

*Extraordinary*



# Federal Republic of Nigeria

## Official Gazette

---

No. 65

Lagos - 3rd September, 2013

Vol. 100

---

*Government Notice No. 161*

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

<i>S.I. No.</i>	<i>Short Title</i>	<i>Page</i>
16	Central Bank of Nigeria (Anti-money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulations, 2013 .. .. .	B 227 - B 307

---

Printed and Published by The Federal Government Printer, Lagos, Nigeria  
FGP 98/92013/3,200 (OL 71)

Annual Subscription from 1st January, 2013 is Local : ₦25,500.00 Overseas : ₦37,500.00 [Surface Mail] - ₦49,500.00 [Second Class Air Mail]. Present issue ₦2,500.00 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

**CENTRAL BANK OF NIGERIA (ANTI-MONEY LAUNDERING AND  
COMBATING THE FINANCING OF TERRORISM IN BANKS AND OTHER  
FINANCIAL INSTITUTIONS IN NIGERIA) REGULATIONS, 2013**



ARRANGEMENT OF REGULATIONS

*Regulation :*

PART I—OBJECTIVES, SCOPE AND APPLICATIONS

1. Objective
2. Scope
3. Application

PART II—ANTI-MONEY LAUNDERING AND COMBATING  
THE FINANCING OF TERRORISM DIRECTIVES

4. AML/CFT Institutional Policy Framework
5. Risk Assessment
6. Risk Mitigation
7. Designation and Duties of AML/CFT Compliance Officer
8. Co-operation with Competent Authorities

PART III—OFFENCES, MEASURES AND SANCTIONS

9. Scope of Offences
10. Terrorism Financing Offences
11. Targeted Financial Sanctions Related to Terrorism Financing and Proliferation
12. Limitation of Secrecy and Confidentiality Laws

PART IV—CUSTOMER DUE DILIGENCE, HIGHER RISK CUSTOMERS  
AND ACTIVITIES OF POLITICALLY EXPOSED PERSONS

13. Customer Due Diligence (“CDD”) Measures
14. Identification and Verification of Customers
15. Verification of Beneficial Ownership
16. Application of Enhanced Due Diligence to Higher Risk Customers and Activities
17. Attention to High Risk Countries

18. Politically Exposed Person (PEP)
19. Cross-Border and Correspondent Banking
20. New Technologies and Non face-to-face Transactions
21. Money or Value Transfer (MVT) Services
22. Foreign Branches and Subsidiaries
23. Wire Transfers
24. Simplified Due Diligence Applicable to Lower Risk Customers, Transactions or Products
25. Timing of Verification
26. Existing Customers
27. Failure to Complete CDD
28. Reliance on Intermediaries and Third Parties on CDD Function

PART V—MAINTENANCE OF RECORDS

29. Maintenance of Records on Transactions
30. Attention on Complex and Unusual Large Transactions
31. Suspicious Transaction Monitoring
32. Procedure for the Monitoring and Reporting of Suspicious Transactions

PART VI—MONITORING, INTERNAL CONTROLS, PROHIBITIONS AND SANCTIONS

33. Internal Controls, Compliance and Audit
34. Sanctions and Penalties for Non-Compliance
35. Prohibition of Numbered or Anonymous Accounts, Accounts in Fictitious Names and Shell Banks
36. Other Forms of Reporting
37. AML/CFT Employee-Education and Training Programme
38. Monitoring of Employee Conduct
39. Protection of Staff who Report Violations
40. Additional Areas of AML/CFT Risks
41. Additional Procedures and Mitigants.
42. Testing for the Adequacy of the AML/CFT Compliance
43. Formal Board Approval of the AML/CFT Compliance
44. Culture of Compliance

PART VII—GUIDANCE ON KNOW YOUR CUSTOMER (KYC)

45. Three Tiered KYC Requirements
46. Duty to Obtain Identification Evidence

47. Nature and Level of the Business
48. Application of Commercial Judgment
49. Identification
50. Factors to Consider in Identification
51. Time for Verification of Identity
52. Verification of Identity
53. Exceptions
54. Additional Verification Requirements
55. Identification of Directors and other Signatories
56. Joint Account Holders
57. Verification of Identity for High Risk Business
58. Duty to Keep Watch of Significant Changes in Nature of Business
59. Verification of Identity of Person Providing Funds for Trust
60. Savings Schemes and Investments in Third Parties' Names
61. Personal Pension Schemes
62. Timing of Identification Requirements
63. Consequence of Failure to Provide Satisfactory Identification Evidence
64. Identification Procedures
65. New Business for Existing Customers
66. Certification of Identification Documents
67. Recording Identification Evidence
68. Concession in Respect of Payment Made by Post
69. Term Deposit Account ('TDA')
70. Investment Funds

#### PART VIII—GENERAL INFORMATION

71. Establishing Identity
72. Private Individuals — General Information
73. Private Individuals Resident in Nigeria
74. Documenting Evidence of Identity
75. Physical Checks on Private Individuals Resident in Nigeria
76. Electronic Checks

#### PART IX—FINANCIAL EXCLUSION FOR THE SOCIALLY OR FINANCIALLY DISADVANTAGED APPLICANTS

77. "*Financial Exclusion*" for the Socially or Financially Disadvantaged Applicants Resident in Nigeria

- 78. Private Individuals not Resident in Nigeria
- 79. Non face- to-face Identification
- 80. Refugees or Asylum Seekers
- 81. Students and Minors
- 82. Quasi Corporate Customers

PART X—TRUST, POLICY, RECEIPT AND PAYMENT OF FUNDS

- 83. Trust, Nominees and Fiduciaries
- 84. Off-shore Trusts
- 85. Conventional Family and Absolute Nigerian Trusts
- 86. Receipt and Payment of Funds
- 87. Identification of new Trustees
- 88. Life Policies Placed in Trust
- 89. Powers of Attorney and Third Party Mandates

PART XI—EXECUTORSHIP, CLIENT ACCOUNTS, UN-INCORPORATED AND CORPORATED ORGANIZATIONS

- 90. Executorship Accounts
- 91. "Client Accounts" Opened By Professional Intermediaries
- 92. Un-incorporated Business or Partnership
- 93. Limited Liability Partnership
- 94. Pure Corporate Customers
- 95. The Identity of a Corporate Company
- 96. Non face-to-face Business
- 97. Public Registered Companies
- 98. Private Companies
- 99. Higher Risk Business Applicant
- 100. Higher Risk Business Relating to Private Companies
- 101. Foreign Financial Institutions
- 102. Bureau De Change
- 103. Designated Non-Financial Businesses and Professions (DNFBPs)
- 104. Occupational Pension Schemes
- 105. Registered Charity Organizations
- 106. Religious Organizations (ROs)
- 107. Three - Tiers of Government and Parastatals
- 108. Foreign Consulates

109. Intermediaries or other Third Parties to Verify Identity or to Introduce Business

PART XII—INTRODUCTIONS, APPLICATIONS AND  
FOREIGN INTERMEDIARIES

110. Introductions from Authorized Financial Intermediaries  
111. Written Applications  
112. Non-Written Application  
113. Foreign Intermediaries  
114. Corporate Group Introductions  
115. Business Conducted by Agents  
116. Syndicated Lending  
117. Correspondent Relationship  
118. Acquisition of One Financial Institution and Business by Another  
119. Vulnerability of Receiving Bankers and Agents  
120. Categories of Persons to be Identified  
121. Applications Received through Brokers  
122. Applications Received from Foreign Brokers  
123. Multiple Family Applications

PART XIII—LINKED TRANSACTIONS, FOREIGN ACCOUNTS AND  
INVESTMENT

124. Linked Transactions  
125. Foreign Domiciliary Account (FDA)  
126. Safe Custody and Safety Deposit Boxes  
127. Customer's Identity Not Properly Obtained  
128. Exemption from Identification Procedures  
129. One-off Cash Transaction, Remittances and Wire Transfers  
130. Re-investment of Income  
131. Amendment or Revocation of these Regulations  
132. Interpretation  
133. Citation

SCHEDULES



S. 1. No. 16 of 2013

**CENTRAL BANK OF NIGERIA (ANTI-MONEY LAUNDERING AND  
COMBATING THE FINANCING OF TERRORISM IN BANKS AND OTHER  
FINANCIAL INSTITUTIONS IN NIGERIA) REGULATIONS, 2013**

In exercise of the powers conferred upon me by the provisions of section 51(1) of the Banks and Other Financial Institutions Act, 2004 and all other powers enabling me in that behalf, I, SANUSI LAMIDO SANUSI, Governor of the Central Bank of Nigeria, make the following Regulations—

[ 29th August, 2013 ]

Commence-  
ment.

## PART I—OBJECTIVES, SCOPE AND APPLICATIONS

1. The objectives of these Regulations are to—

Objective.

(a) provide Anti-Money Laundering and Combating the Financing of Terrorism (“AML/CFT”) compliance guidelines for financial institutions under the regulatory purview of the Central Bank of Nigeria (“CBN”) as required by relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism Prevention Act, 2011 (as amended) and other relevant laws and Regulations ;

(b) enable the CBN to diligently enforce AML/CFT measures and ensure effective compliance by financial institutions ; and

(c) provide guidance on Know Your Customer (“KYC”) measures to assist financial institutions in the implementation of these Regulations.

2.—(1) These Regulations cover the relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism Prevention Act, 2011 (as amended) and any other relevant laws or Regulations.

Scope.

(2) These Regulations cover—

(a) the key areas of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy ;

(b) development of Compliance Unit and function ;

(c) Compliance Officer designation and duties ;

(d) the requirement to co-operate with the competent or supervisory authorities ;

(e) conduct of Customer Due Diligence ;

(f) monitoring and filing of suspicious transactions to the Nigerian Financial Intelligence Unit (“NFIU”) and other reporting requirements ;

(g) reporting requirements ;

(h) record keeping ; and

(i) AML/CFT employee training.

3. These Regulations shall apply to banks and other financial institutions in Nigeria within the regulatory purview of the Central Bank of Nigeria.

Application.



PART II—ANTI-MONEY LAUNDERING AND COMBATING  
THE FINANCING OF TERRORISM DIRECTIVES

AML/CFT  
Institutional  
Policy  
Framework.

4.—(1) A financial institution shall adopt policies stating its commitment to comply with Anti-Money Laundering ('AML') and Combating Financing of Terrorism ('CFT') obligations under subsisting laws, regulations and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activities, money laundering or terrorism.

(2) A financial institution shall formulate and implement internal controls and other procedures to deter criminals from using its facilities for money laundering and terrorist financing.

(3) Financial Institutions shall adopt a risk-based approach in the identification and management of their AML/CFT risks in line with the requirements of these Regulations.

(4) Financial Institutions shall comply promptly with requests made pursuant to current AML/CFT legislations and provide information to the Central Bank of Nigeria ("CBN"), Nigeria Financial Intelligence Unit ("NFIU") and other competent authorities.

(5) Financial Institutions shall not in any way inhibit the implementation of the provisions of these Regulations and shall co-operate with the regulators and law enforcement agencies in the implementation of a robust AML/CFT regime in Nigeria.

(6) Financial institutions shall render statutory reports to appropriate authorities as required by law and shall guard against any act that will cause a customer or client to avoid compliance with AML/CFT Legislations.

(7) Financial institutions shall identify, review and record other areas of potential money laundering and terrorist financing risks not covered by these Regulations and report same to the appropriate authorities.

(8) Financial institutions shall reflect AML/CFT policies and procedures in their strategic policies.

(9) Financial institutions shall conduct on-going Due Diligence and where appropriate, enhanced Due Diligence on all business relationships and shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

(10) Financial institutions shall ensure that their employees, agents and others doing business with them, clearly understand the AML/CFT programme.

Risk  
Assessment.

5. A financial institution shall—

(a) take appropriate steps to identify, assess and understand its Money Laundering ('ML') and the Financing of Terrorism ('FT') risks for customers, countries or geographic areas of its operations, products, services and delivery channels ;

- (b) document its risk assessments profile ;
- (c) consider all relevant risk factors before determining the overall level of risk and the appropriate level and type of mitigation to be applied;
- (d) keep the assessments in this regulation up to date ; and
- (e) have the appropriate mechanisms to provide risk assessments reports to regulatory, supervisory and competent authorities, and Self-Regulatory Organizations ('SROs').

**6. A financial institution shall—**

- (a) have policies, controls and procedures which are approved by its board of directors to enable it manage and mitigate the risks that have been identified (either by the country or by the financial institution) ;
- (b) monitor the implementation of the controls in this regulation and enhance them, where necessary ; and
- (c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

Risk  
Mitigation.

**7.—(1) A financial institution shall designate its AML/CFT Chief Compliance Officer with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme.**

Designation  
and Duties  
of AML/  
CFT  
Compliance  
Officer.

**(2) The AML/CFT Compliance Officer shall be appointed at management level and shall report directly to the Board on all matters under these Regulations.**

**(3) The duties of the AML/CFT Compliance Officer referred to in sub-regulation (1) of this regulation shall include—**

- (a) developing an AML/CFT Compliance Programme ;
- (b) receiving and vetting suspicious transaction reports from staff ;
- (c) filing Suspicious Transaction Reports ("STRs") with the NFIU ;
- (d) filing other regulatory returns with the CBN and other relevant regulatory and supervisory authorities ;
- (e) rendering "nil" reports to the CBN and NFIU, where necessary to ensure compliance ;
- (f) ensuring that the financial institution's compliance programme is implemented ;
- (g) co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements ; and
- (h) serving both as a liaison officer between his institution, the CBN and NFIU and a point-of-contact for all employees on issues relating to money laundering and terrorist financing.

Co-operation with Competent Authorities.

**8.**—(1) A financial institution shall give an undertaking that it shall comply promptly with all the requests made pursuant to the provisions of relevant AML/CFT laws and Regulations and provide all requested information to the CBN, NFIU and other competent authorities.

(2) A financial institution's procedures for responding to authorized requests for information on ML and FT shall meet the following—

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

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

(c) protecting the security and confidentiality of such requests.

**PART III—OFFENCES, MEASURES AND SANCTIONS**

Scope of Offences.

**9.**—(1) A financial institution shall identify and file suspicious transaction reports to the NFIU, where funds, assets or property are suspected to have been derived from any of the following criminal activities—

(a) participation in an organized criminal group and racketeering ;

(b) terrorism, including terrorist financing ;

(c) trafficking in persons and migrant smugglings ;

(d) sexual exploitation, including sexual exploitation of children ;

(e) illicit trafficking in narcotic drugs and psychotropic substances ;

(f) illicit arms trafficking ;

(g) illicit trafficking in stolen and other goods ;

(h) corruption ;

(i) bribery ;

(j) fraud ;

(k) currency counterfeiting ;

(l) counterfeiting and piracy of products ;

(m) environmental crime ;

(n) murder ;

(o) grievous bodily injury ;

(p) kidnapping, illegal restraint and hostage-taking ;

(q) robbery or theft ;

(r) smuggling, including smuggling done in relation to customs and excise duties and taxes) ;

(s) tax crimes, related to direct taxes and indirect taxes ;

- (i) extortion ;
- (ii) forgery ;
- (v) piracy ;
- (w) insider trading and market manipulation, or
- (x) any other predicate offence under the Money Laundering (Prohibition) Act, 2011 (as amended) and the Terrorism Prevention Act, 2011 (as amended).

**10.—(1)** Terrorism financing offences extend to any person or entity who solicits, acquires, provides, collects, receives, possesses or makes available funds, property or other services by any means to terrorists or terrorist organizations, directly or indirectly with the intention or knowledge or having reasonable grounds to believe that such funds or property shall be used in full or in part to carry out a terrorist act by a terrorist or terrorist organization in line with section 1 of the Terrorism (Prevention) Act, 2011 (as amended).

Terrorism  
Financing  
Offences.

(2) Under these Regulations, terrorism financing offences are predicate offences for money laundering and shall apply regardless of whether the person or entity alleged to have committed the offence is in the same country or a different country from the one in which the terrorist or terrorist organization is located or the terrorist act occurred or will occur.

**11.—(1)** A financial institution shall report to the NFIU any assets frozen or actions taken in compliance with the prohibition requirements of the relevant United Nations Security Council Resolutions ('UNSCRs') on terrorism, financing of proliferation of weapons of mass destruction, any future successor resolutions and the Terrorism Prevention (Freezing of International Terrorist Funds and Other Related Issues) Regulation, 2013, and any amendments that may be reflected by the competent authorities.

Targeted  
Financial  
Sanctions  
related to  
Terrorism  
Financing  
and  
Proliferation.

(2) The reports in sub-regulation (1) of this regulation shall include all transactions involving attempted and concluded transactions in compliance with the Money Laundering (Prohibition) Act, 2011 (as amended), Terrorism (Prohibition) Act, 2011 (as amended) and the Terrorism Prevention (Freezing of International Terrorist Funds and Other Related Issues) Regulation, 2013, and any amendments that may be reflected by the competent authorities.

(3) The administrative sanctions contained in Schedule I to these Regulations or in the Terrorism Prevention (Freezing of International Terrorist Funds and Other Related Measures) Regulations, 2013 shall be imposed by the CBN on institutions under its regulatory purview.

**12.—(1)** Financial institutions' secrecy and confidentiality laws shall not in any way, be used to inhibit the implementation of the requirements of these Regulations having regard to the provisions of section 38 of Economic and Financial Crimes Commission Act, 2004; section 13 of Money Laundering (Prohibition) Act, 2011 (as Amended) and section 33 of the CBN Act, 2007.

Limitation  
of Secrecy  
and  
Confidentiality  
Laws.

(2) The relevant laws cited in sub-regulation (1) of this regulation have given the relevant authorities the powers 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 necessary or as may be required.

(3) Banking secrecy or preservation of customer confidentiality shall not be invoked as a ground for objecting to the measures set out in these Regulations or for refusing to be a witness to facts likely to constitute an offence under these Regulations, the relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism Prevention Act, 2011 (as amended) and any other relevant subsisting laws or Regulations.

PART IV—CUSTOMER DUE DILIGENCE, HIGHER RISK CUSTOMERS  
AND ACTIVITIES OF POLITICALLY EXPOSED PERSONS

Customer  
Due  
Diligence  
("CDD")  
measures.

**13.**—(1) A financial institution shall undertake Customer Due Diligence ('CDD') measures when—

- (a) business relationships are established ;
- (b) carrying out occasional transactions above the applicable and designated threshold of US\$1,000 or its equivalent in other currencies 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 ;
- (c) 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 ;
- (d) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in these Regulations ; or
- (e) there are doubts on the veracity or adequacy of previously obtained customer identification data.

(2) The measures in paragraphs (a), (b) and (c) of sub-regulation (1) of this regulation, shall not apply to payments in respect of—

- (i) 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 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.
- (ii) Inter-financial institution transfers and settlements where both the originator-person and the beneficial-person are financial institutions acting on their own behalf.

(3) Financial institutions, must not after obtaining all the necessary documents and being so satisfied, repeatedly perform identification and verification exercise every time a customer conducts a transaction except there is a suspicion that the previously obtained information is not complete or has changed.

**14.—**(1) A financial institution shall 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.

Identifica-  
tion and  
verification  
of identity  
of  
Customers.

(2) A financial institution shall carry out the full range of the CDD measures contained in these Regulations, the relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), and any other relevant laws or Regulations.

(3) Financial institutions shall apply the CDD measures on a risk-sensitive basis.

(4) Types of customer information to be obtained and identification data to be used to verify the information are contained in Schedule II to these Regulations.

(5) Where the customer is a legal person or a legal arrangement, the financial institution shall—

(a) identify any person purporting to have been authorized to act on behalf of that customer by obtaining evidence of the customer's identity and verifying the identity of the authorized person ; and

(b) identify and 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.

**15.—**(1) A financial institution shall identify and take reasonable steps to verify the identity of a beneficial-owner, using relevant information or data obtained from a reliable source to satisfy itself that it knows who the beneficial-owner is through methods including—

Verification  
of Beneficial  
Ownership.

(a) for legal persons :

(i) identifying and verifying the natural persons, where they exist, that have ultimate controlling ownership interest in a legal person, taking into cognizance the fact that ownership interests can be so diversified that there may be no natural persons (whether acting alone or with others) exercising control of the legal person or arrangement through ownership ;

(ii) to the extent that it is manifestly clear under sub-paragraph (i) of this paragraph that the persons with the controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, identify and verify the natural persons, where they exist, exercising control of the legal person or arrangement through other means ; and

(iii) where a natural person is not identified under sub-paragraph (i) or (ii) of this paragraph, financial institutions shall identify and take reasonable measures to verify the identity of the relevant natural person who holds senior management position in the legal person.

(b) for legal arrangements—such as trust arrangement, financial institutions shall identify and verify the identity of the settlor, the trustee, the protector where they exist, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate or effective control over the trust including through a chain of control or ownership ; and

(c) for other types of legal arrangements, the financial institutions shall identify and verify persons in equivalent or similar positions.

(2) Financial institutions shall in respect of all customers, determine whether a customer is acting on behalf of another person or not and where the customer is acting on behalf of another person, take reasonable steps to obtain sufficient identification-data and verify the identity of the other person.

(3) A financial institution shall 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.

(4) In the exercise of its responsibility under this regulation, a financial institution shall take into account that natural persons include those persons who exercise ultimate or effective control over the legal person or arrangement and factors to be taken into consideration to satisfactorily perform this function include—

(a) for companies - the natural persons shall own the controlling interests and comprise the mind and management of the company ; and

(b) for trusts – the natural persons shall be the settlor, the trustee or person exercising effective control over the trust and the beneficiaries.

(5) Where a customer or an owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or by law or other enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of the company.

(6) The relevant identification data referred to in the foregoing regulation may be obtained from a public register, the customer and other reliable sources, and for this purpose, ownership of 5% interest or more in a company is applicable.

(7) A financial institution shall obtain information on the purpose and intended nature of the business relationship of its potential customers.

(8) A financial institution shall conduct on-going Due Diligence on a business relationship.

(9) The conduct of on-going Due Diligence includes scrutinizing the transactions undertaken by the customer throughout the course of the financial institution and customer relationship to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, his business, risk profiles and the source of funds.

(10) A financial institution shall ensure that documents, data or information collated under the CDD process are kept up-to-date and relevant by undertaking regular periodic reviews of existing records, particularly the records in respect of higher-risk business-relationships or customer categories.

**16.** A financial institution shall perform Enhanced Due Diligence for higher-risk customers, business relationship or transactions including—

- (a) non-resident customers ;
- (b) private banking customers ;
- (c) legal persons or legal arrangements such as trusts that are personal-assets-holding vehicles ;
- (d) companies that have nominee-shareholders or shares in bearer form ;
- (e) Politically Exposed Persons ('PEPs'), cross-border banking and business relationships, amongst others ;
- (f) cross-border banking and business relationships, and
- (g) any other businesses, activities or professionals as may be prescribed by regulatory, supervisory or competent authorities.

Application of Enhanced Due Diligence to Higher Risk Customers and Activities.

**17.—(1)** A financial institution shall give special attention to business relationships and transactions with persons, including legal persons and other financial institutions, from countries which do not or insufficiently apply the FATF recommendations.

Attention to High Risk Countries.

(2) A financial institution shall report transactions that have no apparent economic or visible lawful purpose to competent authorities with the background and purpose of such transactions as far as possible, examined and written findings made available to assist competent authorities.

(3) A financial institution that does a business with foreign institutions which do not apply the provisions of FATF recommendations shall take measures, including the following—

- (a) 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 ;



(b) enhance relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious ;

(c) in considering requests for approving the establishment of subsidiaries or branches or representative offices of financial institutions, in countries applying the counter measure shall take into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems ; and

(d) warn that non-financial sector businesses that transact 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.

Politically Exposed Persons (PEP).

**18.—**(1) Politically Exposed Persons ('PEPs') are individuals who are or have been entrusted with prominent public functions in Nigeria or in foreign countries, and people or entities associated with them and include—

- (a) Heads of State or Government ;
- (b) State Governors ;
- (c) Local Government Chairmen ;
- (d) senior politicians ;
- (e) senior government officials ;
- (f) judicial or military officials ;
- (g) senior executives of state owned corporations ;
- (h) important political party officials ;
- (i) family members or close associates of PEPs ; and
- (j) members of royal families.

(2) PEPs also include persons who are or have been entrusted with a prominent function by an international organization, including members of senior management including directors, deputy directors and members of the board or equivalent functions other than middle ranking or more junior individuals.

(3) Financial institutions shall 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 PEP.

(4) Financial institutions shall obtain senior management approval before they establish business relationships with a PEP and shall render monthly returns on all transactions with PEPs to the CBN and NFIU.

(5) Where a customer has been accepted or has an ongoing relationship with a financial institution and the customer or beneficial-owner is subsequently found to be or becomes a PEP, the financial institution shall obtain senior management approval to continue the business relationship.

(6) A financial institution shall take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial-owners identified as PEPs.

(7) A financial institution that is in a business relationship with a PEP shall conduct enhanced and on-going monitoring of that relationship and in the event of any transaction that is abnormal, a financial institution shall flag the account and report the transaction immediately to the NFIU as a suspicious transaction.

**19.—**(1) For cross-border and correspondent banking and other similar relationships, a financial institution shall, in addition to performing the normal CDD measures, take the following measures—

Cross-  
Border and  
Correspon-  
dent  
Banking.

(a) gather sufficient information about a respondent institution to understand fully the nature of its business and 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 ;

(b) assess the respondent institution's AML/CFT controls and ascertain that they are in compliance with FATF standards ;

(c) obtain approval from senior management before establishing correspondent relationships ; and

(d) document the respective AML/CFT responsibilities of the respondent institution.

(2) Where a correspondent relationship involves the maintenance of payable through-account, the financial institution shall 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.

**20.—**(1) A financial institution shall identify and assess the money laundering or terrorist financing risks that may arise in relation to the development of new products and new business practices (including new delivery mechanisms) and the use of new or developing technologies for both new and pre-existing products.

New  
Technologies  
and Non  
face-to-face  
Transactions.

(2) Financial institutions are to ensure that any risk assessment to be undertaken is carried out prior to the launch of the new products, business practices or the use of new or developing technologies are to be documented and appropriate measures taken to manage and mitigate such risks.

(3) A financial institution shall have policies and procedures in place to address any specific risk associated with non face-to-face business relationships or transactions.

(4) The policies and procedures required to be taken shall be applied automatically when establishing customer relationships and conducting on-going Due Diligence and measures for managing the risks are to include specific and effective CDD procedures that apply to non face-to-face customers.

Money or  
Value  
Transfer  
(MVT)  
Services.

**21.—**(1) All natural and legal persons performing Money or Value Transfer Service ('MVT operators') shall be licensed by the Banking and Payment Systems Department of the CBN and shall be subject to the provisions of these Regulations, the relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism Prevention Act, 2011 (as amended) and any other relevant laws or Regulations.

(2) MVT Operators shall maintain a current list of their agents and render quarterly returns to the CBN and the NFIU.

(3) In addition to the requirement specified in this regulation, MVT Operators shall gather and maintain sufficient information about their agents and correspondent operators or any other operators or institutions they are or likely to do business with.

(4) MVT Operators shall—

(a) assess their agents' and correspondent operators' AML/CFT controls and ascertains that such controls are adequate and effective ;

(b) obtain approval from the CBN before establishing new correspondent relationships ; and

(c) document and maintain a checklist of the respective AML/CFT responsibilities of each of their agents and correspondent operators.

Foreign  
Branches  
and  
Subsidiaries.

**22.—**(1) A financial institution shall ensure that its foreign branches and subsidiaries observe AML/CFT measures consistent with the provisions of these Regulations and apply the measures to the extent that the local or host country's laws and Regulations permit.

(2) Financial institutions shall ensure that the principle referred to in sub-regulation (1) of this regulation is observed by their branches and subsidiaries in countries which do not or insufficiently apply the requirements of these Regulations.

(3) Where the minimum AML/CFT requirements contained in these Regulations and those of the host country differ, branches and subsidiaries of Nigerian financial institutions in the host country shall apply the higher standard provided in these Regulations and such standards shall be applied to the extent that the host country's laws, regulations or other measures permit.

(4) A financial institution shall inform the CBN in writing when their foreign branches or subsidiaries are unable to observe the appropriate AML/CFT measures where they are prohibited to observe such measures by the host country's laws, regulations or other measures.

(5) Financial institutions shall subject to the AML/CFT principles contained in these Regulations, apply consistently the CDD measures at their group levels, taking into consideration the activity of the customer with the various branches and subsidiaries.

23.—(1) For every wire transfer of US\$ 1,000 or more, the ordering financial institution shall obtain and maintain the following information relating to the originator of the wire transfer—

Wire  
Transfers.

(a) the name of the originator ;

(b) the originator's account number (or a unique reference number where no account number exists) ; and

(c) the originator's address (which address may be substituted with a national identity number).

(2) For every wire transfer of US\$ 1,000 or more, the ordering financial institution shall obtain and verify the identity of the originator in accordance with the CDD requirements contained in these Regulations.

(3) For cross-border wire transfers of US\$ 1,000 or more, the ordering financial institution shall include the full originator information in sub-regulation (1) of this regulation in the message or the payment form accompanying the wire transfer.

(4) Where however, several individual cross-border wire transfers of US\$ 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.

(5) For every domestic wire transfer, the ordering financial institution shall—

(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.

(6) The inclusion of the originator's account number or the originator's unique identifier alone should be permitted by a financial institution only where the originator's full information can be made available to the beneficiary financial institution and to the appropriate authorities within three business days of receiving the request.

(7) Each intermediary and beneficiary financial institution in the payment chain shall ensure that all the originator's information that accompanies a wire transfer is transmitted with the transfer.

(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 shall be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

(9) Beneficiary's financial institution shall adopt effective risk-based procedures for identifying and handling wire transfers that are not accompanied by complete originator's information.

(10) The lack of complete originator's information is considered as a factor in assessing whether a wire transfer or related transactions are suspicious.

(11) Financial institutions shall file a Suspicious Transaction Report on wire transfers with incomplete originator's information to the NFIU.

(12) The beneficiary's financial institution shall restrict or even terminate its business relationship with the financial institutions that fail to meet the standards specified in this regulation.

(13) Cross-border and domestic transfers between financial institutions are not applicable to 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, provided that where 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) transfers and settlements between financial institution where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

**24.—(1)** Where there are low risks, financial institution shall apply reduced or simplified measures.

(2) There are low risks in circumstances where—

(a) the risk of money laundering or terrorist financing is lower ;

(b) information on the identity of the customer and the beneficial owner of a customer is publicly available ; or

(c) adequate checks and controls exist elsewhere in the national systems.

(3) In circumstances of low-risk, financial institution shall apply the simplified or reduced CDD measures when identifying and verifying the identity of their customers and the beneficial-owners.

Simplified  
Due  
Diligence  
Applicable  
to Lower  
Risk  
Customers,  
Transactions  
or  
Products.

(4) The circumstances which the simplified or reduced CDD measures refer to in sub-regulation (3) of this regulation are applicable include cases of—

(a) 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 these Regulations and are supervised for compliance with them ;

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

(c) Insurance policies for pension schemes where there is no surrender-value clause and the policy cannot be used as collateral ; and

(d) 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.

(5) Financial institution shall not apply the simplified CDD measures to a customer where there is suspicion of money laundering or terrorist financing or specific higher risk scenarios and in such a circumstance, enhanced Due Diligence is mandatory.

(6) Financial institutions shall adopt CDD measures on a risk sensitive-basis and have regard to risk involved in the type of customer, product, transaction or the location of the customer and where there is doubt, they are directed to clarify with the CBN.

25.—(1) A financial institution shall obtain and 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.

Timing of  
Verification.

(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 where—

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

(b) it is essential not to interrupt the normal business conduct of the customer in cases of non face-to-face business, securities transactions and others ; or

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

(3) Where a customer is permitted to utilize the business relationship prior to verification, financial institutions shall adopt risk management procedures relevant to the conditions under which this may occur.

(4) The procedures contemplated under sub-regulation (3) of this regulation shall include a set of measures such as—

(a) limitation of the number, types or amount of transactions that may be performed ; and

(b) the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

Existing Customers.

26.—(1) A financial institution shall apply CDD requirements to existing customers on the basis of materiality and risk, and continue to conduct Due Diligence on such existing relationships at appropriate times.

(2) The appropriate time to conduct CDD by financial institutions is where—

(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 ; or

(d) the institution becomes aware that it lacks sufficient information about an existing customer.

(3) A financial institution shall properly identify the customer in accordance with the criteria contained in these Regulations and the customer identification records shall be made available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

Failure to complete CDD.

27.—(1) A financial institution that fails to comply with the CDD measures pursuant to these Regulations shall—

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

(b) be required to render a Suspicious Transaction Report to the NFIU.

(2) The financial institution that has commenced the business relationship shall terminate the business relationship and render Suspicious Transaction Reports to the NFIU.

(3) Where, a financial institution suspects that transactions relate to money laundering or terrorist financing, during the establishment or course of the customer relationship, or when conducting occasional transactions, it shall immediately—

(a) obtain and verify the identity of the customer and the beneficial owner, whether permanent or occasional, irrespective of any exemption or any designated threshold that might otherwise apply ; and

(b) render a Suspicious Transaction Report ('STR') to the NFIU without delay.

(4) Where a financial institution suspects that a transaction relates to money laundering or terrorist financing and it believes that performing the CDD process shall tip-off the customer, it shall—

(a) not pursue the CDD process, and

(b) file an STR to the NFIU without delay.

(5) A financial institution shall ensure that its employees are aware of, and sensitive to the issues mentioned under this regulation.

(6) When assessing risk, financial institution shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied.

(7) Financial institutions are allowed to differentiate the extent of measures, depending on the type and level of risk for the various risk factors and in a particular situation they may—

- (a) apply the normal CDD for customer acceptance measures ;
- (b) enhanced CDD for on-going monitoring ; or
- (c) apply any of the procedures as may be considered appropriate in the circumstance.

28.—(1) A financial institution that relies upon a third party to conduct its CDD shall—

(a) immediately obtain the necessary information concerning the property which has been laundered or which constitutes proceeds from instrumentalities used in or intended for use in the commission of money laundering and financing of terrorism or other relevant offences ; and

(b) satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements shall be made available from the third party upon request without delay.

(2) The financial institution shall satisfy itself that a third party is a regulated and supervised institution and that it has measures in place to comply with requirements of CDD reliance on intermediaries and other third parties on CDD as contained in these Regulations.

(3) Financial institutions relying on intermediaries or other third parties who have no outsourcing, agency, business relationships, accounts or transactions with it or their clients shall perform some of the elements of the CDD process on the introduced business.

(4) The criteria to be met in carrying the elements of the CDD process by the financial institution referred to in sub-regulation (3) of this regulation are to—

(a) immediately obtain from the third party the necessary information concerning certain elements of the CDD process ;

(b) take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements shall be made available from the third party upon request without delay ;

(c) 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 these Regulations ; and

Reliance on  
Intermedia-  
ries and  
Third  
Parties on  
CDD  
Function.



(d) ensure that adequate Know Your Customer ("KYC") provisions are applied to the third party in order to obtain account information for competent authorities.

(5) Notwithstanding the conditions specified in this regulation, the ultimate responsibility for customer identification and verification shall be with the financial institution relying on the third party.

**PART V—MAINTENANCE OF RECORDS**

Maintenance  
of Records  
on  
Transactions.

**29.—**(1) A financial institution shall maintain all necessary records of transactions, both domestic and international for at least five years after completion of the transaction or such longer period as may be required by the CBN and NFIU, provided that this requirement shall apply regardless of whether the account or business relationship is on-going or has been terminated.

(2) The components of records of transaction to be maintained by financial institutions include the—

(a) records of customer's and beneficiary's names, addresses or other identifying information normally recorded by the intermediary ;

(b) nature and date of the transaction ;

(c) type and amount of currency involved ; and

(d) type and identifying number of any account involved in the transaction.

(3) Financial institutions shall maintain records of the identification data, account files and business correspondence for at least five years after the termination of an account or business relationship or such longer period as may be required by the CBN and NFIU.

(4) A financial institution shall 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.

**30.—**(1) A financial institution shall pay special attention to all complex, unusually large transactions or unusual patterns of transactions that have no visible economic or lawful purpose.

(2) A financial institution shall investigate suspicious transactions and report its findings to the NFIU immediately, in compliance with the provision of section 6(2)(c) of Money Laundering (Prohibition) Act, 2011 (as amended).

(3) For the purpose of sub-regulation (1) of this regulation, complex or unusually large transaction' or, 'unusual pattern of transactions' include significant transactions relating 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.

Suspicious  
Transaction  
Monitoring.

**31.—**(1) Where a transaction—

(a) involves a frequency which is unjustifiable or unreasonable ;

(b) is surrounded by conditions of unusual or unjustified complexity ;

(c) appears to have no economic justification or lawful objective ; or

(d) in the opinion of the financial institution involves terrorist financing or is inconsistent with the known transaction pattern of the account or business relationship,

the transaction shall be deemed to be suspicious and the financial institution shall seek information from the customer as to the origin and destination of the fund, the aim of the transaction and the identity of the beneficiary.

(2) Where a financial institution suspects that the funds mentioned under sub-regulation (1) of this regulation—

(a) are derived from legal or illegal sources but are intended to be used for an act of terrorism ;

(b) are proceeds of a crime related to terrorist financing ; or

(c) belong to a person, entity or organization considered as terrorists,

it shall immediately and without delay report the matter to the NFIU and shall not be liable for violation of the confidentiality rules and banking secrecy obligations for any lawful action taken in furtherance of this obligation.

(3) A financial institution shall immediately and without delay ; but not later than within 24 hours—

(a) draw up a written report containing all relevant information on the transaction, together with the identity of the principal and where applicable, of the beneficiary or beneficiaries ;

(b) take appropriate action to prevent the laundering of the proceeds of a crime, an illegal act or financing of terrorism ; and

(c) report to the NFIU any suspicious transaction, stating clearly the reasons for the suspicion and actions taken.

(4) The obligation on financial institutions provided for in this regulation shall apply whether the transaction is completed or not.

(5) A financial institution that fails to comply within the stipulated timeframe with the provisions of—

(a) sub-regulation (1) of this regulation is liable to a fine of ₹1,000,000 for each day the offence subsists ; or

(b) sub-regulation (2) of this regulation is liable to sanction as stipulated under the Terrorism (Prevention) Act, 2011 (as amended).

(6) Any person who being a director or employee of a financial institution warns or in any other way intimates the owner of the funds involved in a suspicious transaction report, or who refrains from making the report as required, is liable to a fine of not less than ₹10,000,000 or banned indefinitely or for a period of not less than 5 years from practicing his profession.

(7) The directors, officers and employees of financial institutions who carry out their duties in good faith shall not be liable to any civil or criminal liability, or have any criminal or civil proceedings brought against them by their customers.

32.—(1) A financial institution shall have a written Policy Framework that guides and enables its staff to monitor, recognize and respond appropriately to suspicious transactions in addition to the list of Money Laundering “Red Flags” provided for in the Third Schedule to these Regulations.

(2) Every financial institution shall appropriately designate an officer as the AML/CFT Compliance Officer to supervise the monitoring and reporting of terrorist financing and suspicious transactions, among other duties.

(3) Financial institutions shall be alert to the various patterns of conduct that are known to be suggestive of money laundering, and shall maintain and disseminate a checklist of such transactions to the relevant staff.

(4) When any staff of a financial institution detects any “red flag” or suspicious money laundering or terrorist financing activity, the institution shall promptly institute a “Review Panel” under the supervision of the AML/CFT Compliance Officer and every action taken shall be recorded.

(5) A financial institution and its staff shall maintain confidentiality in respect of any investigation conducted in pursuance of these Regulations and any suspicious transaction report that may be filed with the NFIU consistent with the provision of the Money Laundering (Prohibition) Act, 2011 (as amended) and the Terrorism (Prevention) Act, 2011 (as amended), and shall not say anything that might “tip off” any person or entity that is under suspicion of money laundering.

(6) 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 shall promptly report its suspicions to the NFIU.

(7) All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved.

(8) The requirement to report suspicious transactions applies regardless of whether they are considered to involve tax matters or other matters.

(9) Financial institutions, their directors, officers and employees whether permanent or temporary, are prohibited from disclosing the fact that a report of a transaction shall be filed with the competent authorities.

(10) In compliance with the Terrorism (Prevention) Act, 2011 (as amended), financial institutions are also required to, forward to the NFIU without delay but not later than within 24 hours, reports of suspicious transactions relating to—

(a) funds derived from illegal or legal sources are intended to be used for any act of terrorism ;

(b) proceeds of a crime related to terrorism financing ; or

(c) proceeds belonging to a terrorist, terrorist entity or organization.

## PART VI—MONITORING, INTERNAL CONTROLS, PROHIBITIONS AND SANCTIONS

**33.—**(1) A financial institution shall establish and maintain internal procedures, policies and controls to prevent money laundering and financing of terrorism and to communicate these to their employees.

Internal  
Controls,  
Compliance  
and Audit.

(2) The procedures, policies and controls established by financial institution shall cover operational matters including the CDD, record retention, the detection of unusual and suspicious transactions and the reporting obligation.

(3) 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.

(4) Financial institutions are accordingly required to develop programs against money laundering and terrorist financing, such as—

(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) on-going employee training programs to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends ;

(c) providing clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting ; and

(d) adequately resourced and independent audit function to test compliance with the procedures, policies and controls.

(5) A financial institution shall put in place a structure that ensures the operational independence of the Chief Compliance Officer ('CCO') and Branch Compliance Officers.

**34.—**(1) Failure to comply with the provisions contained in these Regulations shall attract appropriate sanction in accordance with the provisions of the MLPA, 2011 (as amended), existing laws on AML/CFT and as provided for under the provisions of the Second Schedule to these Regulations.

Sanctions  
and  
Penalties for  
Non-  
Compliance.

(2) A financial institution, its officers or employees shall not benefit from any violation of extant AML/CFT laws and Regulations.

(3) A financial institution that fails to comply with, or contravenes the provisions in these Regulations, shall be subject to sanctions by the CBN (including the suspension or withdrawal of its operating licence).

(4) Any individual, being an official of a financial institution, who fails to take reasonable steps to ensure compliance with the provisions of these Regulations shall be sanctioned accordingly based on relevant provisions of the Money Laundering (Prohibition) Act, 2011 (as amended), the Terrorism (Prevention)

Act, 2011 (as amended) and any other relevant law or Regulations, the extant administrative sanction regime issued by the Central Bank of Nigeria or direction by the Attorney-General of the Federation; including revocation, suspension or withdrawal of professional licences by appropriate self-regulatory organizations.

(5) Criminal cases involving officers and the financial institutions shall be referred to the relevant law enforcement agencies for prosecution and the offender shall be liable to forfeit any pecuniary benefit obtained as a result of the violation or breach.

(6) Incidence of false declaration, false disclosure, non-declaration or non-disclosure of returns to be rendered under these Regulations by a financial institution or its officers shall be subject to administrative review and sanctions as stipulated in these or other Regulations and the appropriate administrative or civil penalties applied.

**35.—(1)** A financial institution shall not keep anonymous accounts or accounts in fictitious names.

Prohibition  
of  
Numbered  
or  
Anonymous  
Accounts,  
Accounts in  
Fictitious  
names and  
Shell banks.

(2) A financial institution shall not establish correspondent relationships with high risk foreign banks, including shell banks with no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks.

(3) Shell banks are prohibited from operating in Nigeria as provided in Money Laundering (Prohibition) Act, 2011 (as amended).

(4) A financial institution shall—

(a) not enter into or continue respondent or correspondent banking relationships with shell banks; and

(b) satisfy itself that a respondent financial institution in a foreign country does not permit its accounts to be used by shell banks.

(5) A financial institution, corporate body or any individual that contravenes the provisions of this regulation shall on conviction be liable to a fine of not less than ₦10,000,000 and in addition to the—

(a) prosecution of the principal officers of the corporate body ; and

(b) winding up and prohibition of its re-constitution or incorporation under any form or guise.

(6) A financial institution shall take all necessary measures to satisfy itself that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

Other forms  
of  
Reporting.

**36.—(1)** A financial institution shall report in writing any single transaction, lodgment or transfer of funds in excess of ₦5,000,000 and ₦10,000,000 or their equivalent made by an individual and corporate body respectively to the NFIU in accordance with section 10 (1) of the Money Laundering (Prohibition) Act, 2011 (as amended).

(2) In compliance with section 2(1) of the Money Laundering (Prohibition)

Act, 2011 (as amended) financial institutions shall render reports in writing on transfers to or from a foreign country of funds or securities by a person or body corporate including a Money Service Business of a sum exceeding US\$10,000 or its equivalent to CBN, Securities and Exchange Commission ('SEC') and the NFIU within 7 days from the date of the transaction.

(3) Details of a report sent by a financial institution to the NFIU shall not be disclosed by the institution or any of its officers to any other person.

37.—(1) A financial institution shall design comprehensive employee education and training programmes, to make employees fully aware of their obligations and also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks.

AML/CFT  
Employee-  
education  
and Training  
Programme.

(2) The timing, coverage and content of the employee training programme shall be tailored to meet the needs of the financial institution to ensure compliance with the requirements and provisions of these Regulations.

(3) A financial institution shall provide comprehensive training programmes for staff covering compliance officers and as part of the orientation programmes for new staff and those posted to the front office, banking operations and branch office staff, particularly cashiers, account opening, mandate, and marketing staff, internal control and audit staff and managers.

(4) A financial institution shall render quarterly returns on their level of compliance on their education and training programmes to the CBN and NFIU.

(5) An employee training programme shall be developed under the guidance of the AML/CFT Compliance Officer in collaboration with the top Management.

(6) The basic elements of the employee training programme of financial institutions shall include—

- (a) AML Regulations and offences ;
- (b) the nature of money laundering ;
- (c) money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies ;
- (d) reporting requirements ;
- (e) Customer Due Diligence ;
- (f) risk-based approach to AML and CFT ; and
- (g) record keeping and retention policy.

(7) A financial institution shall submit its annual AML/CFT employee training programme for the following year to the CBN and NFIU at the end of June and December every financial year.

Monitoring  
of employee  
conduct.

**38.—(1)** A financial institution shall monitor their employees' accounts for potential signs of money laundering.

(2) A financial institution shall subject employees' accounts to the same AML/CFT procedures as applicable to other customers' accounts.

(3) The requirement specified in sub-regulation (2) of this regulation shall be performed under the supervision of the AML/CFT Chief Compliance Officer and the account of this officer is in turn to be reviewed by the Chief Internal Auditor or a person of adequate and similar seniority.

(4) Compliance reports including findings shall be rendered to the CBN and NFIU at the end of June and December of every year.

(5) The AML/CFT performance review of staff shall be part of employees' annual performance appraisals.

Protection  
of Staff who  
Report  
Violations.

**39.—(1)** A financial institution shall make it possible for employees to report any violations of the institution's AML/CFT compliance programme to the AML/CFT Compliance Officer.

(2) A financial institution shall direct its employees in writing to always cooperate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to the NFIU.

(3) Where the violations involve the Chief Compliance Officer, employees shall report the violations to a designated higher authority such as the Chief Internal Auditor, the Managing Director or in confidence to the CBN or to the NFIU.

(4) A financial institution shall inform its employees in writing to make their reports confidential and to assure employees of protection from victimization as a result of making any report.

Additional  
areas of  
AML/CFT  
Risks.

**40.—(1)** A financial institution shall review, identify and record other areas of potential money laundering risks not covered by these Regulations and report the risk quarterly to the CBN and NFIU.

(2) A financial institution shall review its 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 Regulations.

Additional  
Procedures  
and  
Mitigants.

**41.** After carrying out the review of the AML/CFT framework and identified new areas of potential money laundering vulnerabilities and risks, financial institution shall design additional procedures and mitigants as contingency plan in their AML/CFT Operational Manuals with indication on how such potential risks shall be appropriately managed where they crystallize and details of the contingency plan rendered to the CBN and NFIU on the 31st December of every financial year.

Testing for  
the  
adequacy of  
the AML/  
CFT  
Compliance.

**42.—(1)** A financial institution shall make a policy commitment and subject its AML/CFT Compliance Programme to independent-testing or require its internal audit function to determine the adequacy, completeness and effectiveness of the programme.

(2) Report of compliance by a financial institution shall be rendered to the CBN and NFIU by 31st December of every financial year and any identified weaknesses or inadequacies promptly addressed by a financial institution.

**43.**—(1) The ultimate responsibility for AML/CFT compliance is placed on the Board and top Management of every financial institution in Nigeria.

(2) The Board of a financial institution shall ensure that a comprehensive operational AML/CFT Policy and Procedure is formulated annually by Management and presented to the Board for consideration and formal approval.

(3) Copies of the approved AML/CFT Policy and Procedure referred to in sub-regulation (2) of this regulation shall be forwarded to the CBN and NFIU within six months of the release of these Regulations.

(4) Monthly reports on the AML/CFT compliance status of a financial institution shall be presented to the board by the Chief Compliance Officer for its information and necessary action.

**44.** Every financial institution shall have a comprehensive AML/CFT—compliance programme to guide its efforts and to ensure the diligent implementation of its programme, to entrench in the institution a culture of compliance, to minimize the risks of being used to launder the proceeds of crime and also to provide protection against fraud, reputation and financial risks.

#### PART VII—GUIDANCE ON KNOW YOUR CUSTOMER (“KYC”)

**46.**—(1) To further deepen financial inclusion, a three tiered KYC standard shall be utilized to ensure application of flexible account opening requirements for low-value and medium value accounts which shall be subject to caps and restrictions as the amounts of transactions increase where the account opening requirements shall increase progressively with less restrictions on operations stated in this regulation.

(2) Tier one for which—

(a) basic customer information required to be provided are :

(i) passport photograph ;

(ii) name, place and date of birth ;

(iii) gender, address, telephone number, etc ;

(b) information in paragraph (a) of this sub-regulation may be sent electronically or submitted onsite in bank’s branches or agent’s office;

(c) evidence of information provided by a customer or verification of same is not required ;

(d) the accounts shall be closely monitored by the financial institution ;

(e) the accounts may be opened at branches of the financial institutions by the prospective customer or through banking agents ;

(f) no amount is required for opening of accounts ;

Formal  
Board  
approval of  
the AML/  
CFT  
Compliance.

Culture of  
compliance.

Three  
Tiered KYC  
Requirements.



(g) such accounts may cover Mobile Banking products, issued in accordance with the CBN Regulatory Framework for Mobile Payments Services in Nigeria ;

(h) deposits may be made by account holder and 3rd parties while withdrawal is restricted to account holder only ;

(i) may be linked to mobile phone accounts ;

(j) operation is valid only in Nigeria ;

(k) limited ATM transactions are allowed ;

(l) a maximum single deposit amount is limited to ₦20,000 and maximum cumulative balance of ₦200,000 at any point in time ;

(m) international funds transfer is prohibited ; and

(n) accounts are strictly savings ;

(3) Tier two for which—

(a) evidence of basic customer information such as passport photograph, name, place and date of birth, gender and address is required ;

(b) items in paragraph (a) of this regulation may be forwarded electronically or submitted on-site in banks' branches or agents' offices ;

(c) customer information obtained shall be against similar information contained in the official data-bases such as National Identity Management Commission (NIMC), Independent National Electoral Commission (INEC) Voters Register, Federal Road Safety Commission (FSRC) among others ;

(d) accounts may be opened face to face at any branch of a bank by agents for enterprises used for mass payroll or by the account holder ;

(e) evidence of basic customer information is required at this level and identification, verification and monitoring by financial institutions are also required ;

(f) accounts may be contracted by phone or at the institution's website;

(g) accounts may be linked to a mobile phone ;

(h) may be used for funds transfers within Nigeria only ;

(i) the accounts are strictly savings ;

(j) no amount is required for opening of the accounts ;

(k) such accounts cover Mobile Banking products (issued in accordance with the CBN Regulatory Framework for Mobile Payments Services in Nigeria) ;

(l) maximum single deposit of ₦50,000 and a maximum cumulative balance of ₦400,000 are allowed at any time ; and

(m) withdrawal shall be denied where cross-checking of client's identification information is not completed at the point of account opening.

(4) Tier three for which—

(a) a financial institution shall obtain, verify and maintain copies of all the required documents for opening of accounts in compliance with the KYC requirements contained in these Regulations ;

(b) no amount is required for opening of the accounts ;

(c) there is no limit on cumulative balance, deposit and transactions, and

(d) KYC requirements shall apply.

**46.—**(1) A Financial institution shall not establish a business relationship until the relevant parties to the relationship have been identified, verified, and the nature of the business they intend to conduct ascertained.

Duty to  
Obtain  
Identification  
Evidence.

(2) Where an on-going business relationship is established, any activity that is not consistent to the business relationship shall be examined to determine whether or not there are elements of money laundering, terrorist financing or any suspicion activity.

(3) The first requirement of knowing your customer for money laundering and terrorist financing purposes, is for the financial institution to be satisfied that a prospective customer is who he claims to be.

(4) A Financial institution shall not engage in any financial business or provide advice to a customer or potential customer except where the financial institution is sure or certain as to who that person actually is.

(5) Where a customer is acting on behalf of another in a situation where funds are supplied by someone else or the investment is to be held in the name of someone else, a financial institution shall verify the identity of the customer, the agent or trustee except where the customer is itself a Nigerian regulated financial institution.

(6) A Financial institution shall obtain evidence of identification of its customers.

(7) A financial institution shall identify all relevant parties to a business relationship from the beginning in accordance with the general principles of obtaining satisfactory identification evidence set out in these Regulations.

**47.—**(1) A financial institution shall obtain sufficient information on the nature of the business that its customer intends to undertake, including expected or predictable pattern of transactions.

Nature and  
Level of the  
Business.

(2) The information obtained before the commencement of the business shall include—

(a) purpose for opening the account or establishing the relationship ;

(b) nature of the activity that is to be undertaken ;

(c) expected origin of the funds to be used during the relationship ; and

(d) details of occupation, employment or business activities and sources of wealth or income.

(3) A financial institution shall take reasonable steps to keep the information up-to-date as the opportunities arise, include where an existing customer opens a new account.

(4) Any information obtained during any meeting, discussion or other communication with a customer shall be recorded and kept in a customer's file to ensure, as far as practicable, that current customer information is readily accessible by the Anti-Money Laundering Compliance Officers ('AMLCOs') or relevant regulatory bodies.

Application of Commercial Judgment.

**48.**—(1) A financial institution shall take a risk-based approach of KYC requirements.

(2) A financial institution shall decide on the number of times to verify the customers' records during the relationship, the identification evidence required and when additional checks are necessary and its decisions shall be recorded.

(3) A financial institution shall for personal account relationships, identify and verify all joint-account holders.

(4) A financial institution shall for private company or partnership, identify and verify the principal owners or controllers.

(5) The identification evidence obtained from the beginning of a business relationship shall be reviewed against the inherent risks in the business or service.

Identification.

**49.** The customer identification process shall continue to exist throughout the duration of the business relationship.

(2) The process of confirming and updating identity and address, and the extent of obtaining additional KYC information collected may differ from one type of financial institution to another.

(3) The general principles for establishing the identity of legal and natural persons and the guidance on obtaining satisfactory identification evidence set out in these Regulations are not exhaustive.

Factors to consider in identification.

**50.** In determining a customer's identity under these Regulations, the following shall be considered—

(a) the name used ;

(b) date of birth ;

(c) the residential address at which the customer can be located ;

(d) in the case of a natural person, the date of birth shall be obtained as an important identifier in support of the name and there shall be no obligation to verify the date of birth provided by the customer ; and

(e) where an international passport, driver's licence, INEC voter's card or national identity card is taken as evidence of identity, the number, date and place or country of issue (as well as expiry date in the case of international passport and driver's licence) shall be recorded.

**51.—**(1) The identity of a customer shall be verified whenever a business relationship is to be established, on account opening, during one-off transaction or where a series of linked transactions takes place.

Time for  
Verification  
of Identity.

(2) In these Regulations, "transaction" include the giving of advice and "advice" under this regulation shall not apply where information is provided on the availability of products or services and when a first interview or discussion prior to establishing a relationship takes place.

(3) Where the identification procedures have been completed and business relationship established, as long as contact or activity is maintained and records concerning that complete and kept, no further evidence of identity shall be undertaken when another transaction or activity is subsequently undertaken.

(4) Where an investor finally realizes the investment made (wholly or partially), where the amount payable is US\$ 1,000 or its equivalent or above or such other monetary amounts as may, from time to time be stipulated by any applicable money laundering legislation or Regulations, the identity of the investor shall be verified and recorded where this had not been done previously.

(5) Where there is a redemption or surrender of an investment (wholly or partially), a financial institution shall take reasonable measures to establish the identity of the investor where payment is made to—

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

(b) a bank account held (solely or jointly), in the name of the legal owner of the investment by any electronic means.

**52.—**(1) Financial institutions shall obtain sufficient evidence of the client's identity to ascertain that the client is the person he claims to be.

Verification  
of Identity.

(2) Where a person is acting on behalf of another, the obligation is to obtain sufficient evidence of identities of the two persons involved.

**53.—**(1) Notwithstanding the provisions of regulation 52 of these Regulations, in situation of consortium lending, the lead-manager or agent shall supply a confirmation letter as evidence that he has obtained the required identity.

Exceptions.

(2) There is no obligation to look beyond the client where—

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

(b) the client is a bank, broker, fund manager or other regulated financial institutions; or

(c) all the businesses are to be undertaken in the name of a regulated financial institution.

Additional Verification Requirements.

**54.** In other circumstances, except where 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 shall be verified for—

(a) the named account holder or person in whose name an investment is registered ;

(b) any principal beneficial owner of funds being invested who is not the account holder or named investor ;

(c) the principal controller of an account or business relationship including those who regularly provide instructions ; and

(d) any intermediate parties including cases where an account is managed or owned by an intermediary.

Identification of Directors and other Signatories.

**55.** A financial institution shall identify directors and all the signatories to an account.

Joint Account Holders.

**56.** Identification evidence shall be obtained for all joint applicants or account holders.

Verification of Identity for High Risk Business.

**57.** For higher risk business undertaken for private companies including those not listed on the stock exchange sufficient evidence of identity and address shall be verified in respect of—

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

(b) those with principal control over the company's assets (e.g. principal controllers or directors).

Duty to keep watch of significant changes in nature of business.

**58.** A financial institution shall—

(a) be at alert in circumstances that may indicate any significant changes in the nature of a business or its ownership and shall make enquiries accordingly; and

(b) observe the additional provisions for High Risk Categories of Customers under AML/CFT directive in these Regulations.

Verification of identity of Person providing Funds for Trust.

**59.—(1)** A financial institution shall obtain and verify the identity of those providing funds for Trusts.

(2) The identity of those providing funds for Trust envisaged under these regulations include the settlor 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.

**60.** Where an investor sets up a savings account or a regular savings scheme whereby, the funds are supplied by one person for investment in the name of another (such as in the case of a spouse or a child), the person who funds the subscription or makes deposits into the savings scheme is for all intent and purposes, the applicant for the business in question and for such person, identification evidence shall be obtained in addition to that of the legal owner.

Savings schemes and investments in third parties' names.

**61.—(1)** Identification evidence shall 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.

Personal Pension Schemes.

(2) Personal pension advisers are charged with the responsibility of obtaining the identification evidence on behalf of the pension fund provider and confirmation that identification evidence has been taken shall be provided on the transfer of a pension to another pension fund provider.

**62.—(1)** An acceptable time-span for obtaining satisfactory evidence of identity is determined by the nature of the business, the geographical location of the parties and the possibility of obtaining the evidence before commitments are entered into or actual monies given or received.

Timing of Identification Requirements.

(2) Any business conducted before satisfactory evidence of identity has been obtained shall only be in exceptional cases and under circumstances that can be justified with regard to the risk and in such a case, financial institution shall—

(a) 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

(b) where the client does not supply the required information as stipulated in paragraph (a) of this regulation, the financial institution shall discontinue any activity it is conducting for the client and bring to an end any understanding reached with the client.

(3) A financial institution shall also observe the provision in the timing of verification under the AML/CFT directive contained in these Regulations.

(4) A financial institution may however start processing the business or application immediately, provided that it—

(a) promptly takes appropriate steps to obtain identification evidence ; and

(b) does not transfer or pay any money out to a third party until the identification requirements are carried out.

**63.—(1)** The failure or refusal of an applicant to provide satisfactory identification evidence within a reasonable time and without adequate explanation may lead to a suspicion that the depositor or investor is engaged in money laundering.

Consequence of failure to provide satisfactory Identification Evidence.

(2) A financial institution under the situation stipulated in sub-regulation (1) of this regulation shall immediately make an STR to the NFIU based on the information in its possession before the funds involved are returned to the potential client or original source of the funds.

(3) A financial institution shall have in place written and consistent policies of closing an account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.

(4) A financial institution is also required to respond promptly to inquiries made by competent authorities and financial institutions on the identity of their customers.

Identification  
Procedures.

**64.—**(1) A financial institution shall ensure that it is dealing with a real person or organization whether natural, corporate or legal, by obtaining sufficient identification evidence.

(2) Where reliance is placed on a third party to identify or verify the identity of an applicant, the overall responsibility for obtaining satisfactory identification evidence rests with the account holding financial institution.

(3) In all cases, it is mandatory to obtain satisfactory evidence that a person lives at the address he provided 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.

(4) The identification process should be cumulative, as no single form of identification can be fully guaranteed as genuine or representing correct identity.

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

(6) An introduction from a respected customer, a person personally known to a Director or Manager or a member of staff often provides comfort but shall not replace the need for identification evidence requirements to be complied with as set out in this Regulation.

(7) Details of the person who initiated and authorized the introduction should be kept in the customer's mandate file along with other records and the Directors or Senior Managers shall insist on the prescribed identification procedures for every applicant.

New  
Business for  
Existing  
Customers.

**65.—**(1) Where an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, it shall not be necessary 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, provided that procedures are put in place to guard against impersonation or fraud.

(2) The opportunity of opening the new account referred to in sub-regulation (1) of this regulation shall be utilized to ask the customer to confirm the relevant details and to provide any missing KYC information and where—

(a) there was an existing business relationship with the customer and identification evidence had not previously been obtained ;

(b) there had been no recent contact or correspondence with the customer within the past three months ; or

(c) a previously dormant account is re-activated.

(3) In the circumstances in sub-regulation (2) of this regulation, details of the previous account and any identification evidence previously obtained or any introduction records shall be linked to the new account-records and retained for the prescribed period in accordance with the provisions of these Regulations.

66.—(1) In order to guard against the dangers of postal-interception and fraud, prospective customers shall not be asked to send originals of their valuable personal identity documents including international passport, identity card, driver's licence, by post.

Certification  
of  
Identification  
Documents.

(2) Where there is no face-to-face contact with a customer and documentary evidence is required, certified true copies by a lawyer, notary public or court of competent jurisdiction, banker, accountant, senior public servant or their equivalent in the private sector shall be obtained provided that the person undertaking the certification is known and capable of being contacted. In the case of a foreign national, a copy of international passport, national identity card or documentary evidence of his address shall be certified by—

(a) the embassy, consulate or high commission of the country of issue ;

(b) a senior official within the account opening institution ; or

(c) a lawyer or notary public.

(3) Certified True Copies of identification evidence are to be stamped, dated and signed "original sighted by me" by a senior officer of the financial institution.

(4) A financial institution shall always ensure that a good production of the photographic evidence of identity is obtained provided that where this is not possible, a copy of evidence certified as providing a good likeness of the applicant is acceptable in the interim.

67.—(1) Records of the supporting evidence and methods used to verify identity shall be retained for a minimum period of five years after the account is closed or the business relationship ended.

Recording  
Identification  
Evidence.

(2) Where the supporting evidence cannot be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence shall be recorded to enable the documents to be obtained later.



(3) Confirmation of evidence in sub-regulation (2) of this regulation shall 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.

(4) Where checks are made electronically, a record of the actual information obtained or where it can be re-obtained shall be retained as part of the identification evidence.

(5) The record in sub-regulation (4) of this regulation shall make the reproduction of the actual information that would have been obtained before, less cumbersome.

Concession  
in respect of  
Payment  
made by  
Post.

68.—(1) Where the money laundering risk is assessed to be low, concession may be granted for product or services in respect of long-term life insurance business or purchase of personal investment products.

(2) Where payment is to be made from an account held in a customer's name or jointly with one or more other persons, at a regulated financial institution, no further evidence of identity shall be necessary.

(3) Additional verification requirements for postal or electronic transactions shall apply to the following—

(a) products or accounts where funds may be transferred to other types of products or accounts which provide cheque or money transfer facilities ;

(b) situations where funds may be repaid or transferred to a person other than the original customer ; and

(c) investments where the characteristics of the product or account may change subsequently to enable payment to be made to third parties.

(4) Postal concession shall not be an exemption from the requirement to obtain satisfactory evidence of a customer's identity and payment debited from an account in the customer's name shall be capable of constituting the required identification evidence in its own right.

(5) To avoid proceeds of crime from being laundered by a customer who uses a third-party cheque, draft or electronic payment drawn on a bank, payment from joint accounts shall be considered acceptable for this purpose where the name of the account-holder from where the funds have been provided shall be clearly indicated on the record reflecting the payment or receipt, provided that a financial institution may rely upon the required documentary evidence of a third party, without further verification of the identity, where there is no apparent inconsistency between the name in which an application is made and the name on the payment instrument.

(6) In the case of a mortgage institution's cheque or banker's draft, it shall only be possible to rely on the concession in sub-regulation (5) of this regulation where 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, and payment

by direct debit or debit card shall be relied upon except the authentication procedure identifies the name of the account holder from which the payment is drawn and confirms the customer's address.

(7) In respect of direct debits, it shall not be assumed that the account-holding bank or institution may carry out any form of validation of the account name and number or that the mandate shall be rejected where they do not match.

(8) Where payment for the product is to be made by direct debit or debit card or 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 shall only be returned to the account from which the debits were drawn.

(9) Records shall 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.

(10) The concession in this regulation may apply both where an application is made directly to the financial institution and where a payment is passed through a regulated intermediary.

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

(12) Where the customer in sub-regulation (11) of this regulation wishes to migrate to an account that provides cheque or third party transfer facilities, additional identification checks shall be undertaken at that time, and where these circumstances occur on a regular basis a financial institution shall identify all the parties to the relationship at the outset.

**69.** Term Deposit Accounts ('TDA') can be broadly classified as a one-off transaction provided that a financial institution shall 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.

Term  
Deposit  
Account  
(TDA).

**70.** Where the balance in an investment fund 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 not been taken or confirmation obtained from the original fund manager, such evidence shall be obtained at the time of the transfer.

Investment  
Funds.

#### PART VIII—GENERAL INFORMATION

**71.** Establishing identity under these Regulations is divided into three broad categories, namely—

Establishing  
Identity.

- (a) private individual customers ;
- (b) quasi corporate customers ; and
- (c) pure corporate customers.

Private  
Individuals—  
General  
Information.

**72.—(1)** The following information shall be established and independently validated for all private individuals whose identities need to be verified—

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

(2) The information obtained shall provide satisfaction that a person of that name exists at the address given and that the applicant is that same person so indicated, and where an applicant has recently moved from his residence, the previous address shall be validated.

(3) The date of birth shall be obtained as required by the law enforcement agencies, provided that the information need not be verified and the residence or nationality of a customer is ascertained to assist risk assessment procedures.

(4) A risk-based approach shall be adopted when obtaining satisfactory evidence of identity.

(5) The extent and number of checks may 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.

(6) The source of funds of how the payment was made, from where and by whom shall always be recorded to provide an audit trail, provided that for high risk products, accounts or customers, additional steps shall be taken to ascertain the source of wealth or funds.

(7) For low-risk accounts or simple investment products such as deposit or savings accounts without cheque-books or automated money transmission facilities, the financial institution shall satisfy itself as to the identity and address of the customer.

Private  
Individuals  
Resident in  
Nigeria.

**73.—(1)** The confirmation of name and address shall be established by reference to a number of sources.

(2) The checks shall 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.

(3) The overriding requirement to ensure that the identification evidence is satisfactory shall rest with the financial institution opening the account or providing the product or service.

Documenting  
Evidence of  
Identity.

**74.—(1)** To guard against forged or counterfeit documents, care shall be taken to ensure that documents offered are originals.

(2) Copies that are dated and signed 'original seen' by a senior public servant or equivalent in a reputable private organization may be accepted in the interim, pending presentation of the original documents.

(3) Suitable documentary evidence for private individuals resident in Nigerian as contained in the Second Schedule to these Regulations.

(4) Checking of a local or national telephone directory may be used as additional corroborative evidence but shall not be used as a primary check.

75.—(1) A financial institution shall establish the true identity and address of its customer and carry out effective checks to protect the institution against substitution of identities by applicants.

Physical  
Checks on  
Private  
Individuals  
Resident in  
Nigeria.

(2) Additional verification of a customer's identity and the fact that the application was made by the person identified shall 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 ;

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

(c) telephone contact with the applicant prior to opening of 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 previously been provided during the setting up of the account ;

(d) internet sign-on following verification procedures where the customer uses security codes, tokens, 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 ; or

(e) card or account activation procedures.

(3) A financial institution shall ensure that additional information on the nature and level of the business to be conducted and the origin of the funds to be used within the relationship are obtained from the customer.

76.—(1) An applicant's identity, address and other available information may be checked electronically by accessing other data-bases or sources, as an alternative or supplementary to documentary evidence of identity or address.

Electronic  
Checks.

(2) A financial institution shall use a combination of electronic, documentary and physical checks to confirm different sources of the same information provided by a customer.

(3) In respect of electronic checks, confidence as to the reliability of information supplied shall 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.

(4) The number or quality of checks to be undertaken shall vary depending on the diversity as well as the breadth and depth of information available from each source.

(5) Verification that the applicant is the data-subject shall be conducted within the checking process.

(6) Suitable electronic sources of information include—

(a) an electronic search of the electoral register not be used as a sole identity and address check ;

(b) access to internal or external account database ; and

(c) an electronic search of public records where available.

(7) Application of the process and procedures in this regulation shall assist financial institutions to guard against impersonation, invented-identities and the use of false addresses provided that where an applicant is a non face-to-face person, one or more additional measures shall be undertaken for re-assurance.

PART IX—FINANCIAL EXCLUSION FOR THE SOCIALLY OR FINANCIALLY  
DISADVANTAGED APPLICANTS

“Financial  
Exclusion”  
for the  
socially or  
financially  
disadvantaged  
Applicants  
Resident in  
Nigeria.

77.—(1) Notwithstanding that access to basic banking facilities and other financial services is a necessary requirement for most adults, the socially or financially disadvantaged shall not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves.

(2) The socially or financially disadvantaged shall not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves since access to basic banking facilities and other financial services is a necessary requirement for most adults.

(3) Where the socially or financially disadvantaged cannot reasonably comply with sub-regulation (1) of this regulation, the internal procedures of the financial institution shall make allowance for such persons by way of providing appropriate advice to staff on how the identities of such group of persons may be confirmed and what checks shall be made under these exceptional circumstances.

(4) 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 accept as identification evidence, a letter or statement from a person in a position of responsibility such as solicitors, doctors, ministers of religion and teachers who know the client, confirming that the client is who he says he is and his permanent address.

(5) When a financial institution has decided to treat a client as “financially excluded”, it shall record the reasons for doing so along with the account opening documents, and returns of same shall be rendered to the CBN and NFIU quarterly.

(6) Where a letter or statement is accepted from a person in position of responsibility, it shall include a telephone number where the person can be contacted for verification and the financial institution shall verify from an independent source

the information provided by that person so as to satisfy itself that such customer is the person he claims to be.

(7) A financial institution shall include in its internal procedures the "alternative documentary evidence of personal identity and address" that may be accepted to guard against "financial exclusion" and to minimize the use of the exception procedure.

(8) A financial institution shall put in place additional monitoring for accounts opened under the financial inclusion procedures to ensure that such accounts are not misused.

78.—(1) International passports or national identity cards shall generally be available as evidence of the name of a customer and reference numbers, date and country of issue shall be obtained and recorded in the customer's file as part of the identification evidence in respect of prospective customers who are not resident in Nigeria but who make face-to-face contact.

Private  
Individuals  
not resident  
in Nigeria.

(2) A financial institution shall obtain separate evidence of an applicant's permanent residential address from the best available evidence, preferably from an official source.

(3) A Post Office Box number ("P.O.Box Number") alone shall not be accepted as evidence of address and the applicant's residential address shall be such that it may be physically located by way of a recorded description or other means.

(4) Relevant evidence shall 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, provided that particular care shall be taken when relying on identification evidence obtained from other countries.

(5) A financial institution shall ensure that a customer's true identity and current permanent address are actually confirmed. In such cases, copies of relevant identity documents shall be sought and retained.

(6) Where a foreign national has recently arrived in Nigeria, reference may be made to his employer, university, evidence of traveling documents, etc. to verify the applicant's identity and residential address.

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

(8) Documentary evidence of name and address may be obtained from—

(a) an original documentary evidence supplied by the customer ;

(b) a certified copy of the customer's passport or national identity card and a separate certified document including utility bill and driving licence, verifying the customer's address ; or

(c) a branch, subsidiary, head office of a correspondent bank.

(9) Where an applicant does not already have a business relationship with the financial institution that is supplying the information or the financial institution is outside Nigeria, certified copies of relevant underlying documentary evidence shall be sought, obtained and retained by the institution.

(10) An additional comfort shall 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, where necessary.

(11) A financial institution shall use requirements in this regulation in conjunction with the First Schedule to these Regulations.

Non Face-to-Face Identification.

**79.—(1)** In respect of a non face-to-face customer, an additional measure or check shall be undertaken to supplement the documentary or electronic evidence to ensure that an applicant is who he claims to be and these additional measures shall apply whether the applicant is resident in Nigeria or elsewhere and shall be particularly robust where the applicant is requesting a bank account or other product or service that offers money transmission or third party payments.

(2) Procedures to identify and authenticate a customer shall 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.

(3) The extent of the identification evidence required in this regulation shall depend on the nature and characteristics of the product or service and the assessed risk, provided that care shall be taken to ensure that the same level of information is obtained for internet customers and other postal or telephone customers.

(4) Where reliance is placed on intermediaries to undertake the processing of applications on the customer's behalf, checks shall be undertaken to ensure that the intermediaries are regulated for money laundering prevention and that the relevant identification procedures are applied.

(5) A financial institution shall conduct regular monitoring of internet-based business or clients and where a significant proportion of the business is operated electronically, computerized monitoring systems or solutions that are designed to recognize unusual transactions and related patterns of transactions shall be put in place to recognize suspicious transactions.

(6) In all cases, evidence as to how identity has been verified shall be obtained and retained with the account opening records.

(7) AML/CFT compliance officers shall review these systems or solutions, record exemptions and report same quarterly to the NFIU.

Refugees or Asylum Seekers.

**80.—(1)** Where a refugee or asylum seeker requires a basic bank account without being able to provide evidence of identity, authentic references from the Nigerian Immigration Services endorsed by the State Security Services shall be used in conjunction with other readily available evidence.

(2) Additional monitoring procedures shall be undertaken in respect of sub-regulation (1) of this regulation to ensure that the use of the account is consistent with the customer's circumstances.

**81.—**(1) When opening accounts for students or other young people, the normal identification procedures set out in these Regulations shall be followed and where such procedures may not be relevant or do not provide satisfactory identification evidence, verification may be obtained through —

Students  
and  
Minors.

- (a) the home address of the parent ;
- (b) confirming the applicant's address from his institution of learning ; or
- (c) seeking evidence of a tenancy agreement or student accommodation contract.

(2) An account for a minor may be opened by a family member or guardian and 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 shall be obtained in addition to obtaining the birth certificate and passport of the child, provided that strict monitoring shall be undertaken.

(3) For accounts opened through a school-related scheme, the school shall provide the date of birth and permanent address of the pupil and complete the standard account opening documentation on behalf of the pupil.

(4) Account of a minor shall be constantly monitored to ensure that it is not used for the purposes of money laundering or terrorist financing and that the transaction does not exceed an amount that should be determined by the financial institution.

**82.** Trusts, nominee companies and fiduciaries are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the dirty 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.

Quasi  
Corporate  
Customers.

#### PART X—TRUST, POLICY, RECEIPT AND PAYMENT OF FUNDS

**83.—**(1) Trusts, nominees and fiduciary accounts present a higher money laundering risk than others.

Trust,  
Nominees  
and  
Fiduciaries.

(2) Identification and "Know Your Customer's Business" procedures shall be set and managed in accordance with the perceived risk.

(3) The principal objective of money laundering prevention trusts, nominees and fiduciaries shall be to verify the identity of the provider of funds such as the settlor, and those who have control over funds like the trustees and any controllers who have the power to remove the trustees.

(4) For discretionary or offshore trust, the nature and purpose of the trust and the original source of funding shall be ascertain ed.



(5) Whilst reliance may 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 shall vest with the financial institution and the underlying evidence of identity shall be made available to law enforcement agencies in the event of an investigation.

(6) Identification shall 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.

**84.—(1)** Since offshore trusts present a higher money laundering risk, additional measures shall be needed for Special Purpose Vehicles (SPVs) or International Business Companies connected to trusts.

(2) Where trusts are set up in offshore locations with strict bank secrecy or confidentiality rule, those created in jurisdictions without equivalent money laundering procedures in place shall warrant additional enquiries.

(3) Except an applicant for business is a regulated financial institution, measures shall be taken to identify the trust company or the corporate service provider in line with the requirements for professional intermediaries or companies generally.

(4) Certified copies of the documentary evidence of identity for the principals including settlors and controllers on whose behalf the applicant for business is acting shall be obtained.

(5) For overseas trusts, nominee and fiduciary accounts, where the applicant is a financial institution that is regulated for money laundering purposes—

(a) reliance may 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 ;

(b) the trustees or nominees shall be asked to state from the outset the capacity in which they are operating or making the application ; and

(c) documentary evidence of the appointment of the current trustees shall be obtained.

(6) Where the evidence is not retained in Nigeria, enquiries shall be made to determine, that there is no overriding bank secrecy or confidentiality constraint that shall restrict access to the documentary evidence of identity, shall it be needed in Nigeria.

(7) An application to open an account or undertake a transaction on behalf of another without the applicant identifying his trust or nominee capacity shall be regarded as suspicious and shall lead to further enquiries and rendition of reports to the NFIU.

(8) Where a bank in Nigeria is the applicant for an offshore trust on behalf of a customer, where the corporate trustees are not regulated, the Nigerian bank shall undertake due diligence on the trust itself.

(9) Where 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 shall be verified except where the identity of beneficiaries have not previously been verified and verification shall be carried out where payments are made to them.

**85.—(1)** For Conventional Nigerian Trusts, identification evidence shall be obtained for—

Conventional  
Family and  
Absolute  
Nigerian  
Trusts.

(a) those who have control over the funds, the principal trustees, who can include the settlor ;

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

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

(2) Where a corporate trustee such as a bank acts jointly with a co-trustee, any non-regulated co-trustee shall be verified even where the corporate trustee is covered by an exemption and the relevant guidance contained in these Regulations for verifying the identity of persons, institutions or companies shall be followed.

(3) A financial institution may not review an existing trust but the bank confirmation of the settlor and the appointment of any additional trustees shall be obtained.

(4) Copies of any underlying documentary evidence shall be certified as true copies and a check shall be carried out to ensure that any bank account on which the trustees have drawn funds is in their names.

(5) Where a risk based approach is adopted, consideration shall be given as to whether the identity of any additional authorized signatories to the bank account may be verified.

(6) A payment for any trust property shall be made to a trustee and as a matter of practice, some life assurance companies make payments directly to beneficiaries on receiving a request from the trustees, payment shall 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 in such circumstances.

**86.—(1)** Where money is received on behalf of a trust, reasonable steps shall be taken to ensure that the source of funds is properly identified and the nature of the transaction or instruction is understood.

Receipt and  
payment of  
Funds.

(2) A Payment shall be properly authorized in writing by the trustees.

**87.** Where a trustee who has been verified is replaced, the identity of the new trustee shall be verified before he is allowed to exercise control over funds of the Trust.

Identification  
of new  
Trustees.

Life policies placed in Trust.

88. Where a life policy is placed in trust, an applicant for the policy is also a trustee and where the trustees have no beneficial interest in the funds, it shall verify the identity of the person applying for the policy except that the remainder of the trustees shall 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.

89. (1) The authority to deal with assets under a Power of Attorney and Third Party Mandates constitute a business relationship.

(2) At the start of a relationship, identification evidence shall be obtained from a holder of Power of Attorney and third party mandates in addition to the customer or subsequently on a later appointment of a new attorney, where advised, within one year of the start of the business relationship.

(3) An attorney for corporate or trust business shall be verified and a financial institution shall always ascertain the reason for the granting of a power of attorney.

(4) A records of a transaction undertaken in accordance with a Power of Attorney shall be maintained as part of the client's record.

PART XI—EXECUTORSHIP, CLIENT ACCOUNTS, UNINCORPORATED AND CORPORATED ORGANIZATIONS

Executorship Accounts.

90.—(1) Where a bank account is opened for the purpose of winding up the estate of a deceased person, the identity of the executor or administrator of the estate shall be verified.

(2) Identification evidence shall not be required for the executors or administrators where payment is made from an established bank or mortgage institution's account in a deceased's name, solely for the purpose of winding up the estate in accordance with the grant of probate or letter of administration.

(3) Where a life policy pays out on death, identification evidence shall not be obtained for the legal representatives.

(4) A Payment to beneficiaries in sub-regulations (1) (2) and (3) of this regulation on the instructions of the executor or administrator may be made without additional verification requirements, except that where a beneficiary wishes to transact business in his own name, then identification evidence shall be required.

(5) Where suspicion is aroused in respect of the nature or origin of assets comprising an estate that is being wound up, such suspicion shall be reported to the NFIU.

"Client Accounts" Opened By Professional Intermediaries.

91.—(1) Stockbrokers, fund managers, solicitors, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with a financial institution.

(2) Accounts in sub-regulation (1) of this regulation may be general omnibus accounts holding the funds of many clients or they may be opened specifically for a single client.

(3) In each case, it is the professional intermediary who is the financial institution's customer. These situations shall be distinguished from those where an intermediary introduces a client who himself becomes a customer of the financial institution.

(4) Where a professional intermediary is covered and is indeed monitored under the money laundering Regulations or AML/CFT supervisors or their equivalent, identification may be waived on production of evidence.

(5) Notwithstanding sub-regulation (4) of this regulation, where the professional intermediary is not regulated by money laundering Regulations or their equivalent, the financial institution shall verify the identity of the professional intermediary and also verify the identity of the person on whose behalf the professional intermediary is acting.

(6) Where it is impossible for a financial institution to establish the identity of the person for whom a solicitor or accountant is acting, it shall 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 where the professional firm is not itself covered by these Regulations.

(7) Financial institutions shall make reasonable enquiries about transactions passing through client-accounts that give cause for concern and shall report any suspicion to the NFIU.

**92.—(1)** Where an applicant is an un-incorporated business or a partnership whose principal partners or controllers do not already have a business relationship with the financial institution, identification evidence shall be obtained in respect of the principal beneficial owners or controllers and any signatory in whom significant control has been vested by the principal beneficial owners or controllers.

Un-  
incorporated  
Business or  
Partnership.

(2) Evidence of the address of a business or partnership shall be obtained and where a current account is being opened, a visit to the place of business may be made to confirm the true nature of the business activities and a copy of the latest report and audited accounts shall be obtained.

(3) The nature of the business or partnership shall be verified to ensure that it has a legitimate purpose.

(4) Where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account or undertaking of the transaction shall be obtained.

**93.** A limited liability partnership shall be treated as a corporate customer for verification of identity and know your customer purposes.

Limited  
Liability  
Partnership.

**94.—(1)** The legal existence of an applicant-company shall be verified from official documents or sources to ensure that persons purporting to act on its behalf are fully authorized.

Pure  
Corporate  
Customers.

(2) Where the controlling principals cannot be identified, enquiries shall be made to confirm that the legal person is not merely a "brass-plate company".

The identity of a corporate company.

**95.—**(1) The identity of a corporate company shall comprise of—

- (a) registration number ;
- (b) registered corporate name and any trading names used ;
- (c) registered address and any separate principal trading addresses ;
- (d) directors ;
- (e) owners and shareholders ; and
- (f) the nature of the company's business.

(2) The extent of identification measures required to validate the information or the documentary evidence to be obtained in this regulation depends on the nature of the business or service that the company requires from the financial institution and a risk-based approach shall be taken.

(3) Information as to the nature of the normal business activities that the company expects to undertake with the financial institution shall be obtained.

(4) Before a business relationship is established, measures shall 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.

**96.—**(1) Additional procedures shall be undertaken to ensure that the applicant's business, company or society exists at the address provided and it is for a legitimate purpose because of the risks with non face-to-face business, as with the requirements for private individuals.

(2) Where the characteristics of the product or service permit, steps shall be taken to ensure that relevant evidence is obtained to confirm that any individual representing the company has the necessary authority to do so.

(3) Where the principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for the identification of personal customers shall be followed.

Public Registered Companies.

**97.** (1) Corporate customers that are listed on the stock exchange are considered to be publicly-owned and generally accountable and there is no need to verify the identity of the individual shareholders.

(2) The Identity of the directors of a quoted company may not be verified.

(3) A financial institution shall make appropriate arrangements to ensure that an 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.

(4) The Board resolution or other authority for a representative to act on behalf of the company in its dealings with the financial institution shall be obtained.

(5) Phone calls may be made to the Chief Executive Officer of a company in sub-regulation (4) of this regulation to intimate him of the application to open the account in the financial institution.

(6) Further steps shall not be taken to verify identity more than 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.

(7) Due Diligence shall be conducted where the account or service required falls within the category of higher risk business.

**98.** Where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with the financial institution, to verify the business, the following documents shall be obtained from an official or a recognized independent source—

Private  
Companies.

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

(b) a search at the CAC or an enquiry through a business information service to obtain the information on the company ;

(c) an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC ;

(d) a financial institution shall pay attention to the place or origin of the documents and background against which they were produced ; and

(e) where comparable documents cannot be obtained, verification of principal beneficial owners or controllers shall be undertaken.

**99.** 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 shall be obtained either in documentary or electronic form—

Higher Risk  
Business  
Applicant.

(a) for established companies that are incorporated for 18 months or more, a set of the latest report and audited accounts shall be produced ;

(b) a search report at the CAC or an enquiry through a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC ;

(c) 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

(d) the Memorandum and Articles of Association of the company.

**100.—(1)** Where a private company is undertaking a 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.

Higher Risk  
Business  
Relating to  
Private  
Companies.

(2) What constitutes significant shareholding or control for the purpose of this regulation depends on the nature of the company and identification evidence shall be obtained for shareholders with interests of 5% or more.

(3) Identification evidence shall be obtained for the principal-beneficial owner of the company and any other person with principal control over the company's assets.

(4) Where the principal owner is another corporate entity or trust, it shall take measures that look behind that company or vehicle and verify the identity of the beneficial-owner or settlers and where a financial institution is aware that the principal-beneficial owners or controllers have changed, they are required to verify the identities of the new owners.

(5) Financial institutions shall identify directors who are not principal controllers and signatories to an account for risk based approach purpose.

(6) Financial institutions shall visit the place of business to confirm the existence of such business premises and the nature of the business conducted.

(7) Where 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 shall be made to ascertain the reason for the changes.

(8) In full banking relationships, periodic enquiries shall be made to establish changes to controllers, shareholders or the original nature of the business or activity.

(9) Particular care shall be taken to ensure that full identification and KYC requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

Foreign  
Financial  
Institutions.

**101.—(1)** For a foreign financial institution, the confirmation of existence and regulated status shall be checked by—

(a) checking with the home country's Central Bank or relevant supervisory body ;

(b) checking with another office, subsidiary, branch, or correspondent bank in the same country ;

(c) checking with Nigerian regulated correspondent bank of the overseas institution; or

(d) obtaining evidence of its license or authorization to conduct financial and banking business from the institution itself.

(2) Additional information on banks all over the world may be obtained from various international publications and directories or any of the international business information services.

(3) The publications referred to in sub-regulation (2) of this regulation shall not replace the confirmation evidence requirements under these Regulations.

**102.—(1)** A Bureau De Change ("BDC") is subject to the provisions of these Regulations and shall be verified in accordance with the procedures for other financial institutions, and satisfactory evidence of identity, ownership structure, source of funds and a certified copy of the applicant's operating license shall be obtained.

Bureau De  
Change.

(2) A financial institution shall consider the risks associated with doing business with BDCs before entering into a business relationship with them.

**103.—(1)** As part of KYC documentation for designated non-financial businesses and professions, the certificate of registration with Special Control Unit against Money Laundering in the Federal Ministry of Trade and Investment or a certificate from a self-regulatory organization as defined under the relevant Designated Non-Financial Business and Professions ("DNFBP") Regulations shall be obtained including identities of at least two of the directors.

Designated  
Non-  
Financial  
Businesses  
and  
Professions  
(DNFBPs).

(2) Where an application is made on behalf of a club or society, a financial institution shall take reasonable steps to satisfy itself as to the legitimate purpose of the organization by sighting its constitution and the identity of at least two of the principal contact persons or signatories shall be verified in line with the requirements for private individuals and where signatories are changed, a financial institution shall verify the identity of at least two of the new signatories.

(3) Where the purpose of a club or a society is to purchase the shares of a regulated investment company or where all the members are regarded as individual clients, all the members in such cases shall be identified in line with the requirements for personal customers on a case-by-case basis.

**104.—(1)** Where transactions carried out 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 shall be verified.

Occupational  
Pension  
Schemes.

(2) In addition to the identity of the principal employer, the source of funding shall be verified and recorded to ensure that a complete audit trail exists if the employer is dissolved or wound up.

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

(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.

(5) Where individual members of an Occupational Pension Scheme are to be given personal investment advice, their identities shall be verified but where the



Trustees and principal employer have been satisfactorily identified (and the information is still current) it can be appropriate for the employer to provide confirmation of the identity of individual employees.

Registered  
Charity  
Organiza-  
tions.

**105.**—(1) A financial institution shall adhere to the identification procedures requirements for opening of accounts on behalf of charity organizations ; and the confirmation of the authority to act in the name of the organization.

(2) The opening of accounts on behalf of charity organizations in Nigeria shall be carried out by a minimum of two signatories, duly verified and documentation evidence shall be obtained.

(3) When dealing with an application from a registered charity organization, a financial institution shall obtain and confirm the name and address of the organization concerned.

(4) Where a person making an application or undertaking a transaction is not the official correspondent or the recorded alternate, a financial institution shall send a letter to the official correspondent, informing him of the charity organizations' application before it and the official correspondent shall respond as a matter of urgency where there is any reason to suggest that the application has been made without authority.

(5) An application on behalf of un-registered charity organization shall be made in accordance with the procedures for clubs and societies as set out in these Regulations.

(6) Where a charity organization is opening a current account, the identity of all signatories shall be verified and where the signatories change, identities of the new signatories shall be verified.

Religious  
Organizations  
(ROs).

**106.** A Religious Organization ("RO") shall have a CAC, and SCUML registered numbers and its identity may be verified by reference to the CAC, appropriate headquarters or regional area of the denomination, and the identity of at least two signatories to its account shall be verified.

Three -  
Tiers of  
Government  
and  
Parastatals.

**107.**—(1) Where the applicant for business is a legal person, a financial institution shall verify the legal standing of the applicant, including its principal ownership and address.

(2) A certified copy of the resolution or other documents which authorise an official representing the body to open an account or undertake any transaction shall be obtained.

(3) A financial institution shall telephone the Chief Executive Officer of the organization or parastatal concerned, to verify and confirm the application to open an account with the financial institution.

(4) An authorization from the Federal or State Accountant-General shall be obtained before any of the three tiers of government or parastatals can open accounts with a financial institution in Nigeria.

**108.** The authenticity of an applicant who requested 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 shall be checked with the Ministry of Foreign Affairs and the relevant authorities in the Consulate's home country or as confirmed by the Head of the High Commission of that country in Nigeria.

Foreign  
Consulates.

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

Intermediaries  
or other  
third parties  
to verify  
identity or  
to introduce  
business.

(a) undertake the identification procedure when introducing a customer and to obtain any additional KYC information from the client ;

(b) confirm the identification details where the customer is not resident in Nigeria ; or

(c) confirm that the verification of identity has been carried out where an agent is acting for a principal.

#### PART XII—INTRODUCTIONS, APPLICATIONS AND FOREIGN INTERMEDIARIES

**110.—(1)** 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 and shall be identified in line with the requirements for personal, corporate or business customers as appropriate.

Introductions  
from  
Authorized  
Financial  
Intermediaries.

(2) An introductory letter shall be issued by the introducing financial institution or person in respect of each applicant for business.

(3) To ensure that product-providers meet their obligations, satisfactory identification evidence shall be obtained and retained for the necessary statutory period.

(4) Each introductory letter shall either be accompanied by certified copies of the identification evidence obtained in line with the usual practice of certification of identification documents or by sufficient details and reference numbers that will permit the actual evidence obtained to be re-obtained at a later stage.

**111.—(1)** Where other arrangements have been made, the service provider shall verify the identity itself and financial intermediary shall provide along with each application, the customer's introductory letter together with certified copies of the evidence of identity which shall be placed in the customer's file.

Written  
Applications.

(2) Where these procedures are followed, a product provider, stockbroker or investment banker shall be considered to have fulfilled its own identification obligations.

(3) Where 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 shall satisfy its obligation by applying its own direct identification procedures.

Non-  
Written  
Application.

**112.—**(1) A Unit Trust Manager and other product providers receiving non-written applications from a financial intermediary, where a deal is made over a telephone or by other electronic means, shall verify the identity of such a customer and ensure that the intermediary provides specific confirmation that identity has been verified.

(2) The answers given by the intermediary shall be recorded and retained for a minimum period of 5 years.

(3) The answers constitute sufficient evidence of identity in the hands of the service provider.

Foreign  
Intermediaries.

**113.** Where business is introduced or received from a regulated financial intermediary who is outside Nigeria, the reliance that shall be placed on that intermediary to undertake the verification of identity-check shall be assessed by the AMLCO 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.

**114.—**(1) Where a customer is introduced by one part of a financial sector group to another, identity shall not be re-verified and neither shall the records be duplicated except—

(a) 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 ;

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

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

(d) in respect of group introducers from outside Nigeria, in which case arrangements shall 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) Where a financial institution has day-to-day access to all the group's KYC information and records, there is no need to identify an introduced customer or obtain a group introduction letter where the identity of that customer has been verified previously.

(3) Where an identity of a 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 shall be obtained.

(4) A financial institution shall 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.

(5) Where such restrictions apply, copies of the underlying records of identity shall, wherever possible, be sought and retained.

(6) Where identification records are held outside Nigeria, it shall be the responsibility of the financial institution to ensure that the records available meet the requirements in these Regulations.

**115.—**(1) Where an applicant is dealing in its own name as agent for its own client, a financial institution shall, in addition to verifying the agent, establish the identity of such a client.

Business  
Conducted  
by Agents.

(2) A financial institution shall accept or admit evidence as sufficient where it has established that the client is—

(a) bound by and has observed these Regulations or the provisions of the Money Laundering (Prohibition) Act, 2011 (as amended) ; and

(b) 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.

(3) Where another financial institution deals with its own client regardless of whether or not such a client has disclosed to the financial institution, then where—

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

(b) a regulated agent from outside Nigeria deals through a customer omnibus account or for a named customer through a designated account, the agent shall provide a written assurance that the identity of all the underlying clients has been verified in accordance with their local requirements ; and

(c) such an assurance cannot be obtained, then the business shall not be undertaken.

(4) Where an agent is either unregulated or is not covered by the money laundering legislation, then each case shall be treated on its own merits.

(5) The knowledge of the agent shall determine the type of the Due Diligence standards to apply and risk-based approach shall be observed by a financial institution.

**116.** Where there is a syndicated lending arrangement, the verification of identity and any additional KYC requirements rest with the lead-manager or agent to supply the normal confirmation letters.

Syndicated  
Lending.

Correspondent  
Relationship.

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

(2) The volume and nature of transactions flowing through correspondent accounts with a financial institution, from high risk jurisdictions or those with inadequacies or material deficiencies shall be monitored against expected levels and destinations and any material variances shall be checked.

(3) A financial institution shall maintain records and ensure 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.

(4) A financial institution shall guard against establishing correspondent relationships with high risk foreign banks such as shell banks or with correspondent banks that permit their accounts to be used by such banks.

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

(6) A financial institution shall terminate an account with a correspondent bank that fails to provide satisfactory answers to questions including confirming the identity of customers involved in unusual or suspicious circumstances.

Acquisition  
of one  
financial  
institution  
and  
business by  
another.

**118.—**(1) Where a financial institution acquires a 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, but it shall carry out due diligence enquiries to confirm that the acquired institution had conformed with the requirements of the provisions of these Regulations.

(2) Verification of identity shall be undertaken 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—

(a) money laundering procedures previously undertaken have not been in accordance with the requirements of these Regulations ;

(b) procedures shall be checked ; or

(c) customer-records are not available to the acquiring financial institution.

**119.**—(1) A receiving financial institution can be used by money launderers in respect of offers for sale where new issues are over-subscribed and their allotment is scaled down; the money launderer is not concerned if there is a cost involved in laundering dirty money.

Vulnerability of Receiving Bankers and Agents.

(2) New issues that trade at a discount will, therefore, still prove acceptable to the money launderer.

(3) 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.

**120.**—(1) A receiving financial institution shall obtain satisfactory identification evidence of a new applicant, 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 or as per the tiered KYC directive issued by the CBN.

Categories of persons to be identified.

(2) Where funds to be invested are being supplied by or on behalf of a third party, the identification evidence for both the applicant and the provider of the funds shall be obtained to ensure that, the audit trail for the funds is preserved.

**121.**—(1) Where an application is submitted, payment made by a broker or an intermediary acting as agent, no steps shall be taken to verify the identity of the underlying applicants, the following standard procedures shall apply—

Applications Received through Brokers.

(a) the lodging agent's stamp shall be affixed on the application form or allotment letter ; and

(b) application and acceptance forms and cover letters submitted by lodging agents shall be identified and recorded in the bank's records.

(2) The terms and conditions of the issue shall state that any requirements to obtain identification evidence are the responsibility of the broker lodging the application and not the receiving financial institution.

(3) Where the original application has been submitted by a regulated broker, no additional identification evidence shall be conducted for subsequent calls in respect of shares issued and partly paid.

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

Applications Received from Foreign Brokers.

**123.**—(1) Where multiple family applications are received supported by one cheque and the aggregate subscription price is US \$1,000 or more; and \$1,000 or more for an individual person, then identification evidence will not be required for—

Multiple Family Applications.

(a) a spouse or any other person whose surname and address are the same as those of the applicant who has signed the cheque;

(b) a joint account holder ; or

(c) 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) Identification evidence of the signatory of the financial instrument shall be required for any multiple family applications for more than \$1,000 or its equivalent; or as per the tiered KYC directive issued by the CBN, where such application is supported by a cheque signed by someone whose name differs from that of the applicant.

(3) Other monetary amounts or more shall, from time to time, be stipulated by any applicable money laundering legislation and guidelines.

(4) Where an application is supported by a financial institution's branch cheque or brokers' draft, the applicant shall state the name and account number from which the funds were drawn –

(a) on the front of the cheque ;

(b) on the back of the cheque together with a branch stamp ; or

(c) attaching other supporting documents.

PART XIII—LINKED TRANSACTIONS, FOREIGN ACCOUNTS AND INVESTMENT

Linked  
Transac-  
tions.

124.—(1) Where a person handling applications that a number of single applications under \$1,000 or its equivalent in different names are linked, such as payments from the same financial institution account apart from the multiple family applications above, identification evidence shall be obtained in respect of parties involved in each single transaction.

(2) Installment payment issues shall be treated as linked transactions where it is known that total payments will amount to \$1,000 or its equivalent or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or guidelines; and either from the beginning or when a particular point has been reached, identification evidence shall be obtained.

(3) An application that is believed to be linked with money laundering shall be processed on a separate batch for investigation after allotment and registration have been completed.

(4) The returns with the documentary evidence shall be rendered to the NFIU accordingly.

(5) Copies of the supporting cheques, application forms and any repayment-cheques shall 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.

**125.—**(1) Where a customer wishes to open a Domiciliary Account (DA) or make a wholesale deposit by means of cash or inter-bank transfer, a financial institution shall obtain identification evidence in accordance with the requirements for private individuals, companies or professional intermediaries operating on behalf of third parties as appropriate.

Foreign  
Domiciliary  
Account  
(FDA).

(2) A financial institution shall satisfy itself that the transferring institution is regulated for money laundering prevention in its country of origin.

**126.—**(1) Precautions shall be taken in relation to requests to hold boxes, parcels and sealed envelopes in a safe custody.

Safe  
Custody  
and Safety  
Deposit  
Boxes.

(2) Where such facilities are made available, the identification procedures set out in these Regulations shall be followed, depending on the type of individual involved or risks associated with the business relationship.

**127.** Where a customer's identity was not properly obtained as contained in these Regulations and the requirements for Account Opening Procedure, a financial institution shall re-establish the customer's identity in line with the provisions of these Regulations.

Customer's  
Identity Not  
Properly  
Obtained.

**128.** Identification evidence shall not be required where the applicant for business is a Nigerian financial institution or person covered and persons regulated by the requirements of these regulations.

Exemption  
from  
Identification  
Procedures.

**129.—**(1) 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 such as walk in customers, present a high risk for money laundering purposes.

One-off  
Cash  
Transaction,  
Remittances  
and Wire  
Transfers.

(2) Adequate procedures shall be established to record the transaction and relevant identification evidence taken; and where such transactions form a regular part of the financial institution's business, the limits for requiring identification evidence of US \$ 1,000 or its equivalent for foreign transfers shall be observed.

**130.** 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 identification requirements shall be obtained before the proceeds are paid to him or be re-invested on his behalf in accordance with the relevant provision of these Regulations.

Re-  
investment  
of Income.

**131.—**(1) The Central Bank of Nigeria may, as it considers appropriate, amend or revoke the provisions of these Regulations which amendment or revocation shall be published in the *Gazette*.

Amendment  
or  
revocation  
of these  
Regulations

(2) The Central Bank of Nigeria (Anti – Money Laundering/Combating the Financing of Terrorism (AML/CFT) Regulations, 2009 (as amended) is hereby revoked.



(3) The revocation of the Regulations specified in sub-regulation (2) of this regulation shall not affect anything done or purported to be done under or pursuant to these Regulations.

Interpreta-  
tion :-

**132.—In these Regulations—**

'*AMCLO*' means Anti-Money Laundering Compliance Officer ;

'*Applicant for Business*' means a 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*' means a transfer comprising a number of individual wire transfers that are being sent to the same financial institution, but may or may not be ultimately intended for different persons ;

'*BDC*' means Bureau De Change ;

'*Beneficial owner*' includes a natural person who ultimately owns or controls a customer or a person on whose behalf a transaction is being conducted and the persons who exercise ultimate control over a legal person or arrangement ;

'*Beneficiary*' includes a natural person who receives charitable, humanitarian or other types of assistance through the services of a Non-Profit Organization (NPO), all trusts other than charitable or statutory permitted non-charitable trusts which may include the settlor, and a maximum time, known as the perpetuity period, normally of 100 years ;

'*Business Relationship*' means any arrangement between the financial institution and the applicant for business the purpose of which 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-border transfer*' means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element ;

'*Designated categories of offences*' includes—

- (a) participation in an organized criminal group and racketeering;
- (b) terrorism, including terrorist financing ;
- (c) trafficking in human beings and migrant smuggling ;
- (d) sexual exploitation, including sexual exploitation of children ;
- (e) illicit trafficking in narcotic drugs and psychotropic substances ;
- (f) illicit arms trafficking ;
- (g) illicit trafficking in stolen and other goods ;
- (h) corruption and bribery ;
- (i) fraud ;

- (j) counterfeiting currency ;
- (k) counterfeiting and piracy of products ;
- (l) environmental crime ;
- (m) murder, grievous bodily injury ;
- (n) kidnapping, illegal restraint and hostage-taking ;
- (o) robbery or theft ;
- (p) smuggling (including in relation to customs and excise duties and taxes ;
- (q) tax crimes (related to direct taxes and indirect taxes) ;
- (r) extortion ;
- (s) forgery ;
- (t) piracy ;
- (u) insider trading and market manipulation ; and
- (v) all other predicate offences as contained in section 15 of Money Laundering (Prohibition) Act, 2011 (as amended).

*“Designated non-financial businesses and professions”* includes any institution as designated by the Minister of Trade and Investment, MLPA, 2011 (as amended) and CBN AML/CFT Regulations, 2013 ;

*‘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 affect the wire transfer may be located in another jurisdiction ;

*‘False declaration or disclosure’* means failing to declare or, to misrepresent the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data requested for by the authorities ;

*‘FATF’* means Financial Action Task Force ;

*‘FATF Recommendations’* means the revised FATF Recommendations issued by the Financial Action Task Force ;

*‘Financial institutions’* include any person or entity who conducts as a business one or more of the following activities on behalf of a customer—

- (a) acceptance of deposits and other repayable funds from the public ;
- (b) lending ;
- (c) financial leasing ;
- (d) the transfer of money or value ;
- (e) issuing and managing means of payment such as credit and debit cards, cheques, travelers’ cheques, money orders and bankers’ drafts, electronic money ;

(f) financial guarantees and commitments ;

(g) trading in—

(i) money market instruments (cheques, bills, CDs, derivatives etc.) ;

(ii) foreign exchange ;

(iii) exchange, interest rate and index instruments ;

(iv) transferable securities ; and

(v) commodity futures trading ;

(h) participation in securities issues and the provision of financial services related to such issues ;

(i) individual and collective portfolio management ;

(j) safekeeping and administration of cash or liquid securities on behalf of other persons ;

(k) otherwise investing, administering or managing funds or money on behalf of other persons ;

(l) underwriting and placement of life insurance and other investment related insurance ; and

(m) money and currency changing.

The list is not exhaustive but subject to the definition contained in BOFIA 2004 ;

'*Financing of terrorism*' extends to all acts so defined under the Terrorism (Prevention) Act, 2011 (as amended) and the Terrorism Prevention ((Freezing of International Terrorists Funds and other Related Measures) Regulations, 2013 ;

'*Funds*' include assets of every kind, tangible or intangible, movable or immovable however acquired, legal documents or instruments in any form, electronic or digital evidencing title or interest in such assets, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit ;

'*Funds transfer*' means 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 and the originator and the beneficiary may be the same person ;

'*Legal arrangement*' means express trusts or other similar legal arrangements ;

'*Legal persons*' mean *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 ;

*'Money or value transfer services (MVTs)'* include financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer or through a clearing network to which the MVTs provider belongs and transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including *hawala, hundi, and fei-chen* ;

*'Non-profit/non-governmental Organization'* means a legal entity or organization 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'* means an 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'* 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'* means correspondent accounts that are used directly by third parties to transact business on their own behalf ;

*'Proceeds'* mean any property or value derived from or obtained, directly or indirectly, through the commission of an offence ;

*'Property'* means assets of every kind, whether corporeal or incorporeal, moveable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets ;

*'Risk'* means the risk of money laundering and/or terrorist financing ;

*'SCUML'* means Special Control Unit against Money Laundering in the Federal Ministry of Trade and Investment ;

*'Settlers'* Settlers include persons or companies who transfer ownership of their assets to trustees by means of a trust deed and where the trustees have some discretion as to the investment and distribution of the trust's 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'* 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 service group that is subject to effective consolidated supervision ;

'Physical presence' means meaningful mind and management located within a country and the existence simply of a local agent or low level staff does not constitute physical presence ;

'Terrorist' has the same meaning as in Terrorism (Prevention) Act, 2011 (as amended) ;

'Terrorist act' has the same meaning as in Terrorism (Prevention) Act, 2011 (as amended) ;

'Terrorist organization' has the same meaning as in Terrorism (Prevention) Act, 2011 (as amended) ;

'Terrorist property' includes a property which—

(a) has been, is being or is likely to be used for any act of terrorism ;

(b) has been, is being or is likely to be used by a proscribed organization ;

(c) is the proceeds of an act of terrorism ; and

(d) is provided or collected for the pursuit of or in connection with an act of terrorism ;

'Those who finance terrorism' include 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 and 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 be used, in full or in part, in order to carry out terrorist acts ;

'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, or a custodian trustee, who holds the assets to the order of the managing trustees ;

'Unique identifier' means any unique combination of letters, numbers or symbols that refers to a specific originator ; and

'Wire transfer' means any transaction carried out on behalf of an originator both natural and legal person, 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; where the originator and the beneficiary may be the same person.

Citation.

133. These Regulations may be cited as Central Bank of Nigeria (Anti-Money Laundering and Combating Financing of Terrorism for Banks and Other Financial Institutions in Nigeria), Regulations, 2013.

## SCHEDULES

## SCHEDULE I—SANCTIONS AND PENALTIES

## SANCTIONS

Sections 15 and 16 of the Money Laundering (Prohibition) Act, 2011 (as amended) provide for fines or term of imprisonment or both upon committing money laundering or aiding and abetting money laundering activities. The administrative sanctions outlined in this document will be imposed consequent upon the examination of a financial institution and observance of contraventions by CBN Examiners and other agencies.

In determining the sanctions to apply, all the circumstances of the case will be taken into account, including -

- |  |  |
|--|--|
| <p>1.—(a) Whether the contravention was deliberate, dishonest or reckless ;</p> <p>(b) The duration and frequency of the contravention ;</p> <p>(c) The amount of any benefit gained or loss avoided due to the contravention ;</p> <p>(d) Whether the contravention reveals serious or systemic weaknesses of the management systems or internal rules relating to all or part of the business ; and</p> <p>(e) The nature and extent of any AML/CFT crime facilitated, occasioned or otherwise attributable to the contravention—</p> <p>(i) whether there are a number of smaller issues, which individually may not justify administrative sanction, but which do so when taken collectively ; and</p> <p>(ii) Any potential or pending criminal proceedings in respect of the contravention which will be prejudiced or barred if a monetary penalty is imposed pursuant to the Administrative Sanctions Procedure.</p> | <p>Nature and seriousness of contravention/exception(s) observed.</p>  |
| <p>2.—(a) How quickly, effectively and completely the financial institution or person concerned in its management brought the contravention to the attention of the CBN or any other relevant regulatory authority ;</p> <p>(b) The degree of co-operation with CBN Examiners or other agency provided during the examination ;</p> <p>(c) Any remedial steps taken since the contravention was identified, including: taking disciplinary action against staff involved (where appropriate); addressing any systemic failures; and taking action designed to ensure that similar problems do not arise in the future ;</p> <p>(d) The likelihood that the same type of contravention will reoccur if no administrative sanction is imposed ; and</p> <p>(e) Whether the contravention was admitted or denied.</p>   | <p>The conduct of the regulated financial institution or person concerned in its management after the contravention.</p> |

General  
considerations.

3. The previous record of the financial institution or person concerned in its management :

(a) Whether CBN has taken any previous action resulting in a settlement, sanctions or whether there are relevant previous criminal convictions ;

(b) Whether the financial institution or person concerned in its management has previously been requested to take remedial action ; and

(c) General compliance history.

4.—(a) Prevalence of the contravention ;

(b) Action taken by CBN in previous similar cases ; and

(c) Any other relevant consideration.

**PENALTIES**

The penalties that the CBN shall apply for contraventions of the MLPA 2011 (as amended), Terrorism Prevention Act (TPA), 2011 (as amended), Terrorism Prevention (Freezing of International Terrorists Funds and Other Related Measures) Regulations, 2013 and CBN AML/CFT Regulation 2013 (comprise revocation or suspension of the operating license, non-monetary and financial penalties) shall be as permitted by BOFIA or any other relevant laws or any regulations issued by the Attorney General of the Federation.

## SCHEDULE II

## INFORMATION TO ESTABLISH IDENTITY

1.—(1) For natural persons, the following information shall be obtained, where applicable—

Natural  
Persons.

(a) legal name and any other names used (such as maiden name) ;

(b) permanent address (full address shall be obtained and the use of a post office box number only, is not sufficient) ;

(c) telephone number, fax number, and e-mail address ;

(d) date and place of birth ;

(e) nationality ;

(f) occupation, public position held and name of employer ;

(g) 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 ;

(h) type of account and nature of the banking relationship ; and

(i) signature.

(2) The Financial Institution shall verify the information referred to in paragraph 1 of this Appendix, by at least one of the following methods—

(a) confirming the date of birth from an official document (such as birth certificate, passport, identity card, social security records);

(b) confirming the permanent address (such as utility bill, tax assessment, bank statement, a letter from a public authority) ;

(c) contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (such as a disconnected phone, returned mail, or incorrect e-mail address shall warrant further investigation);

(d) confirming the validity of the official documentation provided through certification by an authorized person such as embassy official, notary public.

(3) 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.

(4) A Financial Institution shall apply equally, effective customer identification procedures for non-face-to-face customers as for those available for interview.

(5) A Financial Institution shall make an initial assessment of a customer's risk profile from the information provided and particular attention shall be focused on those customers identified as having a higher risk profile and any additional inquiries made or information obtained in respect of those customers shall include—



(a) evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits ;

(b) personal reference by an existing customer of the same institution ;

(c) prior bank reference and contact with the bank regarding the customer ;

(d) source of wealth ; and

(e) verification of employment and public position held where appropriate.

(6) The customer acceptance policy shall 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.

Institutions.

2. The term "Institution" includes any entity that is not a natural person and in considering the customer identification guidance for the different types of institutions, particular attention shall be given to the different levels of risk involved.

Corporate Entities.

3.—(1) For corporate entities such as corporations and partnerships, the following information shall be obtained—

(a) name of the institution ;

(b) principal place of the institution's business operations ;

(c) mailing address of the institution ;

(d) contact telephone and fax numbers ;

(e) some form of official identification number, if available such as tax identification number ;

(f) the original or certified copy of the certificate of incorporation and memorandum and articles of association ;

(g) the resolution of the board of directors to open an account and identification of those who have authority to operate the account ; and

(h) nature and purpose of business and its legitimacy.

(2) The Financial Institution shall verify the information referred to in paragraph 7(1) of this Schedule by at least one of the following methods :

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

(b) 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 ;

(c) 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 ;

(d) utilising an independent information verification process, such as accessing public and private databases ;

- (e) obtaining prior bank references ;
- (f) visiting the corporate entity ; and
- (g) contacting the corporate entity by telephone, mail or e-mail.

(3) The Financial Institution shall 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.

4.—(1) For Corporations or Partnerships, the principal guidance is to look behind the institution to identify those who have control over the business and the company's or partnership's assets, including those who have ultimate control.

Corporation  
or  
Partnership.

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

(3) What constitutes control for this purpose shall 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 authorization, and who would be in a position to override internal procedures and control mechanisms.

(4) For partnerships, each partner shall be identified and it shall identify immediate family members that have ownership control.

(5) Where a company is listed on a recognized stock exchange or is a subsidiary of a listed company, the company itself may be considered to be the principal to be identified and where a listed company is effectively controlled by an individual, group of individuals, another corporate entity or trust, those in control of the company are considered to be principals and shall be identified accordingly.

5.—(1) The following information shall be obtained in addition to that required to verify the identity of the principals in respect of Retirement Benefit Programmes, Mutual or Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, Trusts and Foundations and Professional Intermediaries :

Other  
Types of  
Institution.

- (a) name of account ;
- (b) mailing address ;
- (c) contact telephone and fax numbers ;
- (d) some form of official identification number, such as tax identification number ;
- (e) description of the purpose or activities of the account holder as stated in a formal constitution ; and
- (f) copy of documentation confirming the legal existence of the account holder such as register of charities.

(2) The Financial Institution shall verify the information referred to in paragraph 6 (1) of this Schedule by at least one of the following—

- (a) obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted ;
- (b) obtaining prior bank references ; and
- (c) accessing public and private databases or official sources.

Retirement  
Benefit  
Programme.

6. 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 shall be considered as principals and the financial institution shall take steps to verify their identities.

Mutual or  
Friendly,  
Cooperative  
and  
Provident  
Societies.

7. Where Mutual or Friendly, Cooperative and Provident Societies is an applicant for an account, the principals to be identified shall 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.

Charities,  
Clubs and  
Associations.

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

(2) In all cases, independent verification shall be obtained that the persons involved are true representatives of the institution and independent confirmation shall also be obtained of the purpose of the institution.

Trusts and  
Foundations.

9.—(1) When opening an account for a Trust, the financial institution shall 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.

(2) Beneficiaries shall be identified when they are defined. In the case of a foundation, steps shall be taken to verify the founder, the managers or directors and the beneficiaries.

Professional  
Intermediaries.

10.—(1) Where a professional intermediary opens a client account on behalf of a single client, that client shall be identified and Professional intermediaries shall open "pooled" accounts on behalf of a number of entities; and where funds held by the intermediary are not co-mingled but there are "sub-accounts" which shall be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary shall be identified.

(2) Where the funds are co-mingled, the financial institution shall look through to the beneficial-owners but there may be circumstances that the Financial Institution may not look beyond the intermediary such as when the intermediary is subject to the same due diligence standards in respect of its client base as the financial institution.

(3) 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 shall be considered as principals and the Financial Institution shall take steps to identify:

- (a) the fund itself ;
- (b) its directors or any controlling board, where it is a company ;
- (c) its trustee, where it is a unit trust ;
- (d) its managing (general) partner, where it is a limited partnership ;
- (e) account signatories ; and
- (f) any other person who has control over the relationship such as fund administrator or manager.

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

(5) Intermediaries shall be treated as individual customers of the financial institution and the standing of the intermediary shall be separately verified by obtaining the appropriate information itemized above.

SCHEDULE III

MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS"

Suspicious Transactions "Red Flags".

1. Potential Transactions which may be referred to as 'Red Flags' shall be categorized as follows—

(a) potential transactions perceived or identified as being suspicious which among others shall include :

(i) transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed ;

(ii) transactions involving shell companies ;

(iii) transactions with correspondents that have been identified as higher risk ;

(iv) large transaction activities involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered ; and

(v) transaction activities 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.

(b) money laundering using cash transactions which among others shall include :

(i) significant increases in cash deposits of an individual or corporate entity without apparent cause, particularly where such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer;

(ii) unusually large cash deposits made by an individual or a corporate entity whose normal business is transacted by cheques and other non-cash instruments ;

(iii) frequent exchange of cash into other currencies ;

(iv) customers who deposit cash through many deposit slips such that the amount of each deposit is relatively small but the overall total is quite significant ;

(v) customers whose deposits contain forged currency notes or instruments ;

(vi) customers who regularly deposit cash to cover applications for bank drafts ;

(vii) customers making large and frequent cash deposits with cheques always drawn in favour of persons not usually associated with their type of business ;

(viii) customers who request to exchange large quantities of low denomination banknotes for those of higher denominations ;

(ix) branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors ; and

(x) customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(c) money laundering using deposit accounts, especially where they are inconsistent with a customer's legitimate business, which among others shall include :

(i) minimal, vague or fictitious information provided by a customer that the money deposited in the bank is not in a position to be verified ;

(ii) 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 ;

(iii) a prospective customer who does not have a local residential or business address and there is no apparent legitimate reason for opening a bank account ;

(iv) customers maintaining multiple accounts in a bank or in different banks for no apparent legitimate reason or business rationale whether the accounts are in the same names or have different signatories ;

(v) 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 ;

(vi) accounts with large volumes of activity but low balances or frequently overdrawn positions ;

(vii) customers making large deposits and maintaining large balances with no apparent rationale ;

(viii) customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash transactions from those accounts to other accounts, locally or internationally, leaving only small balances which typically are transactions that are not consistent with the customers' legitimate business needs ;

(ix) Sudden and unexpected increase in account activity or balance arising from deposit of cash and non-cash items which typically are accounts opened with small amounts but subsequently increase rapidly and significantly ;

(x) accounts used as temporary repositories for funds that are subsequently transferred outside the bank to foreign accounts which accounts often have low activity ;

(xi) 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 ;

(xii) customer requests for disbursement of the proceeds of certificates of deposit or other investments by multiple cheques, each below the stipulated reporting threshold ;

(xiii) retail businesses which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs ;

(xiv) frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks ;

(xv) substantial cash deposits by professional customers into client, trust or escrow accounts ;

(xvi) 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 ;

(xvii) large cash withdrawals from a previously dormant or inactive account, or from an account which has just received an unexpected large credit from abroad ;

(xviii) greater use of safe deposit facilities by individuals, particularly the use of sealed packets which are deposited and soon withdrawn ;

(xix) 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 where the deposits are promptly transferred between other client company and trust accounts ;

(xx) large numbers of individuals making payments into the same account without adequate explanation ;

(xxi) high velocity of funds that reflects the large volume of money flowing through an account ;

(xxii) an account opened in the name of a money changer that receives deposits ; and

(xxiii) an account operated in the name of an off-shore company with structured movement of funds.

(d) trade-based money laundering which among others shall include—

(i) over and under-invoicing of goods ;

(ii) multiple invoicing of goods and services ;

(iii) over and under-invoicing of goods and services ;

(iv) 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 ;

(v) transfer pricing ;

(vi) transaction structure which appear unnecessarily complex and designed to obscure the true nature of the transaction ;

(vii) items shipped which are inconsistent with the nature of the customer's normal business and transaction which lack an obvious economic rationale ;

(viii) customer requests payment of proceeds to an unrelated third party; and

(ix) significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

(e) lending activities which among others include :

(i) customers who repay problem loans unexpectedly ;

(ii) a customer who is reluctant or refuses to state the purpose of a loan or the source of repayment or provides a questionable purpose or source of repayment ;

(iii) loans secured by pledged assets held by third parties unrelated to the borrower ;

(iv) loans secured by deposits or other readily marketable assets, such as securities particularly when owned by apparently unrelated third parties ;

(v) loans made for or paid on behalf of a third party with no reasonable explanation ; and

(vi) loans lacking 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) ;

(f) terrorist financing "red flags" which among others include :

(i) persons involved in currency transactions who 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 such as student, unemployed, or self-employed ;

(ii) 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 ;

(iii) 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 ;

(iv) where large numbers of incoming or outgoing funds transfers take 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 ;

(v) where the stated occupation of the customer is inconsistent with the type and level of account activity ;



(vi) where 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 ;

(vii) 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 ;

(viii) foreign exchange transactions which 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 ; and

(ix) 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.

(g) other unusual or suspicious activities which among others include :

(i) where employee exhibits a lavish lifestyle that cannot be justified by his/her salary ;

(ii) where employee fails to comply with approved operating guidelines, particularly in private banking ;

(iii) where employee is reluctant to take a vacation ;

(iv) 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 ;

(v) 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 ;

(vi) customer uses a personal account for business purposes ;

(vii) where official embassy business is conducted through personal accounts ;

(viii) where embassy accounts are funded through substantial currency transactions ; and

(ix) where embassy accounts directly fund personal expenses of foreign nationals.

MADE at Abuja this 29th Day of August, 2013.

SANUSI LAMIDO SANUSI  
Governor of the Central Bank of Nigeria

EXPLANATORY NOTE

*(This note does not form part of these Regulations  
but is intended to explain its purports)*

These Regulations seek to ensure that the Banking Industry and other financial institutions comply with subsisting Anti-Money Laundering and Combating the Financing of Terrorism Legislation.

12/1/18