money laundering procedures.
- Any transactions effected by the Bank on behalf of any customer can be reconstructed.
- Any customer can be properly identified and located.
- All suspicious reports both internal and external can be identified.
- The Bank can satisfy any enquiries or court orders from appropriate authorities.

FOR HOW LONG MUST RECORDS BE RETAINED?

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 & 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.

REPORTING SUSPICIOUS TRANSACTIONS

IDENTIFICATION OF SUSPICIOUS TRANSACTIONS

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

Suspicious transactions shall include:

- Transaction involving a frequency which is unjustifiable or unreasonable, unusual or has unjustified complexity.
- Transaction which appears to have no economic justification or lawful objectives.
- Transactions which are structured to avoid reporting and record keeping requirements.
- Transfers of foreign currency transactions which are recalled twice from the account of a customer by a correspondent bank. (Note that a first recall could be due to error.)
- If the circumstances surrounding the first recall of a foreign currency transactions from the account of a customer by correspondence bank appeared suspicious.
- 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, (as amended) 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:

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

PROCEDURES FOR DISCLOSURE OF SUSPICIOUS TRANSACTIONS

- Any Officer of the Bank who suspects any transaction to be suspicious shall make an immediate report to the Chief Compliance Officer. The Bank has introduced a portal through which such reports are made electronically. The use of the manual STR form (as in Appendix 2) has been discontinued.
- 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.
- 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.
- 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.

The Bank is also in the process of deploying a more robust AML solution called Intellinx.

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, 2013, the Money Laundering (Prohibition) Act 2011, (as amended), 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).

AWARENESS AND TRAINING

The Money Laundering (Prohibition) Act, 2011 (as amended) 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 ML(P)A 2011 (as amended) and CBN AML/CFT Regulations, 2013 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 Department 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.

KNOW YOUR EMPLOYEE (KYE)/MONITORING OF EMPLOYEE CONDUCT

Knowing our employees is as important as knowing our customers. An insider can pose the same money laundering threat as a customer and a criminally co-opted bank employee might facilitate money laundering. The CBN AML/CFT Regulations, 2013 require:

- That financial institutions put in place adequate policies, procedures, and controls including appropriate compliance management arrangement and adequate screening procedures to ensure high standards when hiring employees; and

- That every Employee's accounts be monitored for potential signs of Money laundering and be subjected to the same **AML/CFT** Procedures as applicable to other customers' accounts. **This is required to be performed under the supervision of the CCO.**

KYE PROCEDURE

The following procedures should be followed and strictly adhered to, in order to ensure the Bank recruits not only the best brains but equally people with good character, high ethical standing, honesty and integrity.

- ***KYE*** information such as background information must be obtained prior to job interview, during job interview and just before offer of employment. Any serious gap observed must be documented and should form part of the basis for offer of employment.

- Medical report must be obtained on employees to confirm medical information submitted by prospective employees.

- All prospective hires must be checked against CBN list of blacklisted individual prior to offer of employment.

- After acceptance of offer, but before confirmation; background screening checks must be conducted to verify the identity of employees, viz:

- Certificates must be verified by awarding institutions. Note to ensure that such credentials are sent to awarding institutions for confirmation along with scanned passport photograph of recipients.

- Employee personal referees must be written and satisfactory report on character and suitability of employment obtained prior to confirmation of employee appointment.

- Former employer must be written and positive performance and character report obtained prior to confirmation.

- All information supplied by prospective employees must be verified during probation. Any change in such information, including marital status and additional qualifications obtained during the period must be verified against appropriate documents and issuing institutions.

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.

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.

10.2 WHISTLE-BLOWING PROCEDURES

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. 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.

ix. 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.

x. 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.

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

xii. 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 victimization.

xiii. 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.

xiv. 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.

xv. 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.

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

xvii. 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.

xviii. 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.

xix. 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.

AUDIT OF AML/CFT

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

REVIEW OF POLICY

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