09-462 37404

09-462 37409

May 5, 2010

FPR/DIR/CIR/AML/CFT/01/001

CIRCULAR TO BANKS AND OTHER FINANCIAL INSTITUTIONS: REVISED CBN ANTI-MONEY LAUNDERING/COUNTER TERRORISM FINANCING (AML/CFT) REGULATION, 2009

In October 2009, the CBN circulated the Anti-Money Laundering/Counter Terrorism Financing (AML/CFT) Compliance Manual as an Exposure Draft for comments from stakeholders via our circular **Ref: BSD/DIR/GEN/AML/03/009/1.**

The Manual has now been finalized and gazetted to give it full effect of law. It is now renamed as **"CBN AML/CFT REGULATION (2009)"** and can be accessed on the CBN website, www.cenbank.org.

Consequently, all banks and other financial institutions are, by this circular, required to comply with the requirements of the **CBN AML/CFT Regulation** attached to this circular.

The Exposure Draft released vide our circular **Ref: BSD/DIR/GEN/AML/03/009/1 of** October 2009 is hereby recalled.

I.T. NWAOHA
For: DIRECTOR FINANCIAL POLICY AND REGULATION

Extraordinary

Federal Republic of Nigeria
Official Gazette

No. 79 **Lagos - 28th December, 2009** **Vol. 96**

Government Notice No. 297

The following is published as Supplement to this *Gazette* :

Printed and Published by The Federal Government Printer, Abuja, Nigeria
FGP 130/122009/650 (OL 74)

Annual Subscription from 1st January, 2009 is Local : ₦15,000.00 Overseas : ₦21,500.00 [Surface Mail] ₦24,500.00 [Second Class Air Mail]. Present issue ₦500.00 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Abuja for amended Subscriptions.

ARRANGEMENT OF SECTIONS

APPENDIX C : MONEY LAUNDERING AND TERRORIST FINANCING "REDFLAGS"

INTRODUCTION

There have been increased stringent AML/CFT measures worldwide, particularly since the September 11, 2001 terrorist attaeks in the U.S. Nigeria, not being left out in the global efforts to fight the menace, has taken some AML/CFT measures in recognition of the dangers posed.

With the enactment of AML/CFT legislations in Nigeria, the country is giving increased attention to implementing these laws. Indeed, the benefits of having AML/CFT laws in place would not be realized unless there is diligent implementation of the enforcement measures by the CBN and compliance by financial institutions. It is against the above background that this *AML/CFT Regulation* was developed for the guidance of the financial institutions under the regulatory purview of the CBN.

The Regulation has been enriched by the enabling AML/CFT legislation enacted by Nigeria, particularly by the relevant FATF-Recommendations, the Guidelines of the Basle Committee on Banking Supervision and some international best practices documents.

To provide a further guide and to avoid ambiguity, the Guidance on KYC is also provided to assist financial institutions in their implementation of this Regulation.

Purpose and Overview of this Regulation

Financing of Terrorism (FT) is defined here to include both legitimate and illegitimate money characterized by concealment of the origin or intended criminal use of the funds.

Money Laundering (ML) is defined as the process whereby criminals attempt to conceal the origin and/or ownership of property and assets that are the fruits or proceeds of criminal activities. It is, thus, a derivative crime.

Money laundering and terrorist financing are global phenomena and there has been growing recognition in recent times, and indeed well-documented evidence, that both money laundering and terrorist financing pose major threats to international peace and security which could seriously undermine Nigeria's development and progress.

Consequently, concerted global efforts have been made to check these crimes. Financial institutions, in particular, have come under unprecedented regulatory pressure to enhance their monitoring and surveillance systems with a view to preventing, detecting and responding appropriately to money laundering and terrorist financing.

This Regulation covers the following key areas of AML/CFT policy; compliance officer designation and duties; the requirement to cooperate with the competent/supervisory authorities; customer due diligence; monitoring and responding to suspicious transactions; reporting requirements; record keeping; AML/CFT employee training program, among others.

Financial institutions are exposed to varying money laundering risks and serious financial and reputational damage if they fail to manage these risks adequately. Diligent

implementation of the provisions of this Regulation would not only minimize the risks faced by financial institutions of being used to launder the proceeds of crime but also provide protection against fraud and reputational and financial risks. In this connection, the affected institutions are urged to adopt a risk-based approach in the identification and management of their AML/CFT risks.

Nigerian financial institutions are also reminded that AML/CFT laws in all the jurisdictions in which they operate should not only designate money laundering and predicate offences but should prescribe sanctions for non-compliance with the relevant laws and regulations on customer due diligence, non-rendition of prescribed reports and not keeping of appropriate records. It is, therefore, in their best interest to entrench a culture of compliance which would be facilitated by this Regulation.

This Regulation is structured in two parts. *Part A* is made up of the new AML/CFT Directives while *Part B* provides guidance on KYC.

S. I. 40 of 2009

ANTI-MONEY LAUNDERING/ COMBATING FINANCING OF TERRORISM (AML/CFT) REGULATION FOR BANKS AND OTHER FINANCIAL INSTITUTIONS IN NIGERIA

The Governor of the Central Bank of Nigeria in exercise of the powers conferred on him under Section 57(1) of the Banks and Other Financial Institutions Act, 2004 and of all other powers enabling him in that behalf hereby issues Anti-Money Laundering/ Combating Financing of Terrorism (AML/CFT) Regulation for Banks and other Financial Institutions in Nigeria.

PART A—AML/CFT DIRECTIVES

AML/CFT INSTITUTIONAL POLICY FRAMEWORK

General Guidelines on Institutional Policy.

1. Every financial institution is required to adopt policies stating its commitment to comply with AML/CFT obligations under the law and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activity or terrorism.

Every financial institution is requested to formulate and implement internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations are always met.

AML/CFT Compliance Officer Designation and Duties.

Each financial institution is required to designate its AML/CFT Chief Compliance Officer with the ***relevant competence, authority and independence*** to implement the institution's AML/CFT compliance programme.

The duties of the AML/CFT Compliance Officer, among others, include :

(*i*) Developing an AML/CFT Compliance Programme ;

(*ii*) Receiving and vetting suspicious transaction reports from staff ;

(*iii*) Filing suspicious transaction reports with the NFIU ;

(*iv*) Rendering "nil" reports with the NFIU, where necessary to ensure compliance ;

(*v*) Ensuring that the financial institution's compliance programme is implemented ;

(*vi*) Co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements ; and

(*vii*) Serving both as a liaison officer with the CBN and NFIU and a point-of- contact for all employees on issues relating to money laundering and terrorist financing.

Cooperation with Competent Authorities.

Each financial institution is required to state that it will comply promptly with all the requests made in pursuant with the law and provide information to the CBN, NFIU and other relevant government agencies.

Each financial institution's procedures for responding to authorised requests for information on money laundering and terrorist financing are required to meet the following:

(*i*) ***searching immediately the institution's records*** to determine whether it maintains or has maintained any account for or has engaged in any transaction with each individual, entity, or organisation named in the request ;

(*ii*) ***reporting promptly to the requesting authority*** the outcome of the search ; and

(*iii*) ***protecting the security and confidentiality*** of such requests.

Scope of Offensive Proceeds.

1.1.1. Financial institutions are required to identify and report to the CBN & NFIU, the ***proceeds of crime derived from*** the following :

- Participation in an organized criminal group and racketeering ;
- Terrorism, including terrorist financing ;
- Trafficking in human beings and migrant smuggling ;
- Sexual exploitation, including sexual exploitation of children ;
- Illicit trafficking in narcotic drugs and psychotropic substances ;
- Illicit arms trafficking ;
- Illicit trafficking in stolen and other goods ;
- Corruption and bribery ;
- Fraud ,
- Counterfeiting currency ;
- Counterfeiting and piracy of products ;
- Environmental crime ;
- Murder, grievous bodily injury ;
- Kidnapping, illegal restraint and hostage-taking ;
- Robbery or theft ;
- Smuggling ;
- Extortion ;
- Forgery ;
- Piracy ; and
- Insider trading and market manipulation.

Measures to be taken against ML/ TF.

1.2. Financial institution secrecy and confidentiality laws shall not in ***any*** way, be used to inhibit the implementation of the requirements in this Regulation in view of ***sections 38 of EFCC Act, 2004; 12 of MLP Act, 2004 and 33 of the CBN Act, 2007.*** The Acts eited here have given the relevant

authorities the power required to access information to properly perform their functions in combating money laundering and financing of terrorism; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions, where this is required or necessary.

Customer Due Diligence (CDD).

1.3. Financial institutions are not permitted to keep anonymous accounts or accounts in fictitious names.

When CDD Is Required.

1.3.1. Financial institutions are required to undertake customer due diligence (CDD) measures when :

1.3.1.1. business relations are established ;

1.3.1.2. carrying out occasional transactions above the applicable ***designated threshold of $1,000 USD or its equivalent*** or as may be determined by the CBN from time to time, including where the transaction is carried out in a single operation or several operations that appear to be linked.

1.3.1.3. carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between financial institutions and when credit or debit cards are used as a payment system to effect money transfer. It does not, however, include the following types of payment :

- any transfer flowing from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanying such transfers does flow from the transactions such as ***withdrawals from a bank account through an ATM machine, cash advances from a credit card or payment for goods.***
- financial institution -to- financial institution transfers and settlements where both the originator-person and the beneficial-person are financial institutions acting on their own behalf.

1.3.1.4. there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in this Regulation ; or

1.3.1.5 ***There are doubts about the veracity or adequacy of previously obtained customer identification data.***

Financial institutions, however, are not required (after obtaining all the necessary documents and being so satisfied) to repeatedly perform identification and verification exercise every time a customer conducts a transaction.

B 1398

CDD Measures.

1.4.1 Financial institutions are required to identify their customers (whether ***permanent or occasional; natural or legal persons; or legal arrangements***) and verify the customers' identities using reliable, independently sourced documents, data or information. All financial institutions are required to ***carry out the full range of the CDD measures in this Regulation.*** **However, in** ***reasonable circumstances,*** financial institutions ***can apply the CDD measures on a risk-sensitive basis.***

1.4.2 Types of customer information to be obtained and identification data to be used to verify the information are provided as ***Appendix A*** to this Regulation.

In respect of customers that are ***legal persons or legal arrangements,*** financial institutions are required :

(*a*) to verify any person purporting to have been authorized to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person ; and

(*b*) to verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Corporate Affairs Commission (CAC) or similar evidence of establishment or existence and any other relevant information.

1.4.3. Financial institutions are required to identify a ***beneficial-owner*** and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is.

1.4.4. Financial institutions are required ***in respect of all customers*** to determine whether or not a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the FI is required to take reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.

1.4.5. Financial institutions are required to take reasonable measures ***in respect of customers that are legal persons or legal arrangements*** to :

(*a*) understand the ownership and control structure of such a customer ; and

(*b*) determine the ***natural persons*** that ultimately own or control the customer.

The natural persons include those persons who exercise ultimate and effective control over the legal person or arrangement. Examples of types of measures needed to satisfactorily perform this function include :

- ***For companies*** - The natural persons are those who own the controlling interests nd those who comprise the ***mind*** and ***management*** of the company ; and

• *For trusts* – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

Where the customer or the owner of the controlling interest is a public company subject to regulatory disclosure requirements (i.e. a public company listed on a recognized stock exchange) it is not necessary to identify and verify the identity of the shareholders of such a public company.

1.4.6. Financial institutions are required to ***obtain information on the purpose and intended nature of the business relationship of their potential customers.***

1.4.7. Financial institutions are required to conduct ***ongoing due diligence*** on the business relationship as stated by the customers above.

1.4.8. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the financial institution/customer relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

1.4.9. Financial Institutions are required to ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business-relationships or customer categories.

Higher Risk Customers.

1.5.1. Financial institutions are required to ***perform enhanced due diligence for higher-risk customer, business relationship or transaction.***

Examples of higher-risk customers :

(*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 ; and

(*e*) Politically exposed persons (PEPs), cross-border banking and business relationships, etc.

1.5.2: Where ***there are low risks, financial institutions are required to apply reduced or simplified measures.*** There are low risks in ***circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in national systems.*** In circumstances of low-risk, financial institutions are required to apply the simplified or reduced CDD measures

when identifying and verifying the identity of their customers and the beneficial-owners.

Lower Risk Customers, Transactions or Products.

1.6.1. These include:

1.6.1.1. Financial institutions—provided they are subject to the requirements for the combat of money laundering and terrorist financing which are consistent with the provisions of this Regulation and are supervised for compliance with them ;

1.6.1.2. Public companies (listed on a stock exchange or similar situations) that are subject to regulatory disclosure requirements ;

1.6.1.3. Government ministries and parastatals /enterprises ;

1.6.1.4. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by NAICOM ;

1.6.1.5. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral ;

1.6.1.6. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme ; and

1.6.1.7. Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBPs) provided that they are subject to the requirements for the combat of money laundering and terrorist financing consistent with the provisions of the Money Laundering (Prohibition) Act, 2004.

1.6.2. Financial institutions that apply simplified or reduced CDD measures to customers resident abroad are required to limit such to customers in countries that have effectively implemented the FATF Recommendations.

1.6.3. ***Simplified CDD measures are not acceptable and therefore cannot apply to a customer whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios. In such a circumstance, enhanced due diligence is mandatory.***

1.6.4. Financial institutions are to adopt ***CDD measures on a risk sensitive-basis.*** Examples of higher risk categories are ***included in item 1.5.1(a – e) above*** and financial institutions are required to determine in each case whether the risks are low or not, having regard to the type of customer, product, transaction or the location of the customer. Where there is doubt, financial institutions are directed to clear with the CBN.

Timing of Verification.

1.7.1. Financial institutions are required to verify the identity of the customer, beneficial-owner and occasional customers ***before or during***

the course of establishing a business relationship or conducting transactions for them.

1.7.2. Financial institutions are ***permitted to complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, only when*** :

(*a*) this can take place as soon as reasonably practicable ;

(*b*) it is essential not to interrupt the normal business conduct of the customer ; and

(*c*) the money laundering risks can be effectively managed.

1.7.3. Examples of situations ***where it may be essential not to interrupt the normal conduct of business include*** :

☐ ***Non face-to-face business.***

☐ ***Securities transactions*** — In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them and the performance of the transaction may be required before verification of identity is completed.

☐ ***Life insurance business*** in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

1.7.4. Where a customer is permitted to utilize the business relationship prior to verification, financial institutions are required to adopt ***risk management procedures*** concerning the conditions under which this may occur. These ***procedures include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions*** being carried out outside the expected norms for that type of relationship.

Failure to Complete CDD.

1.8.1. The financial institution which does not comply with ***items 1.4.1 to 1.4.6*** above is :

(*a*) not permitted to open the account, commence business relations or perform the transaction ; and

(*b*) required to render a suspicious transaction report to the NFIU.

1.8.2. The financial institution that has already commenced the business relationship (e.g. items ***1.3.1.5, 1.7.2 or 1.9.1, 1.4.1 to 1.4.5 above***) is required to terminate the business relationship and render ***suspicious transaction reports to the NFIU.***

Existing Customers.

1.9.1. Financial institutions are required to ***apply CDD requirements to existing customers*** on the basis of materiality and risk and to continue to conduct due diligence on such existing relationships at appropriate times.

1.9.2. The appropriate time to conduct CDD by financial institutions is when (*a*) a transaction of significant value takes place, (*b*) a customer documentation standards change substantially, (*c*) there is a material change in the way that the account is operated, and (*d*) the institution becomes aware that it lacks sufficient information about an existing customer.

The financial institution is required to properly identify the customer in accordance with these criteria. The customer identification records should be made available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

Definition of a Politically Exposed Person (PEP).

1.10.1. *PEPS are individuals who are or have been entrusted with prominent public functions in Nigeria and/or foreign countries and people/ entities associated with them.*

Examples of PEPs include, but are not limited to :

- Heads of State or government ;
- State 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 ; and
- Members of Royal Families.

1.10.2. Financial institutions are required, in addition to performing CDD measures, ***to put in place appropriate risk management systems*** to determine whether a potential customer or existing customer or the beneficial-owner is a politically exposed person.

1.10.3. Financial institntions are also required to obtain senior management approval before they establish bnsiness relationships with a PEP and to render monthly returns on all their transactions with PEPs to the CBN and NFIU.

1.10.4. ***Where a customer has been accepted or has an ongoing relationship with the financial institution and the customer or beneficial-owner is subsequently found to be or becomes a PEP, the financial institution is required to obtain senior management approval in order to continue the business relationship.***

1.10.5. Financial institutions are required to ***take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial-owners*** identified as PEPs.

1.10.5. A Financial institution in a business relationship with a PEP is required to conduct ***enhanced ongoing monitoring*** of that relationship. In the event of ***any transaction that is abnormal, FIs are required to flag the account and to report immediately to the NFIU.***

Cross-Border and Correspondent Banking.

1.11. ***Correspondent banking*** is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable-through-accounts and foreign exchange services.

1.11.1. In relation to cross-border and correspondent banking and other similar relationships, ***financial institutions are required to***, in addition to performing the normal CDD measures, ***take the following measures*** :

- Gather sufficient information about a respondent institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to a money laundering or terrorist financing investigation or regulatory action.

- Assess the respondent institution's AML/CFT controls and ascertain that they are in compliance with FATF standard.

- Obtain approval from senior management before establishing correspondent relationships.

- Document the respective AML/CFT responsibilities of such institution.

1.11.2. Where a correspondent relationship involves the maintenance of payable-through- account, the financial institution should be satisfied that :

(*a*) its customer (the respondent bank or financial institution) has performed the normal CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution ; and

(*b*) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

New Technologies and Non-Face-to-Face Transactions.

1.12.1. Financial institutions are required ***to have policies in place or take such measures as may be needed to prevent the misuse of technological developments*** such as ***internationally accepted Credit or Debit Cards and mobile Telephone Banking systems for purpose of money laundering and terrorist financing schemes.***

1.12.2. Financial institutions are required to have ***policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions***. These policies and procedures shall be applied automatically when establishing customer relationships and conducting ongoing due diligence. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

1.12.3. A financial institution that ***relies upon a third party should immediately obtain the necessary information concerning property which has been laundered or which constitutes proceeds from, instrumentalities used in and intended for use in the commission of money laundering and financing of terrorism or other predicate offences***. Such financial institution should satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

1.12.4. The Financial Institution should satisfy itself that the ***third party is a regulated and supervised institution*** and has measures in place to comply with requirements of CDD and reliance on intermediaries and other third parties on CDD as contained in this Regulation.

Reliance on Intermediaries and Third Parties on CDD Function.

1.13.1. ***Financial institutions relying on intermediaries or other third parties which have no outsourcing or agency relationships, business relationships, accounts or transactions between financial institutions for their clients are required to perform some of the elements of the CDD process on the introduced business.*** The following criteria should also be met :

- Immediately obtain from the third party the necessary information concerning certain elements of the CDD process ;
- Take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay ;
- Satisfy themselves that the third party is regulated and supervised in accordance with Core Principles of AML/CFT and has measures in place to comply with the CDD requirements set out in this Regulation ; and
- Make sure that adequate KYC provisions are applied to the third party in order to obtain account information for competent authorities.

The ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

Maintenance of Records on Transactions.

1.14.1. Financial institutions are required to maintain all necessary records of transactions, both domestic and international, ***for at least five years following completion of the transaction (or longer if requested by***

the CBN and NFIU in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

1.14.2. Examples of the ***necessary components of transaction-records include customer's and beneficiary's names, addresses*** (or other identifying information normally recorded by the intermediary), ***the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transaction***.

1.14.3. Financial institutions are required to maintain records of the identification data, account files and business correspondence ***for at least five years following the termination of an account or business relationship*** (or longer if requested by the CBN and NFIU in specific cases).

1.14.4. Financial institutions are required to ensure that all customer-transaction records and information are available on a timely basis to the CBN and NFIU.

Attention on Complex and Unusual Large Transactions (STRs).

1.15.1. Financial institutions are required to pay special attention to all complex, unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance or transactions which fall outside the regular pattern of the account's activity.

1.15.2. Financial institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the NFIU ; and make them available for CBN, NFIU, other competent authorities and auditors for at least five years.

Suspicious Transactions, Compliance Monitoring and Response to Suspicious Transactions.

1.16.1. ***Definition of a Saspicious Transaction***

There are numerous types of suspicious transactions and these reflect the various ways in which money launderers operate. For the purpose of this Regulation, a suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. It includes such a transaction that is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks obvious economic rationale.

1.16.2. ***Institutional Policy***

1.16.2.1. Every financial institution is required to have a written policy framework that would guide and enable its staff to monitor,

recognize and respond appropriately to suspicious transactions. A list of ***Money Laundering "Red Flags"*** is provided in ***Appendix C*** to this Regulation.

1.16.2.2. Every financial institution is required to ***designate an officer appropriately as the AML/CFT Compliance Officer to supervise the monitoring and reporting of suspicious transactions, among other duties.***

1.16.2.3. Every financial institution should be alert to the ***various patterns of conduct that have been known to be suggestive of money laundering and maintain a checklist of such transactions which should be disseminated to the relevant staff.***

1.16.2.4. When any staff of a financial institution detects any "red flag" or suspicious money laundering activity, the institution is ***required to promptly institute a "Review Panel" under the supervision of the AML/CFT Compliance Officer. Every action taken must be recorded***. The institution and its staff are required to maintain confidentiality in respect of such investigation and any suspicious transaction report that may be filed with the competent authority. This action is, however, in compliance with the provisions of the money laundering law that criminalize ***"tipping off"*** (i.e. doing or saying anything that might tip off someone else that he is under suspicion of money laundering).

1.16.2.5. A financial institution that suspects or has reason to suspect that funds are the proceeds of a criminal activity or are related to terrorist financing, is required to report promptly its suspicions to the NFIU. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved. This requirement to report snspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

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

Internal Controls, Compliance and Audit.

1.17.1. Financial institutions are required ***to establish and maintain internal procedures, policies and controls to prevent money laundering and financing of terrorism and to communicate these to their employees***. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

1.17.2. The AML/CFT compliance officer and appropriate staff are to have timely access to customer identification data, CDD information, transaction records and other relevant information.

1.17.3. Financial institutions are therefore ***required to develop programs against money laundering and terrorist financing*** that include :

(*a*) The development of internal policies, procedures and controls, including appropriate compliance management arrangement and ***adequate screening procedures to ensure high standards when hiring employees*** ;

(*b*) An ongoing employee training programs to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting; and

(*c*) ***Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.***

Financial Institutions are required to put in place a structure that ensures the operational independence of the Chief Compliance Officer (CCO) and Branch Compliance Officers.

1.18. OTHER MEASURES

These measures are meant to deter money laundering and terrorist financing. They include measures on sanctions, shell banks, other forms of reporting, special attention for high risk countries and foreign branches and subsidiaries of Nigerian financial institutions.

Sanctions.

1.18.1.1. The sanctions provided here are not only proportionate and dissuasive but are such that will affect legal persons/financial institutions and their directors/senior management staff also, depending on the provisions of the Regulation breached. Every financial institution which fails to comply or contravenes the provisions contained in this Regulation shall be subject to sanction by the CBN. Any individual, being an official of a financial institution, who fails to take reasonable steps to ensure compliance with the provisions of this Regulation shall be sanctioned accordingly. For purpose of emphasis, ***incidence of false declaration or false disclosure by a financial institution or its officers shall be subject to administrative review and sanction as stipulated in this Regulation.***

1.18.1.2. Any financial institution or its officer that contravenes the provisions of this Regulation shall be subject to applicable sanctions by the CBN as follows:

1.18.1.3. ***Against the Institution***

(*a*) Imposition of a penalty not exceeding ₦2,000,000 from the first to the fifth instances on each offence ; and

(*b*) On the sixth instance, the ***CBN shall set up an investigation panel*** to :

(*i*) examine the institution's operations and identify the role of the Board, Management and officers in respect of the malpractice ;

possible, be examined and written findings made available to assist competent authorities.

Financial institutions are also required to report suspicious transactions relating to terrorism financing to the NFIU.

1.18.4.3. Financial institutions that do business with foreign institutions which do not continue to apply or insufficiently apply the provisions of FATF Recommendations are required to take measures such as the following :

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from that jurisdiction ;

- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

- In considering requests for approving the establishment of subsidiaries or branches or representative offices of financial institutions, in countries applying the countermeasure, take into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;

- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering; limiting business relationships or financial transactions with the identified country or persons in that country.

Foreign Branches and Subsidiaries.

1.18.5.1. Financial institutions are required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the provisions of this Regulation and to apply them to the extent that the local/host country's laws and regulations permit.

1.18.5.2. Financial institutions are required to ensure that the above principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply such requirements as contained in this Regulation. Where these minimum AML/CFT requirements and those of the host country differ, branches and subsidiaries of Nigerian financial institutions in the host country are required to apply the higher standard and such must be applied to the extent that the host country's laws, regulations or other measures permit.

1.18.5.3. ***Financial institutions are required to inform the CBN in writing when their foreign branches or subsidiaries are unable to***

observe the appropriate AML/CFT measures because they are prohibited by the host country's laws, regulations or other measures.

1.18.5.4. Because financial institutions are subject to these AML/CFT principles, they are therefore required to apply consistently the CDD measures at their group levels, taking into account the activity of the customer with the various branches and subsidiaries.

AML/CFT Employee-Education and Training Programme.

1.18.6.1. ***Institutional Policy***

1.18.6.1.1. Financial institutions are required to design comprehensive employee education and training programs not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks. Indeed, the establishment of such an employee training program is not only considered as best practice hut also a statutory requirement.

1.18.6.1.2. The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the financial institution. Nevertheless, a comprehensive training program is required to encompass staff/areas such as Compliance officers; new staff (as part of the orientation program for those posted to the front office); banking operations/brauch office staff (particularly cashiers, account opening, mandate, and marketing staff); internal control/audit staff and managers. ***Finaneial institutions are required to render quarterly returns on their level of compliance to the CBN and NFIU.***

1.18.6.1.3. The employee training program is required to be developed under the guidance of the AML/CFT Compliance Officer in collaboration with the top Management. The basic elements of the employee training program are expected to include :

- AML regulations and offences
- The nature of money laundering
- Money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies
- Reporting requirements
- Customer due diligence
- Risk-based approach to AML/CFT
- Record keeping and retention policy.

Financial Institutions are required to submit their Annual AML/CFT Employee training program for the next year to the CBN and NFIU not later than the 31st of December every financial year.

1.18.7.1 Financial institutions are required to monitor their employees' accounts for potential signs of money laundering. They are also required to subject employees' accounts to the same AML/CFT procedures as applicable to other customers' accounts. ***This is required to be performed under the supervision of the AML/CFT Chief Compliance Officer***. The latter's own account is to be reviewed by the Chief Internal Auditor or a person of adequate/similar seniority. ***Compliance reports including findings are to be rendered to the CBN and NFIU at the end of June and December every year.***

Monitoring of Employee Conduct.

1.18.7.2. The AML/CFT performance review of staff is required to be part of employees' annual performance appraisals.

1.18.8.1. Financial institutions are required to ***direct their employees in writing to always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to the NFIU.*** They are also required to make it possible for employees to report any violations of the institution's AML/CFT compliance program to the AML/CFT Compliance Officer. Where the violations involve the Chief Compliance Officer, employees are required to report such to a designated higher authority such as the Chief Internal Auditor.

Protection of Staff who Report Violations.

1.18.8.2. Financial institutions are required to inform their employees in writing to make such reports confidential and that they will be protected from victimization for making them.

1.19.1. ***Financial institutions are required to review, identify and record other areas of potential money laundering risks not covered by this Regulation and report same quarterly to the CBN and NFIU.***

Additional Areas of AML/CFT Risks.

1.19.2. Financial institutions are therefore required to review their AML/CFT frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks not covered by the AML/CFT Regulation.

1.20. Having reviewed the AML/CFT framework and identified new areas of potential money laundering vulnerabilities and risks, ***financial institutions are required to design additional procedures and mitigants as contingency plan*** in their AML/CFT Operational Manuals. These will provide how such potential risks will be appropriately managed if they crystallize. ***Details of the contingency plan are to be rendered to the CBN and NFIU as at 31st December every financial year.***

Additional Procedures and Mitigants.

1.21. Every financial institution is required to make a policy commitment and to subject its AML/CFT Compliance Program to independent-testing or require its internal audit function to determine its adequacy, completeness and effectiveness. ***Report of compliance is required to be rendered to the***

Testing for the Adequacy of the AML/CFT Compliance.

CBN and NFIU as at 31st December every financial year. Any identified weaknesses or inadequacies should be promptly addressed by the financial institution.

Formal Board Approval of the AML/CFT Compliance.

1.22. The ultimate responsibility for AML/CFT compliance is placed on the Board/Top Management of every financial institution in Nigeria. It is, therefore, required that the Board ensures that a ***comprehensive operational AML/CFT Regulation is formulated by Management and presented to the Board far consideration and formal approval.*** Copies of the approved Regulation above are to be forwarded to the CBN and NFIU within six months of the release of this Regulation. Quarterly reports on the AML/CFT-compliance status of the financial institution are to be presented to the Board for its information and necessary action.

Culture of Compliance.

1.23. Every financial institution is required to have a ***comprehensive AML/CFT- compliance program*** to guide its compliance efforts and to ensure the diligent implementation of its Programme. Indeed, entrenching a culture of compliance would not only minimize the risks of being used to launder the proceeds of crime but also provide protection against fraud, reputation and financial risks.

Special Recommendations.

1.24.1. Terrorist financing offences extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that the funds would be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist.

1.24.2. Terrorist financing offences are extended to any *funds* whether from a legitimate or illegitimate source. ***Terrorist financing offences, therefore, do not necessarily require that the funds are actually used to carry out or attempt a terrorist-act or be linked to a specific terrorist-act. Attempt to finance terrarist/terrorism and to engage in any of the types of conduct as set out above is also an offence.***

1.24.3. Terrorist financing offences are predicate offences for money laundering. Terrorist financing offences therefore apply, regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist/terrorist organization is located or the terrorist act occurred or will occur.

Money or Valne Transfer (MVT) Services.

1.25.1. All natural and legal persons that perform ***Money or Value Transfer Service (MVTs operators)*** are required to be licensed by the CBN. The operators are therefore subject to the provisions of this Regulation.

1.25.2. ***MVT service operators are required to maintain a current list of its agents and quarterly returns of such be rendered to the CBN.*** They are required to gather and maintain sufficient information about their agents and correspondent operators or any other operators or institutions they may do business with.

1.25.3. MVT operators are required to assess their agents' and correspondent operators' AML/CFT controls and ascertain that they are adequate and effective. They are required to obtain approval from the CBN before establishing new correspondent relationships. They are also required to document and maintain a checklist of the respective AML/CFT responsibilities of each of its agents and correspondent operators.

Wire Transfers.

1.26.1. ***For all wire transfers of USD 1,000 or more***, the ordering financial institutions are required to obtain and maintain the following information relating to the originator of the wire transfer :

- The name of the originator ;
- The originator's account number (or a unique reference number if no account number exists) ; and
- The originator's address (the address can be substituted with a national identity number).

1.26.2. ***For all wire transfers of USD 1,000 or more***, the ordering financial institution is required to verify the identity of the originator in accordance with the CDD requirements contained in this Regulation.

1.26.3. ***For cross-border wire transfers of USD 1,000 or more,*** the ordering financial institution is required to include the full originator information above in the message or the payment form accompanying the wire transfer.

1.26.4. ***However, if several individual cross-border wire transfers of USD 1,000 or more from a single originator are bundled in a batch-file for transmission to beneficiaries in another country,*** the ordering financial institution should only include the originator's account number or unique identifier on each individual cross-border wire transfer, provided that the batch-file (in which the individual transfers are batched) contains full originator information that is fully traceable within the recipient country.

1.26.5. ***For domestic wire transfers,*** the ordering financial institution is required to either :

(*a*) include the full originator information in the message or the payment form accompanying the wire transfer ; or

(*b*) include only the originator's account number or a unique identifier, within the message or payment form.

1.26.6. The second option should be permitted by financial institution only if full originator information can be made available to the beneficiary financial institution and to the appropriate authorities within three business days of receiving the request.

1.26.7. Each intermediary and beneficiary financial institution in the payment chain is required to ensure that all originator information that accompanies a wire transfer is transmitted with the transfer.

1.26.8. ***Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from being transmitted with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.***

1.26.9 Beneficiary financial institutions are required to adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator information. ***The lack of complete originator information is considered as a factor in assessing whether a wire transfer or related transactions are suspicious. The financial institutions are therefore required to report to the NFIU.***

1.26.10. ***The beneficiary financial institution is required to restrict or even terminate its business relationship with the financial institutions that fail to meet the above standards.***

1.26.11. Cross-border and domestic transfers between financial institutions are, however, not intended to cover the following types of payments :

(*a*) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction, such as withdrawals from a bank account through an ATM machine, cash advances from a credit card or payments for goods and services. However, ***when credit or debit cards are used as a payment system*** to effect a money transfer the necessary information should be included in the message ; and

(*b*) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

PART B—GUIDANCE ON KNOW YOUR CUSTOMER (KYC)

2.0 Financial institutions should not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the business they intend to conduct ascertained. Once an on-going business relationship is established, any inconsistent activity can then be examined to determine whether or not there is an element of money laundering or its suspicion.

Duty to Obtain Identification Evidence.

2.1.1. The first requirement of knowing your customer for money laundering purposes is for the financial institution to be satisfied that a prospective customer is who he/she claims to be.

2.1.2. Financial institutions should not carry out or agree to carry out financial business or provide advice to a customer or potential customer unless they are certain as to who that person actually is. If the customer is acting on behalf of another (the funds are supplied by someone else or the investment is to be held in the name of someone else) ***then the financial institution has the obligation to verify the identity of both the customer and the agent/trustee unless the customer is itself a Nigerian regulated financial institution.***

2.1.3. Financial institutions have the duty to obtain evidence in respect of their customers. There are certain exceptions to this duty as set out in ***Section 2.9 of this Regulation.*** Since exemptions are difficult to apply, financial institutions are required ***to identify all relevant parties to the relationship from the outset***. The general principles and means of obtaining satisfactory identification evidence are also set out below :

Nature and Level of the Business.

2.2.1. ***Financial institutions are*** required to ***obtain sufficient information on the nature of the business that their customer intends to undertake,*** including the expected or predictable pattern of transactions.

The information collected at the outset for this purpose should include :

- purpose and reason for opening the account or establishing the relationship;
- nature of the activity that is to be undertaken;
- expected origin of the funds to be used during the relationship; and
- details of occupation/employment/business activities and sources of wealth or income.

2.2.2. ***Financial institutions*** are required to take reasonable steps to keep the information up to date as the opportunities arise, such as when an existing customer opens a new account. Information obtained during any meeting, discussion or other communication with the customer is required to be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily accessible to the Money Laundering Compliance Officers (MLCO) or relevant regulatory bodies.

Apply Commercial Judgment.

2.3.1. Financial institutions are required to take a risk-based approach to the 'Know Your Customer' requirements. Financial institutions are also required to decide the number of times to verify the customers' records during the relationship, the identification evidence required and when additional checks are necessary. These decisions are equally required to be recorded. For personal account relationships, all joint-account holders

need to be verified. In respect of private company or partnership, focus should be on the principal owners/controllers and their identities must also be verified.

2.3.2. ***The identification evidence collected at the outset should be viewed against the inherent risks in the business or service.***

2.4. ESTABLISHING IDENTITY

Identification Evidence.

2.4.1.2. The customer identification process should not start and end at the point of establishing the relationship but continue as far as the business relationship subsists. The process of confirming and updating identity and address, and the extent of obtaining additional KYC information collected will however differ from one type of financial institution to another.

2.4.1.3. The general principles for establishing the identity of both legal and natural persons and the guidance on obtaining satisfactory identification evidence set out in this Regulation are by no means exhaustive.

What is Identity?

2.4.2.1. Identity generally means a set of attributes such as names used, date of birth and the residential address at which the customer can be located. These are features which can uniquely identify a natural or legal person.

2.4.2.2. In the case of a natural person, ***the date of birth is required to be obtained as an important identifier in support of the name.*** It is, however, not mandatory to verify the date of birth provided by the customer.

2.4.2.3. Where an international passport/national identity card is taken as evidence of identity, the number, date and place/country of issue (as well as expiring date in the case of international passport) are required to be recorded.

When Must Identity be Verified?

2.4.3.1. Identity is required to be verified whenever a business relationship is to be established, on account opening or during one-off transaction or when a series of linked transactions takes place. ***"Transaction" in this Regulation is defined to include the giving of advice.*** "Advice" here does not apply when information is provided about the availability of products or services when a first interview/discussion prior to establishing a relationship takes place.

2.4.3.2. Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that customer are complete and kept, no further evidence of identity is needed when another transaction or activity is subsequently undertaken.

Redemptions/ Surrenders.

2.4.4.1. When an investor finally realizes his investment (wholly or partially), if the amount payable is US$ 1,000 or above or its equivalent thereof; or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or regulation, the identity of the investor must be verified and recorded if it had not been done previously.

2.4.4.2. In the case of redemption or surrender of an investment (wholly or partially), a financial institution is required to take reasonable measures to establish the identity of the investor where payment is made to :

· the legal owner of the investment by means of a cheque crossed "account payee" ; or

· a bank account held (solely or jointly) in the name of the legal owner of the investment by any electronic means effective for transfer funds.

Whose Identity Must Be Verified?

2.4.5.1. (1) ***Clients*** - sufficient evidence of the identity must be obtained to ascertain that the client is the very person he/she claims to be.

2.4.5.2. (2) ***the person acting on behalf of another*** - The obligation is to obtain sufficient evidence of identities of the two persons involved. This rule is however, subject to some exceptions. In consortium lending, the lead-manager/agent is required to supply a confirmation letter as evidence that he has obtained the required identity.

2.4.5.3. There is no obligation to look beyond the client where :

· the latter is acting on its own account (rather than for a specific client or group of clients) ;

· the client is a bank, broker, fund manager or other regulated financial institutions; and

· All the businesses are to be undertaken in the name of a regulated financial institution.

2.4.5.4. In other circumstances, unless the client is a regulated financial institution acting as agent on behalf of one or more underlying clients within Nigeria, and has given written assurance that it has obtained the recorded-evidence of identity to the required standards, identification evidence should be verified for :

· ***the named account holder/person*** in whose name an investment is registered ;

· ***any principal beneficial owner of funds*** being invested who is not the account holder or named investor ;

· ***the principal controller(s) of an account*** or business relationship (i.e. those who regularly provide instructions) ; and

· ***Any intermediate parties*** **(*e.g.*** where an account is managed or owned by an intermediary).

2.4.5.6. ***Financial institutions are required to take appropriate steps to identify directors and all the signatories to an account.***

2.4.5.7. ***Joint applicants/account holders*** - identification evidence should be obtained for all the account holders.

2.4.5.8 ***For higher risk business*** undertaken for private companies (i.e. ***those not listed on the stock exchange***) sufficient evidence of identity and address should be verified in respect of :

· the principal underlying beneficial owner(s) of the company with 5% interest and above: and

· Those with principal control over the company's assets (e.g. principal controllers/directors).

2.4.5.9. Financial institutions are required to be alert to circumstances that might indicate any ***significant changes in the nature of the business or its ownership*** and make enquiries accordingly and to observe the ***additional provisions for High Risk Categories of Customers under AML/CFT Directive in this Regulation.***

2.4.5.10. ***Trusts*** – Financial institutions are required to obtain and verify the identity of those providing funds for the Trust. They include the settler and those who are authorized to invest, transfer funds or make decisions on behalf of the Trust such as the principal trustees and controllers who have power to remove the Trustees.

Savings Schemes and Investments in Third Parties' Names.

2.4.6. When an investor sets up a savings accounts or a regular savings scheme whereby the funds are supplied by one person for investment in the name of another (such as a spouse or a child), ***the person who funds the subscription or makes deposits into the savings scheme*** should be regarded as the applicant for business for whom identification evidence must be obtained ***in addition to the legal owner.***

Personal Pension Schemes.

2.4.7.1. Identification evidence must be obtained at the outset for all investors, except personal pensions connected to a policy of insurance taken out by virtue of a contract of employment or pension scheme.

2.4.7.2. Personal pension advisers are charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider. Confirmation that identification evidence has been taken should be given on the transfer of a pension to another provider.

Timing of Identification Requirements.

2.4.8.1 An acceptable time-span for obtaining satisfactory evidence of identity will be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain

the evidence before commitments are entered into or money changes hands. ***However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regard to the risk.***

2.4.8.2. To this end, financial institutions are required to :

(*i*) obtain identification evidence as soon as reasonably practicable after it has contact with a client with a view to agreeing with the client to carry out an initial transaction; or reaching an understanding (whether binding or not) with the client that it may carry out future transactions; and

(*ii*) Where the client does not supply the required information as stipulated in (I) above, the financial institution is required to ***discontinue any activity it is conducting for the client*** ; and bring to an end any understanding reached with the client.

2.4.8.3. ***Financial institutions are required to also observe the provision in the Timing of Verification under the AML/CFT Directive of this Regulation.***

2.4.8.4. A financial institution may however start processing the business or application immediately, provided that it :

· ***promptly takes appropriate steps to obtain identification evidence ; and***

· ***Does not transfer or pay any money out to a third party until the identification requirements have been satisfied.***

2.4.8.5. The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation may lead to a suspicion that the depositor or investor is engaged in money laundering. ***The financial institution is required to therefore make a Suspicious Activity Report to the NFIU based on the information in its possession before the funds involved are returned to the potential client or where they came from.***

2.4.8.6. Financial institutions are required to ***have in place written and consistent policies of closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.***

2.4.8.7. Financial institutions are also required to respond promptly to inquiries made by competent authorities and financial institutions relating to the identity of their customers.

Cancellation and Cooling-off Rights.

2.4.9. Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid subject to some deductions, where applicable. Since cancellation/cooling-off rights could offer a readily available,route for laundering money. financial institutions should be alert

to any abnormal exercise of these rights by an investor or in respect of business introduced through an intermediary. ***In the event where abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported to the NFIU.***

2.5. IDENTIFICATION PROCEDURES

General Principles.

2.5.1.1. A financial institution is required to ensure that it is dealing with a real person or organization (natural, corporate or legal) by obtaining sufficient identification evidence. ***When reliance is being placed on a third party to identify or confirm the identity of an applicant, the overall responsibility for obtaining satisfactory identification evidence rests with the account holding financial institution.***

2.5.1.2. The requirement in all cases is to obtain satisfactory evidence that a person of that name lives at the address given and that the applicant is that person or that the company has identifiable owners and that its representatives can be located at the address provided.

2.5.1.3. Because no single form of identification can be fully guaranteed as genuine or representing correct identity, the identification process should be cumulative.

2.5.1.4. The procedures adopted to verify the identity of private individuals and whether or not identification was done face to face or remotely are required to be stated in the customer's file. The reasonable steps taken to avoid single, multiple fictitious applications or substitution (impersonation) fraud are required to be stated also by the financial institution.

2.5.1.5. An introduction from a respected customer, a person personally known to a Director or Manager or a member of staff often provides comfort ***but must not replace the need for identification evidence requirements to be complied with as set out in this Regulation.*** Details of the person who initiated and authorized the introduction should be kept in the customer's mandate file along with other records. ***It is therefore mandatory that Directors/Senior Managers insist on following the prescribed identification procedures for every applicant.***

New Business for Existing Customers.

2.5.2.1. When an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address for such a customer unless the name or the address provided does not tally with the information in the financial institution's records. However, procedures are required to be put in place to guard against impersonation or fraud. The opportunity of opening the new account should also be taken to ask the customer to confirm the relevant details and to provide any missing KYC information. This is particularly important :

· if there was an existing business relationship with the customer and identification evidence had not previously been obtained ; or

· if there had been no recent contact or correspondence with the customer within the past three months ; or

· When a previously dormant account is re-activated.

2.5.2.2. In the circumstances above, details of the previous account(s) and any identification evidence previously obtained or any introduction records should be linked to the new account-records and retained for the prescribed period in accordance with the provision of this Regulation.

Certification of Identification Documents.

2.5.3.1. In order to guard against the dangers of postal-interception and fraud, prospective customers should not be asked to send by post originals of their valuable personal identity documents such as international passport, identity card, drivers' licence, etc.

2.5.3.2. Where there is no face-to-face contact with the customer and documentary evidence is required, copies certified by a lawyer, notary public/court of competent jurisdiction, banker, accountant, senior public servant or their equivalent in the private sector should be obtained. The person undertaking the certification must be known and capable of being contacted if necessary.

2.5.3.3. In the case of foreign nationals, a copy of international passport, national identity card or documentary evidence of his/her address is required to be certified by :

the embassy, consulate or high commission of the country of issue ; or

a senior official within the account opening institution; or

a lawyer, attorney or notary public.

2.5.3.4. Certified copies of identification evidence are to be stamped, dated and signed ***"original sighted by me"*** by a senior officer of the financial institution. Financial institutions are required to always ensure that a good production of the photographic evidence of identity is obtained. ***Where this is not possible, a copy of evidence certified as providing a good likeness of the applicant could only be acceptable in the interim.***

Recording Identification Evidence.

2.5.4.1. ***Records of the supporting evidence and methads used to verify identity are required to be retained for a minimum period of five years after the account is closed or the business relationship ended.***

2.5.4.2. Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details

of the identification evidence are required to be recorded to enable the documents to be obtained later. Confirmation is required to be provided that the original documents were seen by certifying either on the photocopies or on the record that the details were taken down as evidence.

2.5.4.3. Where checks are made electronically, a record of the actual information obtained or where it can be re-obtained must be retained as part of the identification evidence. Such records will make the reproduction of the actual information that would have been obtained before, less cumbersome.

Concession in respect of Payment made by Post.

2.5.5.1. Concession may be granted for produet or services (***where the money laundering risk is considered to be low***) in respect of long-term life insurance business or purchase of personal investment products. If payment is to be made from an account held in the customer's name (or jointly with one or more other persons) at a regulated financial institution, no further evidence of identity is necessary.

2.5.5.2. Waiver of additional verification requirements for postal or electronic transactions ***does not apply to the following*** :

- products or accounts where funds can be transferred to other types of products or accounts which provide cheque or money transfer facilities ;
- situations where funds can be repaid or transferred to a person other than the original customer ;
- investments where the characteristics of the product or account may change subsequently to enable payments to be made to third parties.

2.5.5.3. ***Postal concession is not an exemption from the requirement to obtain satisfactory evidence of a customer's identity.*** Payment debited from an account in the customer's name shall be capable of constituting the required identification evidence in its own right.

2.5.5.4. ***In order*** to avoid criminal money from being laundered by a customer who uses a third-party cheque, draft or electronic payment drawn on a bank, etc, financial institutions may rely upon the required documentary evidence of the third party, without further verification of the identity, where there is no apparent inconsistency between the name in which the application is made and the name on the payment instrument. Payments from joint accounts are considered acceptable for this purpose. ***The overriding requirement is that the name of the account-holder from where the funds have been provided must be clearly indicated on the record reflecting the payment/ receipt.***

2.5.5.5. In the case of a mortgage institution's cheque or banker's draft, it will only be possible to rely on this concession if the holder of

the account from which the money is drawn is confirmed to have met the KYC requirements by the mortgage institution or bank. Likewise, payments by direct debit or debit card cannot be relied upon unless the authentication procedure identifies the name of the account holder from which the payment is drawn and confirms the customer's address.

2.5.5.6. In respect of direct debits, it cannot be assumed that the account-holding bank/institution will carry out any form of validation of the account name and number or that the mandate will be rejected if they do not match. Consequently, where payment for the product is to be made by direct debit or debit card/notes, and the applicant's account details have not previously been verified through sighting of a bank statement or cheque drawn on the account, ***repayment proceeds should only be returned to the account from which the debits were drawn.***

2.5.5.7. Records are required to be maintained indicating how a transaction arose, including details of the financial institution's branch and account number from which the cheque or payment is drawn.

2.5.5.8. The concession can apply both where an application is made directly to the financial institution and where a payment is passed through a regulated intermediary.

2.5.5.9. ***A financial institution that has relied on the postal concession to avoid additional verification requirements (which must be so indicated on the customer's file) cannot introduce thot customer to another financial institution for the purpose of offering bank accounts or other products that provide cheque or money transmission facilities.***

2.5.5.10. If such a customer wishes to migrate to an account that provides cheque or third party transfer facilities, then additional identification checks must be undertaken at that time. Where these circumstances occur on a regular basis, financial institutions are required to identify all the parties to the relationship at the outset.

Term Deposit Account (TDA).

2.5.6. TDA can be broadly classified as a one-off transaction. However, financial institutions should note that concession is not available for TDAs opened with cash where there is no audit trail of the source of funds or where payments to or from third parties are allowed into the account. The identity verification requirements will therefore differ depending on the nature and terms of the TDA.

Investment Funds.

2.5.7. In circumstances where the balance in an investment funds account is transferred from one Funds Manager to another and the value at that time is above $1,000 or its equivalent and identification evidence has neither been taken nor confirmation obtained from the original Fund Manager, then such evidence should be obtained at the time of the transfer.

2.6. ESTABLISHING IDENTITY

Establishing identity under this Regulation is divided into three broad categories :

- Private individual customers ;
- Quasi corporate customers ; and
- Pure corporate customers.

2.6.1. PRIVATE INDIVIDUALS

General Information.

2.6.1.1.1. The following information is to be established and independently validated for all private individuals whose identities need to be verified :

- the true full name(s) used ; and
- the permanent home address, including landmarks and postcode, where available.

2.6.1.1.2 The information obtained should provide satisfaction that a person of that name exists at the address given and that the applicant is that person. Where an applicant has recently moved from a house, the previous address should be validated.

2.6.1.1.3. ***It is important to obtain the*** date of birth as it is required by the law enforcement agencies. However, the information need not be verified. It is also important for the residence/nationality of a customer to be ascertained to assist risk assessment procedures.

2.6.1.1.4. A risk-based approach should be adopted when obtaining satisfactory evidence of identity. The extent and number of checks can vary depending on the perceived risk of the service or business sought and whether the application is made in person or through a remote medium such as telephone, post or the internet. The source of funds of how the payment was made, from where and by whom must always be recorded to provide an audit trail. ***However, for high risk products, accounts or customers, additional steps should be taken to ascertain the source of wealth/funds***.

2.6.1.1.5. For low-risk accounts or simple investment products such as deposit or savings accounts without cheque-books or automated money transmission facilities, there is an overriding requirement for the financial institution to satisfy itself as to the identity and address of the customer.

Private Individuals Resident in Nigeria.

2.6.1.2. The confirmation of name and address is to be established by reference to a number of sources. The checks should be undertaken by cross-validation that the applicant exists at the stated address either through

the sighting of actual documentary evidence or by undertaking electronic checks of suitable databases, or by a combination of the two. ***The overriding requirement to ensure that the identification evidence is satisfactory rests with the financial institution opening the account or providing the product/service.***

Documenting Evidence of Identity.

2.6.1.3.1. In order to guard against forged or counterfeit-documents, ***care should be taken to ensure that documents offered are originals. Copies that are dated and signed 'original seen' by a senior public servant or equivalent in a reputable private organization could be accepted in the interim, pending presentation of the original documents.*** Hereunder are examples of suitable documentary evidence for Nigerian resident private individuals :

(i) Personal Identity Documents

Primary

- Current International Passport
- National Identity card
- Current Drivers' Licence issued by the Federal Road Safety Commission (FRSC)

Secondary

- Residence Permit issued by the Nigerian Immigration Services (NIS)
- Inland Revenue Tax Clearance Certificate
- Birth Certificate/Sworn Declaration of Age

(ii) Documentary Evidence of Address

- Record of home visit in respect of non-Nigerians
- Confirmation from the electoral register that a person of that name lives at that address
- Recent utility bill (e.g. PHCL, NITEL, etc.)
- State/Local Government Rates
- Bank statement or passbook containing current address
- Solicitor's letter confirming recent house purchase or search report from the Land Registry
- Tenancy Agreement
- Search reports on prospective customer's place of employment and residence signed by a senior officer of the financial institution.

2.6.1.3.2. ***Checking of a local or national telephone directory can be used as additional corroborative evidence but this should not be used as a primary check.***

Physical Checks on Private Individuals Resident in Nigeria.

2.6.1.4.1. ***It is mandatory for financial institutions to establish the true identities and addresses of their customers and for effective checks to be carried out to protect the institutions against substitution of identities by applicants.***

2.6.1.4.2. Additional confirmation of the customer's identity and the fact that the application was made by the person identified should be obtained through one or more of the following procedures :

· a direct mailing of account opening documentation to a named individual at an independently verified address ;

· an initial deposit cheque drawn on a personal account in the applicant's name in another financial institution in Nigeria ;

· telephone contact with the applicant prior to opening the account on an independently verified home or business number or a "welcome call" to the customer before transactions are permitted, utilizing a minimum of two pieces of personal identity information that had been previously provided during the setting up of the account ;

· internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which had been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address ;

· card or account activation procedures.

2.6.1.4.3. ***Financial institutions are required to*** ensure that additional information concerning the nature and level of the business to be conducted and the origin of the funds to be used within the relationship are also obtained from the customer.

Electronic Checks.

2.6.1.5.1. As an alternative or supplementary to documentary evidence of identity and address, the applicant's identity, address and other available information may be checked electronically by accessing other data-bases or sources. Each source may be used separately as an alternative to one or more documentary checks.

2.6.1.5.2. ***Financial institutions are required to*** use a combination of electronic and documentary checks to confirm different ***sources of the same information provided by the customers***. Physical and electronic checks of the same statement of account are the different sources.

2.6.1.5.3. In respect of electronic checks, confidence as to the reliability of information supplied will be established by the cumulative nature of checking across a range of sources, preferably covering a period of time or through qualitative checks that assess the validity of the information supplied. The number or quality of checks to be undertaken

will vary depending on the diversity as well as the breath and depth of information available from each source. Verification that the applicant is the data-subject also needs to be conducted within the cheeking process.

2.6.1.5.4. Some examples of suitable electronic sources of information are set out below :

· An electronic search of the Electoral Register (is not to be used as a sole identity and address check) ;

· Access to internal or external account database ; and

· An electronic search of public records where available.

2.6.1.5.5. Application of the above process and procedures will assist financial institutions to guard against impersonation, invented-identities and the use of false address. ***However, if the applicant is a non-face to face person, one or more additional measures must be undertaken for re-assurance.***

2.6.1.5.6. ***"Financial Exclusion" For the socially and/or financially disadvantaged Applicants Resident in Nigeria.***

2.6.1.5.7. Access to basic banking facilities and other financial services is a necessary requirement for most adults. It is important therefore that the socially-and/or-financially disadvantaged should not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves. ***In circumstances where they cannot reasonably do so, the internal procedures of the financial institutians must make allowance for such persons by way of providing appropriate adviee to staff on how the identities of such group of persons can be confirmed and what checks should he made under these exceptional circumstances.***

2.6.1.5.8. Where a financial institution has reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, ***the institution may aecept as identification evidence a letter or statement from a person in a position of responsibility such os solicitors, doctors, ministers of religion and teachers who know the client, confirming that the client is who he says he is, and to confirm his permanent address.***

2.6.1.5.9. ***When a financial institution has decided to treat a client as "financially excluded", it is required to record the reasons for doing so along with the account opening documents. Returns should then be rendered to the CBN and NFIU quorterly on this category of customers.***

2.6.1.5.10. The financial institution should satisfy itself that such customer is the person he/she claims to be. ***Therefore, where a letter/ statement is accepted from a person in position of responsibility, it should include a telephone number where the person can be contacted for verification. The financiol institution should verify from an independent source the information provided by that person.***

2.6.1.5.11. ***In order to*** guard against "financial exclusion" and to minimize the use of the exception procedure, ***financial institutions must include in their internal procedures the "alternative documentary evidence of personal identity and address" that can be accepted.***

2.6.1.5.12. Financial institutions are required to ***put in place additional monitoring for accounts opened under the financial exclusion exception procedures to ensure that such accounts are not misused.***

Private Individuals not resident in Nigeria.

2.6.1.6.1. For those prospective customers who are not resident in Nigeria but who make face-to- face contact, international passports or national ideutity cards should generally be available as evidence of the name of the customer. 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.

2.6.1.6.2. Financial institutions are required to obtain separate evidence of the applicant's permanent residential address from the best available evidence, preferably from an official source. ***A "P. O. Box number" alone is not accepted as evidence of address***. The applicant's residential address should be such that it can be physically located by way of a recorded description or other meaus.

2.6.1.6.3. Relevant evidence should be obtained by the financial institution directly from the customer or 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. Financial institutions are required to ensure that the customer's true identity and current permanent address are actually confirmed. ***In such cases, copies of relevant identity documents should be sought and retained.***

2.6.1.6.4. Where a foreign national has receutly arrived in Nigeria, reference might be made to his/her employer, university, evidence of traveling documents, etc. to verify the applicant's identity and residential address.

Private Individuals not Resident in Nigeria: Supply of Informatiou.

2.6.1.7.1. For a private individual not resident in Nigeria, who wishes to supply documentary information by post, telephone or electronic means, ***a risk-based approach must be taken.*** The financial institution is required to ***obtain one separate item of evidence of identity in respect of the name of the customer and one separate item for the address.***

2.6.1.7.2. Documentary ***evidence of name and address*** can be obtained :

· by way of original documentary evidence supplied by the customer ; or

· by way of a certified copy of the customer's passport or national identity card and a separate certified document verifying address e.g. a driving licence, utility bill, etc ; or

· through a branch, subsidiary, head office of a correspondent bank.

2.6.1.7.3. ***Where the applicant does not already have a business relationship with the financial institution that is supplying the information or the financial institution is not within Nigeria, certified copies of relevant underlying documentary evidence must be sought, obtained and retained by the institutions.***

2.6.1.7.4. Where necessary, an additional comfort must be obtained by confirming the customer's true name, address and date of birth from a reputable credit institution in the customer's home country.

Financial institutions are requested to use these requirements in conjunction with Appendix A to this Regulation.

Non Face-to-Face Identification.

2.6.1.8.1. Because of possible false identities and impersonations that can arise with non face-to-face customers, it is important to ensure that the applicant is who he/she claims to be. Accordingly, ***one additional measure or check should be undertaken to supplement the documentary or electronic evidence.*** These additional measures will apply whether the applicant is resident in Nigeria or elsewhere and must be particularly robust where the applicant is requesting a bank account or other product/service that offers money transmission or third party payments.

2.6.1.8.2. ***Procedures to identify and authenticate the customer have to ensure that there is sufficient evidence either documentary or electronic to confirm his address and personal identity and to undertake at least one additional check to guard against impersonation or fraud.***

2.6.1.8.3. ***The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk.*** However, care must be taken to ensure that the same level of information is obtained for internet customers and other postal/telephone customers.

2.6.1.8.4. If reliance is being placed on intermediaries to undertake the processing of applications on the customer's behalf, checks should be undertaken to ensure that the intermediaries are regulated for money laundering prevention and that the relevant identification procedures

are applied. ***In all cases, evidence as to how identity has been verified should be obtained and retained with the account opening records.***

2.6.1.8.5. Financial institutions are directed to conduct regular monitoring of internet-based business/clients. If a significant proportion of the business is operated electronically, ***computerized monitoring systems/solutions that are designed to recognize unusual transactions and related patterns of transactions should be put in place to recognize suspicious transactions. AML/CFT compliance officers are required to review these systems/solutions, record exemptions and report same quarterly to the NFIU.***

Refugees and Asylum Seekers.

2.6.1.9.1. A refugee and asylum seeker may require a basic bank account without being able to provide evidence of identity. In such circumstances, authentic references from Ministry of Internal Affairs or an appropriate government agency should be used in conjunction with other readily available evidence.

2.6.1.9.2. Additional monitoring procedures should however be undertaken to ensure that the use of the account is consistent with the customer's circumstances.

Students and Minors.

2.6.1.10.1. When opening accounts for students or other young people, the normal identification procedures set out in this Regulation should be followed as far as possible. Where such procedures would not be relevant or do not provide satisfactory identification evidence, verification could be obtained :

- via the home address of the parent(s) ; or
- by obtaining confirmation of the applicant's address from his/her institution of learning ; or
- by seeking evidence of a tenancy agreement or student accommodation contract.

2.6.1.10.2. Often, an account for a minor will be opened by a family member or guardian. In cases where the adult opening the account does not already have an account with the financial institution, ***the identification evidence for that adult, or of any other person who will operate the account should be obtained in addition to obtaining the birth certificate or passport of the child.*** It should be noted that this type of account could be open to abuse and therefore strict monitoring should be undertaken.

2.6.1.10.3. For accounts opened through a school-related scheme, the school should be asked to provide the date of birth and permanent address of the pupil and to complete the standard account opening documentation on behalf of the pupil.

2.6.2. Quasi Corporate Customers

Trust, Nominees and Fiduciaries.

2.6.2.1.1. Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder. The particular characteristics of Trust that attract the genuine customer, the anonymity and complexity of structures that they can provide are also highly attractive to money launderers.

2.6.2.1.2. Some trusts, nominees and fiduciary accounts present a higher money laundering risk than others. ***Identification and "Know Your Business" procedures need to be set and managed according to the perceived risk.***

2.6.2.1.3. The principal objective of money laundering prevention via trusts, nominees and fiduciaries is to verify the identity of the provider of funds such as the settlor, and those who have control over the funds (the trustees and any controllers who have the power to remove the trustees). ***For discretionary or offshore Trust, the nature and purpose of the Trust and the original source of funding must be ascertained.***

2.6.2.1.4. Whilst reliance can often be placed on other financial institutions that are regulated for money laundering prevention to undertake the checks or confirm identity, the responsibility to ensure that this is undertaken rests with the financial institution. The underlying evidence of identity must be made available to law enforcement agencies in the event of an investigation.

2.6.2.1.5. ***Identification requirements must be obtained and not waived for any trustee who does not have authority to operate an account and cannot give relevant instructions concerning the use or transfer of funds.***

Offshore Trusts.

2.6.2.2.1. Offshore Trusts present a higher money laundering risk and therefore additional measures are needed ***for Special Purpose Vehicles (SPVs) or International Business Companies connected to Trusts, particularly when Trusts are set up in offshore locations with strict bank secrecy or confidentiality rules. Those created in jurisdictions without equivalent money laundering procedures in place should warrant additional enquiries.***

2.6.2.2.2. Unless the applicant for business is itself a regulated financial institution, measures should be taken to identify the Trust company or the corporate service provider in line with the requirements for professional intermediaries or companies generally.

2.6.2.2.3. Certified copies of the documentary evidence of identity for the underlying principals such as settlors, controllers, etc. on whose

behalf the applicant for business is acting, should also be obtained.

2.6.2.2.4. For overseas Trusts, nominee and fiduciary accounts, where the applicant is itself a financial institution that is regulated for money laundering purposes :

· reliance can be placed on an introduction or intermediary certificate letter stating that evidence of identity exists for all underlying principals and confirming that there are no anonymous principals ;

· the trustees/nominees should be asked to state from the outset the capacity in which they are operating or making the application ;

· documentary evidence of the appointment of the current Trustees should also be obtained.

2.6.2.2.5. Where the underlying evidence is not retained within Nigeria, enquiries should be made to determine, as far as practicable, that there are no overriding bank secrecy or confidentiality constraints that will restrict access to the documentary evidence of identity, should it be needed in Nigeria.

2.6.2.2.6. ***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 reports to the NFIU.***

2.6.2.2.7. Where a bank in Nigeria is itself the applicant for an offshore Trust on behalf of a customer, if the corporate Trustees are not regulated, then the Nigerian bank should undertake the due diligence on the Trust itself.

2.6.2.2.8. If the funds have been drawn upon an account that is not under the control of the Trustees, the identity of two of the authorized signatories and their authority to operate the account should also be verified. When the identity of beneficiaries has not previously been verified, verification should be undertaken when payments are made to them.

Conventional Family and Absolute Nigerian Trusts.

2.6.2.3.1. In the case of conventional Nigerian Trusts, identification evidence should be obtained for :

· those who have control over the funds (the principal trustees who may include the settlor) ; and

· the providers of the funds (the settlors, except where they are deceased) ; and

· Where the settlor is deceased, written confirmation should be obtained for the source of funds (grant of probate or copy of the Will or other document creating the Trust).

2.6.2.3.2. Where a corporate Trustee such as a bank acts jointly with a co-Trustee, any non-regulated co-Trustees should be verified even if the corporate Trustee is covered by an exemption. The relevant guidance contained in this Regulation for verifying the identity of persons, institutions or companies should be followed.

2.6.2.3.3. Although a financial institution may not review any existing Trust, confirmation of the settlor and the appointment of any additional Trustees should be obtained.

2.6.2.3.4. Copies of any underlying documentary evidence should be certified as true copies. In addition, a check should be carried out to ensure that any bank account on which the Trustees have drawn funds is in their names. Taking a risk based approach, consideration should be given as to whether the identity of any additional authorized signatories to the bank account should also be verified.

2.6.2.3.5. It is a normal practice for payment of any trust property to be made to all the Trustees. As a matter of practice, some life assurance companies make payments directly to beneficiaries on receiving a request from the Trustees. In such circumstances, ***the payment should be made to the named beneficiary by way of a crossed cheque marked "account payee only" or a bank transfer direct to an account in the name of the beneficiary.***

Receipt and Payment of Funds.

2.6.2.4.1. Where money is received on behalf of a Trust, reasonable steps should be taken to ensure that :

· the source of the funds is properly identified ; and

· the nature of the transaction or instruction is understood.

2.6.2.4.2. It is also important to ensure that payments are properly authorized in writing by the Trustees.

2.6.2.4.3. ***Identification of New Trustees***

Where a Trustee who has been verified is replaced, the identity of the new Trustee should be verified before he/she is allowed to exercise control over the funds.

2.6.2.4.4. ***Life Policies Placed in Trust***

Where a life policy is placed in Trust, the applicant for the policy is also a Trustee and where the Trustees have no beneficial interest in the funds, it should only be necessary ***to verify the identity of the person***

applying for the policy. The remainder of the Trustees would however need to be identified in a situation where policy proceeds were being paid to a third party not identified in the trust deed.

Powers of Attorney and Third Party Mandates.

2.6.2.5.1. The authority to deal with assets under a Power of Attorney and Third Party Mandates constitutes a business relationship. Consequently, at the start of the relationship, ***identification evidence should be obtained from the holders of powers of attorney and third party mandates in addition to the customer*** or subsequently on a later appointment of a new attorney, if advised, particularly within one year of the start of the business relationship. New attorney for corporate or Trust business should always be verified. ***The most important requirement is for financial institution to ascertain the reason for the granting of the power of attorney.***

2.6.2.5.2. Records of all transactions undertaken in accordance with a Power of Attorney should be maintained as part of the client's record.

Executorship Accounts.

2.6.2.6.1. Where a bank account is opened for the purpose of winding up the estate of a deceased person, the identity of ***the executor / administrator of the estate is required to be verified.***

2.6.2.6.2. However, identification evidence would not normally be required for the executors/administrators when payment is being made from an established bank or mortgage institution's account in the deceased's name, solely for the purpose of winding up the estate in accordance with the Grant of Probate or Letter of Administration. Similarly, where a life policy pays out on death, there is normally no need to obtain identification evidence for the legal representatives.

2.6.2.6.3. Payments to the underlying named beneficiaries on the instructions of the executor or administrator may also be made without additional verification requirements. However, if a beneficiary wishes to transact business in his/her own name, then identification evidence will be required.

2.6.2.6.4. ***In the event that suspicions are aroused concerning the nature or origin of assets comprising an estate that is being wound up, then reports of the suspicions are required to be rendered to the NFIU.***

"Client Accounts" Opened By Professional Intermediaries.

2.6.2.7.1. Stockbrokers, fund managers, solicitors, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with financial institutions. Such accounts may be general omnibus accounts holding the funds of many clients or they may be opened specifically for a single client. ***In each case, it is the professional intermediary who is the financial institution's customer.*** These situations should be distinguished from

those where an intermediary introduces a client who himself becomes a customer of the financial institution.

2.6.2.7.2. Where the professional intermediary is itself covered and is indeed monitored by the money laundering regulations and AML/CFT supervisors respectively or their equivalent, identification can be waived on production of evidence.

2.6.2.7.3. However, where the professional intermediary is not regulated under the Money Laundering Regulations or their equivalent, ***the financial institution should not only verify the identity of the professional intermediary but should verify also the identity of the person on whose behalf the professional intermediary is acting.***

2.6.2.7.4. Where it is impossible for a financial institution to establish the identity of the person(s) for whom a solicitor or accountant is acting, it will need to take a commercial decision based on its knowledge of the intermediary, as to the nature and extent of business that they are prepared to conduct if the professional firm is not itself covered by this Regulation. ***Financial institutions, should be prepared to make reasonable enquiries about transactions passing through client-accounts that give cause for concern and should report any transaction where suspicions cannot be satisfied to the NFIU.***

Unincorporated Business/ Partnership.

2.6.2.8.1. Where the applicant is an un-incorporated business or a partnership whose principal partners/controllers do not already have a business relationship with the financial institution, identification evidence should be obtained for the principal beneficial owners/controllers. This would also entail identifying one or more signatories in whom significant control has been vested by the principal beneficial owners/controllers.

2.6.2.8.2. Evidence of the trading address of the business or partnership should be obtained. Where a current account is being opened, a visit to the place of business might also be made to confirm the true nature of the business activities. For established businesses, a copy of the latest report and audited accounts should be obtained.

2.6.2.8.3. The nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained.

Limited Liability Partnership.

2.6.2.9. A limited liability partnership should be treated as corporate customers for verification of identity and Know your customer purposes.

2.6.3. Pure Corporate Customers

General Principles.

2.6.3.1.1. Complex organizations and their structures, other corporate and legal entities are the most likely vehicles for money laundering. Those that are privately owned are being fronted by legitimate trading companies. Care should be taken to verify the legal existence of the applicant-company from official documents or sources and to ensure that persons purporting to act on its behalf are fully authorized. Enquiries should be made to confirm that the legal person is not merely a ***"brass-plate company" where the controlling principals cannot be identified.***

2.6.3.1.2. The identity of a corporate company comprises :

- registration number ;
- registered corporate name and any trading names used ;
- registered address and any separate principal trading addresses ;
- directors ;
- owners and shareholders ; and
- the nature of the company's business.

2.6.3.1.3 The extent of identification measures required to validate this information or the documentary evidence to be obtained depends on the nature of the business or service that the company requires from the financial institution. ***A risk-based approach should be taken.*** In all cases, information as to the nature of the normal business activities that the company expects to undertake with the financial institution should be obtained. Before a business relationship is established, measures should be taken by way of company search at the Corporate Affairs Commission (CAC) and other commercial enquiries undertaken to check that the applicant-company's legal existence has not been or is not in the process of being dissolved, struck off, wound up or terminated.

Non Face-to-Face Business.

2.6.3.2.1. As with the requirements for private individuals, because of the additional risks with non face-to-face business, additional procedures must be undertaken to ensure that the applicant's business, company or society exists at the address provided and it is for a legitimate purpose.

2.6.3.2.2. Where the characteristics of the product or service permit, care should be taken to ensure that relevant evidence is obtained to confirm that any individual representing the company has the necessary authority to do so.

2.6.3.2.3. ***Where the principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for the identification of personal customers should be followed.***

Low Risk Corporate Business.

2.6.3.3.1 ***Public Registered Companies***

2.6.3.3.1.1 Corporate customers that are listed on the stock exchange are considered to be publicly owned and generally accountable. Consequently, there is no need to verify the identity of the individual shareholders.

2.6.3.3.1.2 Similarly, it is not necessary to identify the directors of a quoted company. However, financial institutions are required to make appropriate arrangements ***to ensure that the individual officer or employee (past or present) is not using the name of the company or its relationship with the financial institution for a criminal purpose***. The Board Resolution or other authority for any representative to act on behalf of the company in its dealings with the financial institution should be obtained to confirm that the individual has the authority to act. ***Phone calls can be made to the Chief Executive Officer of such a company to intimate him of the application to open the account before the financial institution.***

2.6.3.3.1.3. No further steps should be taken to verify identity over and above the usual commercial checks where the applicant company is :

- listed on the stock exchange ; or

- there is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company.

2.6.3.3.1.4. ***Due diligence will normally be conducted where the account or service required falls within the category of higher risk business.***

2.6.3.3.2. *Private Companies*

2.6.3.3.2.1. Where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with the financial institution, the following documents should be obtained from an official or recognized independent source to verify the business itself:

(*i*) a copy of the certificate of incorporation/registration, evidence of the company's registered address ***and*** the list of shareholders and directors ;

(*ii*) a search at the Corporate Affairs Commission (CAC) or an enquiry via a business information service to obtain the information in (*i*) above ; **and**

(*iii*) an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC.

2.6.3.3.2.2. Attention should be paid to the place of origin of the documents and the background against which they were produced. If comparable documents cannot be obtained, then verification of principal beneficial owners/controllers should be undertaken.

B 1438

Higher Risk Business.

2.6.3.4.1. ***Bank Accounts for Registered Public Companies***

Where a higher-risk business applicant is seeking to enter into a full banking relationship or any other business relationship where third party funding and transactions are permitted, ***the following evidence must be obtained*** either in documentary or electronic form :

· ***For established companies*** (those incorporated for 18 months or more) a set of the latest report and audited accounts is required to be produced ;

· ***A search report*** at the CAC or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC ;

· ***A certified copy of the resolution of the Board of Directors*** to open an account and confer authority on those who will operate it ; and

· ***The Memorandum and Articles of Association*** of the company.

2.6.3.4.2. ***Higher Risk Business Relating to Private Companies.***

For private companies undertaking higher risk business (in addition to verifying the legal existence of the business) ***the principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets.*** What constitutes significant shareholding or control for this purpose will depend on the nature of the company. ***Identification evidence is required to be obtained for those shareholders with interests of 5% or more.***

2.6.3.4.3. ***The principal control rests with those who are mandated to manage the funds, accounts or investments without requiring authorization and who would be in a position to override internal procedures and control mechanisms.***

2.6.3.4.4 Identification evidence should be obtained for the principal-beneficial owner(s) of the company and any other person with principal control over the company's assets. Where the principal owner is another corporate entity or Trust, the objective is to undertake measures that look behind that company or vehicle and verify the identity of the beneficial-owner(s) or settlors. ***When financial institutions become aware that the principal-beneficial owners/controllers have changed, they are required to ensure that the identities of the new ones are verified.***

2.6.3.4.5. ***Financial institutions are required to also identify directors who are not principal controllers and signatories to an account for risk based approach purpose.***

2.6.3.4.6 In respect of a full banking relationship (irrespective of whether or not the turnover is significant) ***a visit to the place of business must be***

undertaken to confirm the existence of business premises and the nature of the business activities conducted.

2.6.3.4.7. ***If suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a bank or investment account, further checks should be made to ascertain the reason for the changes.***

2.6.3.4.8. For full banking relationships, ***periodic enquiries are required to be made*** to establish whether there have been any changes to controllers, shareholders or to the original nature of the business or activity.

2.6.3.4.9. ***Particular care should be taken to ensure that full identification and "Know Your Customer" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out af a different jurisdiction.***

Foreign Financial Institutions.

2.6.3.5.1 For foreign financial institutions, the confirmation of existence and regulated status should be checked by one of the following means :

- checking with the home country's Central Bank or relevant supervisory body ; or
- ehecking with another office, subsidiary, branch, or correspondent bank in the same country ; or
- checking with Nigerian regulated correspondent bank of the overseas institution ; or
- obtaining evidence of its licence or authorization to conduct financial and banking business from the institution itself .

2.6.3.5.2. Additional information on banks all over the world can be obtained from various international publications and directories or any of the international business information services.

References made to these publications are not meant ta replace the confirmation evidence required above.

Bureaux De Change.

2.6.3.6. Although bureaux de change are subject to the regulations, they must be verified in accordance with the procedures for Other Financial Institutions. ***Satisfactory evidence of identity must include receipt of a certified copy of the applicant's operating licence.***

2.6.3.7 Other Institutions

Clubs and Societies.

2.6.3.7.1 (*a*) In the case of applications made on behalf of clubs or societies, a financial institution is required to take reasonable steps to satisfy itself as to the legitimate purpose of the organization by sighting its constitution. The identity of at least two of the principal contact persons or signatories should be verified initially in line with ***the requirements for***

private individuals. The signing authorities should be structured to ensure that at least ***two of the signatories that authorize any transaction have been verified***. When signatories change, financial institutions are required to ensure that the identity of at least two of the current signatories are verified.

(*b*) Where the purpose of the club or society is to purchase the shares of regulated investment company or where all the members would be regarded as individual clients, all the members in such cases are required to be identified in line with the requirements for personal customers. Financial institutions are required to look at each situation on a case-by-case basis.

2.6.3.7.2. ***Occupational Pension Schemes***

2.6.3.7.2.1 In all transactions undertaken on behalf of an Occupational Pension Scheme where the transaction is not in relation to a long term policy of insurance, the identities of both the Principal Employer and the Trust are required to be verified.

2.6.3.7.2.2 In addition to the identity of the Principal Employer, the source of funding should be verified and recorded to ensure that a complete audit trail exists if the employer is dissolved or wound up.

2.6.3.7.2.3 For the Trustees of Occupational Pension Schemes, satisfactory identification evidence can be based on the inspection of formal documents concerning the Trust which confirm the names of the current Trustees and their addresses for correspondence. In addition to the documents, confirming the trust identification can be based on extracts from Public Registers or references from Professional Advisers or Investment Managers.

2.6.3.7.2.4 Any payment of benefits by or on behalf of the Trustees of an Occupational Pension Scheme will not require verification of identity of the recipient.

2.6.3.7.2.5 Where individual members of an Occupation Pension Scheme are to be given personal investment advice, their identities must be verified. However, where the Trustees and Principal Employer have been satisfactorily identified (and the information is still current) it may be appropriate for the Employer to provide confirmation of the identity of individual employees.

2.6.3.7.3. ***Charities in Nigeria***

(*a*) Adherence to the identification procedures required for money laundering prevention purpose would remove the opportunities for opening unauthorized accounts with false identities on behalf of charities. ***Confirmation of the authority to act in the name of the charity is clearly mandatory.***

(*b*) ***The practice of opening unauthorized accounts of this type under sole control is strongly discouraged. For emphasis, accounts for Charities in Nigeria are required to be operated by a minimum of two signatories, duly verified and documentation evidence obtained.***

2.6.3.7.4. ***Registered Charities***

(*a*) When dealing with an application from a registered charity, the financial institution is required to obtain and confirm the name and address of the charity concerned.

(*b*) To guard against the laundering of fraudulently obtained funds (where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate) a financial institution is required to send a letter to the official correspondent, informing him of the Charity's application before it. The official correspondent should be requested to respond as a matter of urgency especially where there is any reason to suggest that the application has been made without authority.

(*c*) ***Where a charity is opening a current account, the identity of all signatories should be verified initially and when the signatories change, care should be taken to ensure that the identity of any new signatory is verified.***

(*d*) Applications on behalf of un-registered charities should be dealt with in accordance with procedures for clubs and societies set out in ***item 2.6.3.7.1 of this Regulation.***

2.6.3.7.5. ***Religious Organizations (ROs)***

A religious organization is expected by law to be registered by the Corporate Affairs Commission (CAC) and will therefore have a registered number. Its identity can be verified by reference to the CAC, appropriate headquarters or regional area of the denomination. ***As a registered organization, the identity of at least two signatories to its account must be verified.***

Three - Tiers of Government/ Parastatals.

2.6.3.8. Where the applicant for business is any of the above, the financial institution is required to verify the legal standing of the applicant, including its principal ownership and the address. A certified copy of the Resolution or other documents authorizing the opening of the account or to undertake the transaction should be obtained in addition to evidence that the official representing the body has the relevant authority to act. ***Telephone contacts must also be made with the Chief Executive Officer of the organization/parastatals concerned, intimating him of the application to open the account in the financial institution.***

Appropriate authorization from Federal/State Accountant General is a pre-requisite for any of the three tiers of government/parastatals to open accounts with financial institutions in Nigeria.

Foreign Consulates.

2.6.3.9. The authenticity of applicants that request to open accounts or undertake transactions in the name of Nigerian-resident foreign consulates and any documents of authorization presented in support of the application should he checked with the Ministry of Foreign Affairs or the relevant authorities in the Consulate's home country.

2.7. INTERMEDIARIES OR OTHER THIRD PARTIES TO VERIFY IDENTITY OR TO INTRODUCE BUSINESS

Who to rely upon and the circumstances.

2.7.1. Whilst the responsibility to obtain satisfactory identification evidence rests with the financial institution that is entering into the relationship with a client, it is reasonable, in a number of circumstances, for reliance to be placed on another financial institution to :

· undertake the identification procedure when introducing a cnstomer and to obtain any additional KYC information from the client ; or

· confirm the identification details if the customer is not resident in Nigeria ; or

· confirm that the verification of identity has been carried out (if an agent is acting for underlying principals).

Introductions from Authorized Financial Intermediaries.

2.7.2. Where an intermediary introduces a customer and then withdraws from the ensuing relationship altogether, then the underlying customer has become the applicant for the business. He ***must, therefore, be identified in line with the requirements for personal, corporate or business customers as appropriate.*** An introduction letter should therefore be issued by the introducing financial institution or person in respect of each applicant for business. To ensure that product-providers meet their obligations, that satisfactory identification evidence has been obtained and will be retained for the necessary statutory period, each introduction letter must either be accompanied by certified copies of the identification evidence that has been obtained iu line with the usual practice of certification of identification documents or by sufficient details/reference numbers, etc that will permit the actual evidence obtained to be re-obtained at a later stage.

Written Applications.

2.7.3.1 For a written application (unless other arrangements have been agreed that the service provider will verify the identity itself) a financial intermediary must provide along with each application, the customer's introduction letter together with certified copies of the evidence of ideutity which should be placed in the customer's file.

2.7.3.2 If these procedures are followed, the product provider, stockbroker or investment banker will be considered to have fulfilled its own identification obligations. However, if the letter is not forthcoming from the intermediary, or the letter indicates that the intermediary has not verified the identity of the applicant, the service provider is required to

satisfy its obligation by applying its own direct identification procedures.

Non-Written Application.

2.7.4. Unit Trust Managers and other product providers receiving non-written applications from financial intermediaries (where a deal is placed over the telephone or by other electronic means) have an obligation to verify the identity of customers and ensure that the intermediary provides specific confirmation that identity has been verified. ***A record must be made of the answers given by the intermediary and retained for a minimum period of five years. These answers constitute sufficient evidence of identity in the hands of the service provider.***

Introductions from Foreign Intermediaries.

2.7.5. Where introduced business is received from a regulated financial intermediary who is outside Nigeria, the reliance that can be placed on that intermediary to undertake the verification of identity-check must be assessed by the MLCO or some other competent persons within the financial institution on a case by case basis based on the knowledge of the intermediary.

Corporate Group Introductions.

2.7.6.1 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that :

· the identity of the customer has been verified by the introducing parent company, branch, subsidiary or associate in line with the money laundering requirements of equivalent standards and taking account of any specific requirements such as separate address verification ;

· no exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship ;

· a group introduction letter is obtained and placed with the customer's account opening records ; and

· in respect of group introducers from outside Nigeria, arrangements should be put in place to ensure that identity is verified in accordance with requirements and that the underlying records of identity in respect of introduced customers are retained for the necessary period.

2.7.6.2 Where financial institutions have day-to-day access to ***all the Group's "Know Your Customer" information and records***, there is no need to identify an introduced customer or obtain a group introduction letter ***if the identity of that customer has been verified previously***. However, if the identity of the customer has not previously been verified, then any missing identification evidence will need to be obtained and a risk-based approach taken on the extent of KYC information that is available on whether or not additional information should be obtained.

2.7.6.3 Financial institutions are required to ensure that there is no secrecy or data protection legislation that would restrict free access to the

records on request or by law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that sueh restrictions apply, copies of the underlying records of identity should, wherever possible, be sought and retained.

2.7.6.4 Where identification records are held outside Nigeria, it is still the responsibility of the financial institution to ensure that the records available do, in fact, meet the requirements in this Regulation.

Business Conducted by Agents.

2.7.7.1 Where an applicant is dealing in its own name as agent for its own client, a financial institution must, in addition to verifying the agent, establish the identity of the underlying client.

2.7.7.2 A financial institution may regard evidence as sufficient if it has established that the client :

· is bound by and has observed this Regulation or the provisions of the Money Laundering (Prohibition) Act, 2004 ; and

· is acting on behalf of another person and has given a written assurance that he has obtained and recorded evidence of the identity of the person on whose behalf he is acting.

2.7.7.3. Consequently, where another financial institution deals with its own client (regardless of whether or not the underlying client is disclosed to the financial institution) then :

· ***where the agent is a financial institution,*** there is no requirement to establish the identity of the underlying clients or to obtain any form of written confirmation from the agent concerning the due diligence undertaken on its underlying clients; or

· ***where a regulated agent from outside Nigeria deals through a customer omnibus account or for a named customer through a designated account,*** the agent should provide a written assurance that the identity of all the underlying clients has been verified in accordance with their local requirements.

Where such an assurance cannot be obtained, then the business should not be undertaken.

2.7.7.4. ***In circumstances where an agent is either unregulated or is not covered by the relevant money laundering legislation,*** then each case should be treated on its own merits. The knowledge of the agent will inform the type of the due diligence standards to apply. Risk-based approach must also be observed by the financial institution.

Syndicated Lending,

2.7.8. For syndicated lending arrangements, the verification of identity and any additional KYC requirements rest with the lead-manager or agent required to supply the normal confirmation letters.

Correspondent Relationship.

2.7.9.1 Transactions conducted through correspondent relationships need to be managed, taking a risk-based approach. ***"Know Your Correspondent" procedures are required to be established to ascertain whether or not the correspondent bank or the counter-party is itself regulated for money laundering prevention.*** If regulated, the correspondent is required to verify the identity of its customers in accordance with FATF-standards. Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and know your customer procedures.

2.7.9.2. ***The volume and nature of transactions flowing through correspondent accounts with financial institutions from high risk jurisdictions or those with inadequacies or material deficiencies should be monitored against expected levels and destinations and any material variances should be checked.***

2.7.9.3. ***Financial institutions are required to maintain records of having ensured that sufficient due diligence has been undertaken by the remitting bank on the underlying client and the origin of the funds in respect of the funds passed through their accounts.***

2.7.9.4. ***Financial institutions are required to also guard against establishing correspondent relationships with high risk foreign banks (e.g. shell banks) or with correspondent banks that permit their accounts to be used by such banks.***

2.7.9.5. ***Staff dealing with correspondent banking accounts are required to be trained to recognize higher risk circumstances*** and be prepared to challenge the correspondents over irregular activity (whether isolated transactions or trends) and to submit a suspicious activity report to the NFIU.

2.7.9.6. ***Financial institutions are required to terminate their accounts with correspondent banks that fail to provide satisfactory answers to reasonable questions including confirming the identity of customers involved in unusual or suspicious circumstances.***

Acquisition of One Financial Institution/ Business by Another.

2.7.10.1 When one financial institution acquires the business and accounts of another financial institution, it is not necessary for the identity of all the existing customers to be re-identified, provided that all the underlying customers' records are acquired with the business. ***It is, however, important to carry out due diligence enquiries to confirm that the acquired institution had conformed with the requirements in this Regulation.***

2.7.10.2 Verification of identity should be undertaken as soon as it is practicable for all the transferred customers who were not verified by the transferor in line with the requirements for existing customers that open new accounts, where :

· the money laundering procedures previously undertaken have not been in accordance with the requirements of this Regulation ;

· the procedures cannot be checked ; or

· where the customer-records are not available to the acquiring financial institution.

2.8. RECEIVING FINANCIAL INSTITUTIONS AND AGENTS

Vulnerability of Receiving Bankers and Agents.

2.8.1. Receiving financial institutions may be used by money launderers in respect of offers for sale where new issues are over-subscribed and their allocation is scaled down. In addition, the money launderer is not concerned if there is a cost involved in laundering criminal money. New issues that trade at a discount will, therefore, still prove acceptable to the money launderer. Criminal funds can be laundered by way of the true beneficial-owner of the funds providing the payment for an application in another person's name, specifically to avoid the verification process and to break the audit trail with the underlying crime from which the funds are derived.

Who should be identified?

2.8.2.1. Receiving financial institutions should obtain satisfactory identification evidence of new applicants, including such applicants in a rights issue where the value of a single transaction or a series of linked transactions is $1,000 or its equivalent for individuals and ₦500,0000 for corporate body or more.

2.8.2.2 If funds to be invested are being supplied by or on behalf of a third party, it is important that the identification evidence for both the applicant and the provider of the funds are obtained to ensure that the audit trail for the funds is preserved.

Applications Received via Brokers.

2.8.3.1 Where the application is submitted (payment made) by a broker or an intermediary acting as agent, no steps need be taken to verify the identity of the underlying applicants. However, the following standard procedures apply :

· The lodging agent's stamp should be affixed on the application form or allotment letter ; and

· Application/acceptance forms and cover letters submitted by lodging agents should be identified and recorded in the bank's records.

2.8.3.2. The terms and conditions of the issue should state that ***any requirements to obtain identification evidence are the responsibility of the broker lodging the application and not the receiving financial institution.***

2.8.3.3. Where the original application has been submitted by a regulated broker, no additional identification evidence will be necessary for subsequent calls in respect of shares issued and partly paid.

Applications Received from Foreign Brokers.

2.8.4. If the broker or other introducer is a regulated person or institution (including an overseas branch or subsidiary) from a country with equivalent legislation and financial sector procedures, and the broker or introducer is subject to anti-money laundering rules or regulations, then a written assurance can be taken from the broker that he/she has obtained and recorded evidence of identity of any principal and underlying beneficial owner that is introduced.

Multiple Family Applications.

2.8.5.1 Where multiple family applications are received supported by one cheque and the aggregate subscription price is US $1,000 USD or more; and $1,000 USD or more for an individual person, then identification evidence will not be required for :

- a spouse or any other person whose surname and address are the same as those of the applicant who has signed the cheque ;
- a joint account holder ; or
- an application in the name of a child where the relevant company's Articles of Association prohibit the registration in the names of minors and the shares are to be registered with the name of the family member of full age on whose account the cheque is drawn and who has signed the application form.

2.8.5.2 However, identification evidence of the signatory of the financial instrument will be required for any multiple family application for more than $1,000 or its equivalent; or more than ₦250, 000 for an individual; or more than ₦500, 000 for a body corporate where such is supported by a cheque signed by someone whose name differs from that of the applicant. Other monetary amounts or more may, from time to time, be stipulated by any applicable money laundering legislation/guidelines.

2.8.5.3 Where an application is supported by a financial institution's branch cheque or brokers' draft, the applicant should state the name and account number from which the funds were drawn:

- on the front of the cheque ; or
- on the back of the cheque together with a branch stamp ; or
- providing other supporting documents.

Linked Transactions.

2.8.6.1 If it appears to a person handling applications that a number of single applications under $1,000 or its equivalent and N500,000 in different names are linked (e.g. payments from the same financial institution account) apart from the multiple family applications above, identification evidence must be obtained in respect of parties involved in each single transaction.

2.8.6.2 Installment payment issues should be treated as linked transactions where it is known that total payments will amount to $1,000 USD or its equivalent for an individual; or ₦500,0000 for body corporate

or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or guidelines. Either at the outset or when a particular point has been reached, identification evidence must be obtained.

2.8.6.3 Applications that are believed to be linked and money laundering is suspeeted are required to be processed on a separate batch for investigation after allotment and registration have been completed. Returns with the documentary evidence are to be rendered to the NFIU accordingly. ***Copies of the supporting cheques, application forms and any repayment-cheques must be retained to provide an audit trail until the receiving financial institution is informed by CBN, NFIU or the investigating officer that the records are of no further interest.***

Domiciliary Account (DA).

2.8.7. Where a customer wishes to open a DA or make a wholesale deposit by means of cash or inter-bank transfer, the financial institution is required to obtain identification evidence in accordance with the requirements for private individuals, companies or professional intermediaries operating on behalf of third parties as appropriate. It should satisfy itself that the transferring institution is regulated for money laundering prevention in its country of origin.

Safe Custody and Safety Deposit Boxes.

Precautions should be taken in relation to requests to hold boxes, parcels and sealed envelopes in a safe custody. Where such facilities are made available to non-account holders, the ***identification procedures set out in this Regulation must be followed, depending on the type of individual involved.***

2.9. EXEMPTION FROM IDENTIFICATION PROCEDURES

Where a customer's identity was not properly obtained as contained in this Regulation and Requirements for Account Opening Procedure, financial institutions are required to re-establish the customer's identity in line with the contents of this Regulation, except where it concerns:

Nigerian Fiuancial Institutions.

2.9.1. Identification evidence is not required where the applicant for business is a Nigerian ***financial institution or*** person covered and regulated by the requirements of this Regulation.

One-off Cash Transaction (Remittances, Wire Transfers, etc.)

2.9.2. Cash remittances and wire transfers (either inward or outward) or other monetary instruments that are undertaken against payment in cash for customers who do not have an account or other established relationship with the financial institution (i.e. walk in customers) present a high risk for money laundering purposes. It is therefore required that adequate procedures are established to record the transaction and relevant identification evidence taken, where necessary. Where such transactions form a regular part of the financial institution's business, the limits for requiring identification evidence of US $ 1,000 USD or its equivalent for foreign transfers must, however, be observed.

Re-investment of Income.

2.9.3. The proceeds of a one-off transaction due can be paid to a customer or be further re-invested where records of his identification requirements were obtained and kept. In the absence of this his/her identification requirements must be obtained before the proceeds are paid to him or be re-invested on his behalf in accordance with the relevant provision of this Regulation.

2.10. SANCTIONS FOR NON-COMPLIANCE WITH KYC

Failure to comply with the provisions contained in this Regulation will attract appropriate sanction in accordance with existing laws and as detailed in the AML/CFT section of this Regulation.

APPENDIX A:

INFORMATION TO ESTABLISH IDENTITY

Natural Persons.

A. For natural persons the following information should be obtained, where applicable :

· Legal name and any other names used (such as maiden name) ;

· Correct permanent address (full address should be obtained and a Post Office box number is not sufficient) ;

· Telephone number, fax number, and e-mail address ;

· Date and place of birth ;

· Nationality ;

· Occupation, public position held and name of employer ;

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

· Type of account and nature of the banking relationship ; and

· Signature.

The financial institution should verify this information by at least one of the following methods :

· Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records) ;

· Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority) ;

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

· Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public).

The examples quoted above are not the only possibilities. There may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.

Financial institutions are required to apply equally effective customer

identification procedures for non-face-to-face customers as for those available for interview.

From the information provided, financial institutions should be able to make an initial assessment of a customer's risk profile. Particular attention needs to be focused on those customers identified as having a higher risk profile. Additional inquiries made or information obtained in respect of those customers should include the following :

- Evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits ;
- Personal reference (i.e. by an existing customer of the same institution) ;
- Prior bank reference and contact with the bank regarding the customer ;
- Source of wealth ;
- Verification of employment, public position held (where appropriate).

The customer acceptance policy should not be so restrictive to amount to a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged (see details in AML/CFT Regulation).

Institutions.

B. The term institution includes any entity that is not a natural person. In considering the customer identification guidance for the different types of institutions, particular attention should be given to the different levels of risk involved.

(*i*) *Corporate Entities*

For corporate entities (i.e. corporations and partnerships), the following information should be obtained :

- Name of institution;
- Principal place of institution's business operations;
- Mailing address of institution;
- Contact telephone and fax numbers;
- Some form of official identification number, if available (e.g. Tax identification number);
- The original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;
- The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
- Nature and purpose of business and its legitimacy.

The financial institution should verify this information 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 :
- Utilising an independent information verification process, such as accessing public and private databases ;
- Obtaining prior bank references ;
- Visiting the corporate entity ; and
- Contacting the corporate entity by telephone, mail or e-mail.

The financial institution should also take reasonable steps to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

(*ii*) *Corporation/Partnership*

For corporations/partnerships, the principal guidance is to look behind the institution to identify those who have control over the business and the company's/partnership's assets, including those who have ultimate control.

For corporations, particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals.

What constitutes control for this purpose will depend on the nature of a company, and may rest in those who are mandated to manage the funds, accounts or investments without requiring further authorisation, and who would be in a position to override internal procedures and control mechanisms.

For partnerships, each partner should be identified and it is also important to identify immediate family members that have ownership control.

Where a company is listed on a recognised stock exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration should be given to whether there is effective control of a listed company by an individual, small

group of individuals or another corporate entity or trnst. If this is the case then those controllers should also be considered to be principals and identified accordingly.

Other Types of Institution.

C. The following information should be obtained in addition to that required to verify the identity of the principals in respect of Retirement Benefit Programmes, Mutuals/Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, Trusts and Foundations and Professional Intermediaries :

- Name of account ;
- Mailing address ;
- Contact telephone and fax numbers ;
- Some form of official identification number, such as tax identification number ;
- Description of the purpose/activities of the account holder as stated in a formal constitution ; and
- Copy of documentation confirming the legal existence of the account holder such as register of charities.

The financial institution should verify this information by at least one of the following :

- Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted ;
- Obtaining prior bank references ; and
- Accessing public and private databases or official sources.

(*i*) *Retirement Benefit Programme*

Where an occupational pension programme, employee benefit trust or share option plan is an applicant for an account the trustee and any other person who has control over the relationship such as the administrator, programme manager, and account signatories should be considered as principals and the financial institution should take steps to verify their identities.

(*ii*) *Mutual/Friendly, Cooperative and Provident Societies*

Where these entities are an applicant for an account, the principals to be identified should be considered to be those persons exercising control or significant influence over the organisation's assets. This often includes board members, executives and account signatories.

(iii) Charities, Clubs and Associations

In the case of accounts to be opened for charities, clubs, and societies, the financial institution should take reasonable steps to identify and verify at least two signatories along with the institution itself. The principals who should be identified should be considered to be those persons exercising control or significant influence over the organisation's assets. This includes members of the governing body or committee, the President, board members, the treasurer, and all signatories.

In all cases, independent verification should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

(iv) Trusts and Foundations

When opening an account for a Trust, the financial institution should take reasonable steps to verify the trustee, the settlor of the trust (including any persons settling assets into the trust) any protector, beneficiary and signatories: Beneficiaries should be identified when they are defined. In the case of a foundation, steps should be taken to verify the founder, the managers/ directors and the beneficiaries.

(v) Professional Intermediaries

When a professional intermediary opens a client account on behalf of a single client that client must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities. Where funds held by the intermediary are not co-mingled but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the financial institution should look through to the beneficial-owners. However, there may be circumstances that the financial institution may not look beyond the intermediary (e.g. when the intermediary is subject to the same due diligence standards in respect of its client base as the financial institution).

Where such circumstances apply and an account is opened for an open or closed ended investment company (unit trust or limited partnership) also subject to the same due diligence standards in respect of its client base as the financial institution, the following should be considered as principals and the financial institution should take steps to identify them :

- The fund itself ;
- Its directors or any controlling board, where it is a company ;
- Its Trustee, where it is a Unit Trust ;
- Its managing (general) partner, where it is a limited partnership ;

· Account signatories ;

· Any other person who has control over the relationship such as fund administrator or manager.

Where other investment vehicles are involved, the same steps should be taken as in above (where it is appropriate to do so). In addition, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control over the funds.

Intermediaries should be treated as individual customers of the financial institution and the standing of the intermediary should be separately verified by obtaining the appropriate information itemised above.

APPENDIX B

DEFINITION OF TERMS

For the proper understanding of this Regulation, certain terms used within are defined as follows :

Terms	*Definition*
Applicant for Business	The person or company seeking to establish a 'business relationship' or an occasional customer undertaking a 'one-off' transaction whose identity must be verified.
Batch transfer	A batch transfer is a transfer comprising a number of individual wire transfers that are being sent to the same financial institutions, but may/ may not be ultimately intended for different persons.
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/ or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Beneficiary	Beneficiary owner refers to those natural persons, or groups of natural persons who receive charitable, humanitarian or other types of assistance through the services of the NPO. They include all trusts (other than charitable or statutory permitted non-charitable trusts) must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years.
Business Relationship	'Business relationship' is any arrangement between the financial institution and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.

Cross-bordertransfer

Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdietions. This term also refers to any chain of wire transfers that has at least one cross-border element.

Designated categories of offences

Designated categories of offences means :

- participation in an organised criminal group and racketeering ;
- terrorism, including terrorist financing ;
- trafficking in human beings and migrant smuggling ;
- sexual exploitation, including sexual exploitation of children ;
- illicit trafficking in narcotic drugs and psychotropic substances :
- illicit arms trafficking ;
- illicit trafficking in stolen and other goods ;
- corruption and bribery ;
- fraud ;
- counterfeiting currency ;
- counterfeiting and piracy of products :
- environmental crime ;
- murder, grievous bodily injury ;
- kidnapping, illegal restraint and hostage-taking ;
- robbery or theft ;
- smuggling ;
- extortion ;
- forgery ;
- piracy ; and
- insider trading and market manipulation.

Designated non-financial businesses and professions

Designated non-financial businesses and professions mean :

(*a*) Casinos (which also includes internet casinos).

(*b*) Real estate agents.

(*c*) Dealers in precious metals.

(*d*) Dealers in precious stones.

(*e*) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals

that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

(*f*) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under this Regulation, and which as a business, provide any of the following services to third parties :

- ☐ acting as a formation agent of legal persons ;
- ☐ acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons ;
- ☐ providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement ;
- ☐ acting as (or arranging for another person to act as) a trustee of an express trust ;
- ☐ acting as (or arranging for another person to act as) a nominee shareholder for another person.

Domestic transfer

Domestic transfer means any wire transfer where the originator and beneficiary institutions are both located in Nigeria. This term therefore refers to any chain of wire transfers that takes place entirely within Nigeria's borders, even though the system used to effect the wire transfer may be located in another jurisdiction.

False declaration

False declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

False disclosure

False disclosure refers to a misrepresentation of the valne of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required

The FATF Recommendations

The FATF Recommendations refers to the Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.

Financial institutions

Financial institution means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer :

1. Acceptance of deposits and other repayable funds from the public.
2. Lending.
3. Financial leasing.
4. The transfer of money or valne.
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in :

(*a*) money market instruments (cheques, bills, CDs, derivatives etc.) ;
(*b*) foreign exchange ;
(*c*) exchange, interest rate and index instruments ;
(*d*) transferable securities ;
(*e*) commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on beha'f of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life iusurance and other investment related insurance.

	13. Money and currency changing. The list is not exhaustive but subject to the definition contained in BOFIA 2004.
Funds Transfer	The term funds transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
Legal arrangement	Legal arrangement refers to express trusts or other similar legal arrangements.
Legal persons	Legal persons refer to bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.
Non-profit Organizations/ Non-governmental Organizations	The term non-profit organization/non-governmental organization refers to a legal entity or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works.
Originator	The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.
One-off Transaction	A 'one-off transaction' means any transaction carried out other than in the course of an established business relationship. It is important to determine whether an applicant for business is undertaking a one-off transaction or whether the transaction is or will be a part of a business relationship as this can affect the identification requirements.
Payable through account	Payable through account refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Proceeds	Proceeds refer to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Risk	All references to risk in this Regulation refer to the risk of money laundering and/or terrorist financing.
Settlor	Settlors are persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trusts assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.
Shell bank	Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a conntry. The existence simply of a local agent or low level staff does not constitute physical presence.
Terrorist	It refers to any natural person who : (*i*) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully ; (*ii*) participates as an accomplice in terrorist acts ; (*iii*) organises or directs others to commit terrorist acts ; or (*iv*) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Terrorist act	A terrorist act includes but are not limited to : (*i*) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997) ; and (*ii*) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist financing	Terrorist financing (FT) includes the financing of terrorist acts, and of terrorists and terrorist organizations.
Terrorist financing offence	A terrorist financing (FT) offence refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organization	Refers to any group of terrorists that : (*i*) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully ; (*ii*) participates as an accomplice in terrorist acts ; (*iii*) organises or directs others

to commit terrorist acts ; or (*iv*) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Those who finance Terrorism

Those who finance terrorism refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to he used, in full or in part, in order to carry out terrorist acts.

Trustee

Trustees, include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets. They invest and dispose of them in accordance with the settlor's trust deed, taking account of any letter of wishes. There may also be a protector who may have power to veto the trustees' proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

Unique identifier

A unique identifier refers to any unique combination of letters, numbers or symbols that refer to a specific originator.

Wire transfer

The term wire transfer refers to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.

APPENDIX C:

MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS"

Introduction.

1. Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Financial institutions are, therefore, required to put in place effective and efficient transaction monitoring programmes to facilitate the process.

Althongh the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic featnres which tend to give reasonable cause for suspicion of money laundering.

This appendix, which lists various transactions and activities that indicate potential money laundering, is not exhaustive. It does reflect the ways in which money launderers have been known to operate.

Transactions or activities highlighted in this list are not necessarily indicative of actual money laundering if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here should put financial institutions on enquiry and provoke further investigation to determine their true legal status.

Suspicious Transactions "Red Flags"

2.—(*i*) *Potential Transactions Perceived or Identified as Suspicious*

• Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.

• Transactions involving sbell companies.

• Transactions with correspondents that have been identified as higher risk.

• Large transaction activity involving monetary instruments such as traveller's cheques, bank drafts, money order, particularly those that are serially numbered.

• Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test an institution's own internal monitoring threshold or controls.

(*ii*) *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 cash deposits made by an 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 deposit cash through many deposit slips such that the amount of each deposit is relatively small, the overall total is quite significant.

• Customers whose deposits contain forged currency notes or instruments.

• Customers 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 usually 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.

(iii) 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 a 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.

• Customers 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 customers' legitimate business needs.

• Sudden and unexpected increase in account activity or balance arising from deposit of cash and 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 certificates 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 deposit or other investments by multiple cheques, each below the stipulated reporting threshold.

• Retail businesses 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 individuals, 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 client 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 a money changer that receives deposits.

• An account operated in the name of an off-shore company with structured movement of funds.

(*iv*) *Trade-Based Money Laundering*

• Over and under-invoicing of goods.

• Multiple invoicing of goods and services.

• Over and under-invoicing of goods and services.

• Falsely described goods and services and "phantom" shipments whereby the exporter does not ship any goods at all after payments had 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 economic rationale.

• Customer requests payment of proceeds to an unrelated third party.

• Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

(*v*) *Lending Activity*

• 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 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 the borrower).

(vi) 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 seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).

• Financial transaction by a nonprofit or charitable organisation, 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 organisation 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 no logical business or other economic purpose for the transfers, particularly when this activity involves designated 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 organisations 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.

(vii) Other Unusual or Suspicious Activities

• Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.

• Employee fails to comply with approved operating guidelines, particularly in private banking.

• Employee is reluctant to take a vacation.

• Safe deposit boxes or safe custody accounts opened by individuals who do not reside or 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 purposes.

• Official Embassy business is conducted through personal accounts.

• Embassy accounts are funded through substantial currency transactions.

• Embassy accounts directly fund personal expenses of foreign nationals.

MADE at Abuja this 23rd day of December, 2009.

SANUSI LAMIDO SANUSI
Governor, Central Bank of Nigeria