CENTRAL BANK OF NIGERIA

SUPERVISORY FRAMEWORK FOR PAYMENT SERVICE BANKS

JULY 2021

Contents

PREAMBLE

The Central of Nigeria (CBN), hereafter called the Bank, has introduced various initiatives to enhance access to financial services for the unbanked population of the Nigerian economy. This included the deployment and facilitation of the use of technology to drive the financial inclusion ambition of the CBN. To this end, the Guidelines for the Licensing and Regulation of Payment Service Banks (PSBs) in Nigeria was issued in 2018 (revised 2020).

The Payment Service Banks are expected to leverage on technology to provide services that would be easily accessed by the unbanked population and those who are in hard-to-reach areas of the country. This framework hereby provides a set of regulations that are targeted at streamlining the operations of Payment Service Banks, ensuring transparency in their operations as well as ensuring adequate customer protection. The framework focuses on corporate governance, risks management of the PSBs, and safety of funds to the consumers of the Payment Service Banks' products. This Framework also aims to ensure that sound risk management practices are embedded in the operations of the Payment Service Banks.

Payment Service Banks are required to comply with relevant extant regulations and CBN's prudential guidelines and circulars which are issued periodically.

1.0 STRUCTURE OF PAYMENT SERVICE BANKS

The Payment Service Banks shall use the words “Payment Service Bank” in its name to differentiate it from other banks. However, the name of a PSB shall not include any word that links it to its parent company or promoter.

Also, they shall:

i. Operate mostly in the rural areas and unbanked locations targeting financially excluded persons, with not less than 25% financial service touch points in such rural areas as defined by the CBN from time to time;

ii. Enter into direct partnership with card scheme operators. Such cards shall not be eligible for foreign currency transactions;

iii. Deploy ATMs in some of these areas;

iv. Deploy Point of Sale devices;

v. Be at liberty to operate through banking agents (in line with the CBN’s Guidelines for the Regulation of Agent Banking and Agent Banking Relationships in Nigeria);

vi. Roll out agent networks with the prior approval of the CBN;

vii. Use other channels including electronic platforms to reach-out to its customers;

viii. Establish coordinating centres in clusters of outlets to superintend and control the activities of the various financial service touch points and banking agents;

ix. Be technology-driven and shall conform to best practices on data storage; security and integrity; and

x. Set up consumer help desks (physical and online) at its main office and coordinating centres.

2.0 PERMISSIBLE AND NON-PERMISSIBLE ACTIVITIES

2.1 Permissible Activities

Payment Service Banks shall carry out the following activities:

i. Accept deposits from individuals and small businesses, which shall be covered by the deposit insurance scheme;

ii. Carry out payments and remittances (including inbound cross-border personal remittances) services through various channels within Nigeria;

iii. Sale of foreign currencies realized from inbound cross-border personal remittances to authorized foreign exchange dealers;

iv. Without prejudice to 2.1 ‘i’ and ‘ii’ above, comply with provisions of the extant Foreign Exchange Regulations of the CBN;

v. Issue debit and pre-paid cards on its name;

vi. Operate electronic wallet;

vii. Render financial advisory services;

viii. Invest in FGN and CBN securities; and

ix. Carry out such other activities as may be prescribed by the CBN from time to time.

2.2 Non-Permissible Activities

Payment Service Banks shall not carry out the following activities:

i. Grant any form of loans, advances and guarantees (directly or indirectly). They may lend to their employees in line with their employee loan policy, subject to the approval of their Board;

ii. Accept foreign currency deposits;

iii. Deal in the foreign exchange market except as prescribed in 4.1 (ii & iii) above;

iv. Insurance underwriting;

v. Undertake any other transaction which is not prescribed by this Guidelines;

vi. Accept any closed scheme electronic value (e.g. airtime) as a form deposit or payment;

vii. Establish any subsidiary except as prescribed in the CBN Regulation on the Scope of Banking and Ancillary Matters, No 3, 2010.

3.0 OWNERSHIP AND LICENSING REQUIREMENTS

This shall be as provided in Sections 5.0 and 6.0 of the Guidelines for Licensing and Regulation of Payment Service Banks (2020), or the extant Regulation.

4.0 CORPORATE GOVERNANCE

To ensure sound corporate governance culture, all Payment Service Banks shall adopt structures and practices that will protect the interest of all stakeholders. To this end all

Payment Service Banks shall comply with the following specific provisions, in addition to the provisions of Corporate Governance Guidelines for Payment Service Banks.

4.1 BOARD STRUCTURE AND COMPOSITION

(a) The Procedure for appointment to the Board shall be formal, transparent and documented in the Board Charter.

(b) Members of the Board of Directors shall be appointed by the shareholders of the PSB and approved by the CBN.

(c) The size of the Board of any PSB shall be limited to a minimum of five (5) and a maximum of thirteen (13).

(d) The Board of a PSB shall have at least one (1) Non-Executive Director as Independent Director. For publicly listed Payment Service Banks, the provisions of CAMA 2019 shall apply.

(e) The Board shall reflect diversity in its composition. Both genders shall be adequately represented on the Board.

(f) Members of the Board shall be qualified persons of proven integrity and shall be knowledgeable in business, financial matters and/or information technology.

(g) At least two (2) non-executive directors shall be required to have banking or related financial industry experience.

(h) Not more than two members of an extended family shall be on the Board of a Payment Service Bank, its subsidiary or Financial Holding Company (HoldCo) at the same time. Furthermore, only one extended family member can occupy the position of either MD/CEO, Chairman or ED at any point in time.

(i) The expression 'extended family' in this Framework includes director's spouse, parents, children, siblings, cousins, uncles, aunts, nephews, nieces, in-laws and any other construed relationship as to be determined by the CBN.

(j) Prospective directors on the Board of a Payment Service Bank are required to disclose board memberships on boards of other organisations, and current directors shall notify the Board of prospective appointments on boards of other organisations. The PSB shall obtain CBN's approval in both instances.

(k) A director (except an INED) of a Payment Service Bank may be appointed a Non-Executive Director only within a Holding Company or a Group structure which the Payment Service Bank is a member, provided the aggregate number of directors from the Payment Service Bank at any point in time shall not exceed 30 per cent of the membership of the Board of the holding company and vice versa.

(l) The position of an Executive Vice Chairman shall not be recognized in the board structure of any Payment Service Bank.

(m) A director on the Board of a Payment Service Bank shall only be presented for reappointment at the last AGM before the expiration of the tenure of such a director.

4.2 BOARD AND BOARD COMMITTEES MEETINGS

(a) The schedules of the Board and its committees' meetings shall be proposed and approved by the Board ahead of each financial year.

(b) To effectively perform its oversight function and monitor management's performance, the Board and its Committees shall meet at least once every quarter.

(c) The meeting of the Board and its committees shall be held at a specified location.

(d) The quorum for the Board and its committees' meetings shall be two-thirds of members, majority of whom shall be NEDs.

(e) Every Director is required to attend all meetings of the Board and Board Committees he or she is a member. In order to qualify for reappointment, a director must have attended at least two-thirds of all Board and Board Committee meetings.

(f) Minutes of meetings of the Board and its Committees shall be properly written in English language, adopted and signed off by the Board/Committee Chairman and Secretary, pasted in the minute's book and domiciled at the PSB's Head Office.

4.3 BOARD EVALUATION

(a) There shall be an annual appraisal of the Board, its Committees, Chairman and individual Directors covering all aspects of the Boards' structure, composition, responsibilities, processes and relationships or as may be prescribed by the CBN from time to time.

(b) The Board appraisal shall be conducted by an Independent Consultant with adequate experience, knowledge and competence. The report of the annual Board appraisal shall be forwarded to the CBN by March 31st following the end of every accounting year and be presented to shareholders at the AGM.

5.0 APPROVED PERSONS REGIME & COMPETENCY FRAMEWORK

All Payment Service Banks shall comply with the provisions of the Assessment Criteria for Approved Persons' Regime for Payment Service Banks, which clearly stipulates the roles, responsibilities, minimum qualifications and/or experience for principal officers of Payment Service Banks.

The roles, responsibilities and minimum qualifications for principal officers of Payment Service Banks are as follows.

5.1 CHAIRMAN OF THE BOARD

a. Responsibilities

The Chairman (Chair) of the Board shall be responsible for:

i. Setting the board's agenda and ensuring that adequate time is available for discussion of all agenda items, in particular strategic issues. The Chair shall also promote a culture of openness and debate by facilitating the effective contribution of Non-Executive Directors and ensuring constructive relations between executive and Non-Executive Directors.

ii. Evaluating the performance of the Board and its sub-committees;

iii. Leading the development and overseeing the implementation of the Payment Service Bank's policies and procedures for the induction, training and development of all directors.

iv. Leading the development of the Payment Service Bank's culture by the bank's Board.

v. Overseeing the assessment of fitness and propriety of the Payment Service Bank's INEDs.

vi. Chairing and overseeing the performance of the Nomination Committee.

b. Qualifications

i. A first degree or its equivalent in any discipline

ii. Membership of Institute of Directors or any other relevant and recognized professional institute.

c. Years of Experience

i. Relevant experience in business/executive role

ii. 15 years post-graduation experience

iii. 5 years board experience in Financial Services, Electronic Payments and ICT Industry

5.2 MANAGING DIRECTOR/CHIEF EXECUTIVE OFFICER (MD/CEO)

a) Responsibilities

The MD/CEO shall be responsible for:

i. **Allocation of all Prescribed Responsibilities:** He/she shall consider and agree 'Prescribed Responsibilities' for all Executive Directors and other members of staff who report to the MD/CEO, ensuring that these responsibilities are readily understood, shared, implemented, and monitored on a regular basis.

ii. **Overseeing the adoption of the Payment Service Bank's culture in the day-to-day management of the bank:** He/she shall entrench organizational culture in all the areas of the Payment Service Bank; directs the development and implementation of all policies and procedures that support the cultural objectives of the Payment Service Bank in line with the tone set by the Board.

iii. **Overseeing the performance of the Risk function and ensuring the integrity and independence of the Payment Service Bank's risk function:** He/she shall have a line management responsibility for the Executive Director, Risk. The MD/CEO shall delegate implementation of the Risk function to the Executive Director, Risk.

iv. **The production and integrity of the Payment Service Bank's financial information:** He/she shall have a line management responsibility for the Chief Financial Officer, and shall ensure that the setting, communication, and delivery of the bank's total expenditure and income budget is in line with the Payment Service Bank's budget as set by the Board. The MD/CEO is also responsible for ensuring regular updates to the Board on the Payment Service Bank's financial information.

v. **The development and maintenance of the bank's business model and strategy:** He/she shall be responsible for setting the Payment Service Bank's overall strategy and business model (subject to approval by the Board).

The MD/CEO shall ensure that business strategies are communicated internally and implemented by all staff and ensure that regular updates are made available to all relevant stakeholders.

vi. **Talent management:** He/she shall be responsible for developing and delivering a talent management plan for the Payment Service Bank, including regular updates to the Board on succession plans for the senior management team.

vii. **Budget:** He/she shall have line management responsibility for the Chief Financial Officer, and shall ensure that the setting, communication, and delivery of the bank's total expenditure and income budget is in line with the budget as approved by the Board.

viii. **Risk:** He/she shall have line management responsibility for the Executive Director, Risk, and shall ensure that the bank has a risk profile consistent with ensuring the delivery of its objectives.

b) Qualifications

A minimum of first degree or its equivalent in any discipline plus a higher degree or professional qualification in any business-related discipline or IT related disciplines.

c) Years of Experience

Candidate shall have a minimum of twenty (20) years post-graduate experience, out of which at least fifteen (15) years shall be in the banking industry and electronic payments service and financial inclusion related jobs, and at least 5 years as a senior management staff. The expected experience should span agent network development and expansion, customer service, business development and compliance.

5.3 DEPUTY MANAGING DIRECTOR/EXECUTIVE DIRECTORS

a. Responsibilities

The Deputy Managing Director/Executive Directors shall:

i. Oversee all operations, functions and activities under his/her purview;

ii. Be responsible for giving the proper strategic direction and implementing board policies as well as ensuring function(s) under his/her purview operates efficiently and effectively to meet business goals.

b. Qualification

A minimum of first degree or its equivalent in any discipline plus a higher degree or professional qualification in any business/IT related discipline.

c. Years of Experience

Candidate shall have a minimum of eighteen (18) years post-graduate experience, out of which at least 12 must have been in banking, electronic payments and financial inclusion related jobs, and at least 2 as General Manager. Evidence of experience in diverse areas such as agent network development, customer service, banking operations and compliance shall be provided for the candidate.

A Deputy Managing Director/Executive Director must have served for a minimum of two (2) years for him/her to be qualified for appointment as a Managing Director.

5.4 NON-EXECUTIVE DIRECTORS (OTHER THAN THE CHAIRMAN)

a. Responsibilities

Non-Executive Directors shall carry out the following responsibilities:

i. **Strategy** - Non-Executive Directors shall constructively contribute to the process of developing proposals on strategy.

ii. **Performance** - Non-Executive Directors shall scrutinize the performance of management in meeting agreed goals and objectives and monitor the reporting of performance.

iii. **Risk** - Non-Executive Directors shall satisfy themselves on the integrity of financial information and that financial controls and systems of risk management are robust.

iv. **People** - Non-Executive Directors shall as members of the Remuneration Committee determine appropriate levels of remuneration for Executive Directors. They should have a prime role in succession planning, appointment, and removal of Executive Directors.

b. Qualifications

i. A first degree or its equivalent in any discipline

ii. Membership of Institute of Directors or any other relevant and recognized institute

c. Years of Experience

i. A minimum of 15 years' post- graduate experience;

ii. Proven skills and competencies in their fields;

iii. Knowledge of the operations of banks/electronic payments business and relevant laws and regulations guiding the financial services industry; and

iv. Ability to interpret financial statements and make meaningful contributions to board deliberations;

In considering nominees with limited academic/professional qualifications and industry experience, the CBN shall take into account the following:

i. Direct involvement of the nominee in an established business enterprise with total assets of not less than N300million.

ii. The quality of courses and seminars attended in the last five (5) years prior to his nomination.

iii. The size, scope and complexity of the institution;

iv. The relevant experience and qualifications of other Board members;

v. The existence and number of Independent Directors on the Board;

vi. An assurance that the proposed director(s) would be exposed to accelerated training over a short period of time; and

vii. Assignment of responsibilities commensurate with their experiences.

5.5 INDEPENDENT NON-EXECUTIVE DIRECTORS (INED)

a. Responsibilities

i. Be an anchor, as required, for views by other Non-Executive Directors on the performance of the Chairman

ii. Chair a formal annual session of the Nomination and Governance Committee members (excluding the Chairman) to agree the Chairman's objectives and review his performance

iii. Be responsible for appraising the Chairman's performance taking into account the views of Executive Directors and other stakeholders.

iv. Be the focal point for board members for any concerns regarding the Chairman, or the relationship between the Chairman and MD/CEO.

b. Qualification

i. A first degree or its equivalent in any discipline

ii. Membership of Institute of Directors or any other relevant and recognized professional institute.

c. Years of Experience

1. Independent Directors shall be appointed in accordance with:

i. The CBN's extant Guidelines for the Appointment of Independent Directors;

ii. The extant Corporate Governance for Payment Service Banks;

iii. Companies and Allied Matters Act (CAMA), 2020;

iv. Any other relevant law, rules and regulations issued from time to time by the CBN.

2. In particular, an Independent Director shall be a member of the Board of Directors who has no direct material relationship with the Payment Service

Bank or any of its officers, major shareholders, subsidiaries and affiliates; a relationship which may impair the director's ability to make independent judgments or compromise the director's objectivity in line with Corporate Governance best practices.

3. An Independent Director shall not:

i. beyond his services on the Board of a Payment Service Bank, provide financial, legal and/or consulting services to the institution or its subsidiaries/affiliates or had done so in the preceding 5 years;

ii. be a current or former employee who had served in the Payment Service Bank in the past and none of his immediate family members should be an employee or former staff of the Payment Service Bank at the senior management level in the preceding 5 years;

iii. be part of management, executive committee or board of trustees of an entity, charity or otherwise, supported by the Payment Service Bank;

iv. serve on the Board of a subsidiary or affiliate of the Payment Service Bank.

4. An Independent Director shall have:

i. sound knowledge of the operations of listed companies, the relevant laws and regulations guiding the industry,

ii. a minimum academic qualification of first degree or its equivalent with not less than 15 years of relevant working experience.

iii. proven skills and competencies in their fields.

5. In addition, the requirements for Non-Executive Directors stated above shall apply.

5.6 CHAIRMAN OF BOARD AUDIT AND RISK MANAGEMENT COMMITTEE (BARMC)

a. Responsibilities

The Chairman of BARMC shall be responsible for:

i. Chairing and overseeing the performance of BARMC.

ii. Ensuring and overseeing the integrity and independence of the Payment Service Bank's internal audit function (including the Head of Internal Audit).

iii. Ensuring the integrity, independence and effectiveness of the Payment Service Bank's policies and procedures on whistleblowing and ensuring staff that raise concerns are protected from detrimental treatment.

iv. Monitoring the integrity of the financial statements.

v. Overseeing the selection process for new external auditors.

vi. Approving the letter of appointment of the external auditor.

vii. Approving the remit and resources of the internal audit function and disclose in the Annual Report whether BARMC is satisfied that the internal audit function has appropriate resources.

viii. Reviewing and report on the effectiveness of the Payment Service Bank's risk framework, risk standards, risk management policies and systems of internal control.

b. Qualification

i. A first degree or its equivalent in any discipline

ii. Membership of Institute of Directors or any other relevant and recognized professional institute

c. Years of Experience

i. Relevant experience in business/executive role

ii. 15 years post-graduate experience

iii. 5 years board experience in Financial Services/Electronic Payments Industry

d. Mandatory Continuous Professional Training (MCPT)

For continued retention in the role, in addition to performance on the position, the Chairman, BARMC shall provide evidence of at least forty (40) hours of Mandatory Continuous Professional Training (MCPT) on Leadership, Strategic Management, Corporate Governance as well as specific areas of the board.

5.7 CHAIRMAN OF REMUNERATION COMMITTEE (REMCO)

a. Responsibilities

The Chairman of RemCo shall be responsible for:

i. Determining all matters relating to the remuneration, including pension benefits and costs, of the MD/CEO and Executive Directors.

ii. Advising the Board on major changes in remuneration structures within the Payment Service Bank, including pension benefits, and other remuneration matters specifically referred to it by the Board.

iii. Approving the remuneration report for inclusion in the Payment Service Bank's Annual Report.

b. Qualification

i. Minimum qualification:

ii. A first degree or its equivalent in any discipline

c. Years of Experience

i. Relevant experience in business/executive role

ii. 15 years post-graduation experience

iii. 5 years board experience in Financial Services Industry

5.8 CHAIRMAN OF NOMINATION COMMITTEE

a. Responsibilities

The Chairman, Nomination Committee shall:

i. Put in place a policy promoting diversity on the Board;

ii. Identify and recommend for approval, by the Board, candidates to fill Board vacancies, having evaluated the balance of knowledge, skills, diversity and experience of the Board;

iii. Prepare a description of the roles and capabilities for appointment, and assesses the time commitment required;

iv. Ensure representation on the Board is diverse and prepare a policy to ensure diversity in composition of Board members;

v. Periodically, and at least annually, assesses the structure, size, composition and performance of the Board and make recommendations to the Board with regard to any changes;

vi. Periodically and at least annually, assess the knowledge, skills and experience of individual members of the Board and of the Board collectively, and report this to the Board;

vii. Periodically review the policy of the Board for selection and appointment of senior management and make recommendations to the Board; and

viii. Ensure on an ongoing basis, that the Board's decision making is not dominated by any one individual or small group of individuals in a manner that is detrimental to the interest of the Payment Service Bank as a whole

b. Qualification

A first degree or its equivalent in any discipline

c. Years of Experience

A minimum of 15 years of experience within the financial services and electronic payments industry.

5.9 EXECUTIVE DIRECTOR (ED), RISK

a. Responsibilities

The ED, Risk shall:

i. Provide policy direction and oversight for the institution's second-line risk functions to ensure: that all material risks are identified, measured and reported; that those functions are appropriately involved in material risk management decisions; and that the Payment Service Bank has an effective risk management framework.

ii. Provide leadership, governance, and management necessary to identify, evaluate, mitigate, and monitor the Payment Service Bank's overall risk exposures.

b. Qualifications

i. A first degree or its equivalent in any discipline.

ii. Relevant postgraduate/professional certifications in risk management

c. Years of Experience

A minimum of eighteen (18) years post-graduate experience, out of which at least thirteen (13) years shall be in the banking industry with at least two (2) years as a general manager. Evidence of experience in diverse areas such as agent network development, customer service, banking operations and compliance shall be provided for the candidate.

5.10 EXECUTIVE COMPLIANCE OFFICER

a. Responsibilities

The Executive Compliance Officer (ECO) shall be an Executive Director and ensure compliance across the Payment Service Bank through oversight of the necessary control processes, policies, culture, and all relevant regulations by the CBN.

b. Qualifications

i. A first degree or its equivalent in any discipline

ii. Recognized professional certification will be an added advantage

c. Years of Experience

i. A minimum of eighteen (18) years post-graduate experience, out of which at least thirteen (13) years shall be in the banking industry with at least two (2) as a general manager.

ii. Evidence of experience in diverse areas such as agent network development, customer service, banking operations and compliance shall be provided for the candidate.

5.11 CHIEF FINANCIAL OFFICER (CFO) or whoever that has the overall

a. Responsibilities

The CFO shall be responsible for the following:

i. Finance

Financial control, budgeting, management reporting and analysis, statutory reporting and tax matters.

ii. The Payment Service Bank's capital and funding from a budget perspective.

The maintenance of the Payment Service Bank's capital and funding from a budget perspective is the responsibility of the CFO, who reports to the MD/CEO.

iii. The production and integrity of the Payment Service Bank's financial information and its regulatory reporting.

The CFO has responsibility for the production and integrity of the Payment Service Bank's financial information. The responsibility is shared with the MD/CEO and Chair of Board.

iv. Regulatory Returns

The CFO shall be responsible for periodic regulatory returns on financial matters to the CBN and any other regulator within the financial system (where required).

b. Qualifications

i. A first degree or equivalent in any discipline.

ii. Recognized professional certification such as ACCA, ACA, ANAN, CFA, etc.

c. Years of Experience

Minimum of 10 years post qualification experience in Finance & Performance Management role within the Financial Services Industry. Out of which at least 5 must have been at a senior management level.

5.12 HEAD, INTERNAL AUDIT

a. Responsibilities

The Head, Internal Audit shall be responsible for the preparation and delivery of an annual audit plan which is commensurate with business risk, evaluation of the effectiveness of internal controls, risk management and governance processes in all areas of the Payment Service Bank. The Internal Audit authority, role and responsibility shall be defined in the Board approved Internal Audit Charter.

b. Qualifications

i. A first degree or equivalent in any discipline.

ii. Recognized professional Accounting certification such as ACCA, ACA, etc.

c. Years of Experience

Minimum of 10 years' experience in the financial management/accounting function, 5 of which must be in senior position within the audit function

5.13 CHIEF RISK OFFICER

a. Responsibilities

The Chief Risk Officer (CRO) shall:

i. Develop Enterprise Risk Management Framework, practices, and policies to analyse and report enterprise risks, and to manage risks according to a Board approved enterprise risk management framework.

ii. Monitor and report on adherence to and consistency of strategic initiatives with Board-approved risk appetite framework, risk tolerances and risk profile.

iii. Ensure that the organization's risk management policies and strategies are in compliance with applicable regulations, rating agency standards, and strategic imperatives of the Payment Service Bank.

iv. Establish the Enterprise Risk Management architecture for the financial Payment Service Bank.

v. Monitor and analyze risks within the company's business units and reports on these risks to the Board Audit and Risk Management Committees

b. Qualifications

i. A first degree or its equivalent in any discipline

ii. Recognized professional certification will be an added advantage

c. Years of Experience

A Minimum of 15 years post qualification experience in risk management or related area within the Financial Services or Information Technology Industry, of which at least 7 must have been in the Banking Sector and 5 years must have been at senior management level.

5.14 CHIEF COMPLIANCE OFFICER

a. Responsibilities

The Chief Compliance Officer (CCO) shall:

i. Carry out a regular assessment of the adequacy of the Payment Service Bank's operational systems and controls to ensure that they continue to comply with laws and regulations.

ii. Implement and maintain (as approved by the Board) procedures sufficient to ensure compliance of the Payment Service Bank

iii. Provide guidance on steps that a Payment Service Bank can take to reduce the risk that its systems might be used to further financial crimes

iv. Assess and monitor the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in the Payment Service Bank's compliance with all laws and regulations; and

v. Advise and assist the relevant persons responsible for carrying out regulated activities to comply with the Payment Service Bank's compliance procedures

vi. Oversee the independence, autonomy and effectiveness of the Payment Service Bank's policies and procedures on whistleblowing including the procedures for protection of staff (where the whistle was blown by a staff).

b. Qualifications

i. A first degree or its equivalent in any discipline

ii. Membership of International Compliance Association will be an added advantage

c. Years of Experience

A Minimum of 15 years post-graduation qualification experience in Risk/Control functions within the Financial Services and Electronic Payments Industry.

d. Mandatory Continuous Professional Training (MCPT)

For continued retention in the role, in addition to general performance on the job, the CCO shall provide evidence of at least forty (40) hours of Mandatory Continuous Professional Training (MCPT) in Financial Reporting, Cyber security, Regulatory management and AML/CFT related programs.

5.15 CHIEF TREASURER

a. Responsibilities

The Chief Treasurer shall be responsible for:

i. Proper application of treasury policy, in particular to verify compliance with trading and other limits

ii. The forecast of cash flow positions, related borrowing needs, and funds available for investments

iii. The maintenance of institution's liquidity position.

b. Qualifications

A first degree or its equivalent in any discipline and relevant professional certification e.g. ACI or Treasury Dealership Certificate

c. Years of Experience

A Minimum of 15 years post-graduation experience out of which 8 years must have been spent in treasury related function.

5.16 MONEY LAUNDERING REPORTING OFFICER

a. Responsibilities

The Money Laundering Reporting Officer shall:

i. Put in place appropriate documentation of the Payment Service Bank's risk management policies (as approved by the Board) and risk profile in relation to money laundering, including documentation of application of those policies;

ii. Provide appropriate report on AML/CFT to the Board and senior management at least annually on the operation and effectiveness of those systems and controls;

iii. Ensure that when appropriate, the information or other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the Board;

iv. Assess internal trends, external regulatory & law enforcement environment to make recommendations, understand risk areas and alter or add to current processes;

v. Develop the overall program plan, oversee the execution of the plan and provide regular status report to executives on AML/CFT issues;

vi. Establish and maintain an effective Customer Due Diligence/Enhanced Due Diligence risk rating and ensure ongoing assessments, review and analysis of unusual/suspicious account activity;

vii. Conduct AML/CFT risk assessments annually or as needed with consideration to products, services, customers, and geographies that may present AML/CFT related risks; and

viii. Be responsible for periodic regulatory returns on AML/CFT matters to the CBN and any other regulator within the financial system (where required)

b. Qualification

A first degree and relevant certification in AML/CFT

c. Years of Experience

At least 10 years post qualification experience

5.17 CHIEF INFORMATION SECURITY OFFICER (CISO)

a. Responsibilities

The CISO shall:

i. Be responsible for the strategic policy (as approved by the Board) of the Payment Service Bank's information security program

ii. Manage strategy, operation and the budget for the protection of the enterprise information assets

iii. Stay abreast of information security issues and regulatory changes affecting the information security at the national and global level, communicate to the business segments on a regular basis about emerging developments

iv. Manage company-wide information security governance processes and lead Information Security Liaisons with regulatory bodies and law enforcement agencies

v. Lead information security planning processes and establish comprehensive information security program for the Payment Service Bank covering business, financial, legal and administrative information systems and technology.

b. Qualification

A University degree and relevant IT security/Audit certification

c. Years of Experience

At least 10 years post qualification experience 5 years in senior Management position and not less than 5 years in IT security/Audit certification role.

6.0 KNOW YOUR CUSTOMER (KYC) & ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT)

Payment Service Banks shall ensure that their systems are not used for money laundering and the financing of terrorism. They shall therefore comply with the provisions of the Central Bank of Nigeria (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and Other Financial Institutions in Nigeria) Regulation 2019 (as amended) and extant laws of the Federation aimed at combatting money laundering and the financing of terrorism.

6.1 ANTI-MONEY LAUNDERING/COMBATING FINANCING OF TERRORISM (AML/CFT) REGULATION PSBS IN NIGERIA

OBJECTIVES, SCOPE AND APPLICATIONS

a. Objectives

The objectives of this section of the framework shall be to:

i. Provide Anti-Money Laundering and Combating the Financing of Terrorism ("AML/CFT") compliance guidance or guidelines for the PSBs 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;

ii. Enable the CBN diligently enforce AML/CFT measures and ensure effective compliance by PSBs; and

iii. Provide guidance on Know Your Customer ("KYC") and to assist PSBs in the implementation of the provisions of this section of the framework.

b. Scope

This section of the framework covers:

i. the key areas of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) policy;

ii. development of compliance unit and function;

iii. compliance officer designation and duties;

iv. the requirement to cooperate with the competent or supervisory authorities;

v. conduct of Customer Due Diligence;

vi. monitoring and responding to suspicious transactions;

vii. reporting requirements; record keeping; and

viii. AML/CFT employee training.

c. Application

This section of the framework shall apply to Payment Service Banks in Nigeria within the regulatory purview of the Central Bank of Nigeria.

d. AML/CFT Institutional policy framework

A PSB shall:

i. 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 activity, money laundering or terrorism

ii. Formulate and implement internal controls and other procedures to deter criminals from using its facilities for money laundering and terrorist financing.

iii. Adopt a risk-based approach in the identification and management of their AML/CFT risks in line with the requirements of this framework.

iv. 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

v. Shall not in any way inhibit the implementation of the provisions of this section of the Framework and shall co-operate with the regulators and law enforcement agencies in the implementation of a robust AML/CFT regime in Nigeria.

vi. 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.

vii. Identify, review and record other areas of potential money laundering and terrorist financing risks not covered by this framework and report same to the appropriate authorities

viii. Reflect AML/CFT policies and procedures in their strategic policies

ix. Conduct on-going Due Diligence and where appropriate enhanced Due Diligence on all business accounts and shall obtain information on the purpose and intended nature of the business account of their potential customer

x. Ensure that their employees, agents and others doing business with them, clearly understand the AML/CFT programme.

e. Risk assessment

A PSB shall -

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

ii. document its risk assessment profile;

iii. consider all the relevant risk factors before determining what the level of the overall risk and the appropriate level and type of mitigation to be applied;

iv. keep these assessments up to date; and

v. have appropriate mechanisms to provide risk assessment information to regulatory, supervisory and competent authorities as well as Self-Regulatory Bodies ('SRBs').

f. Risk mitigation

A PSB shall –

i. have policies, controls and procedures which are approved by its board of directors to enable it to manage and mitigate the risks that have been identified (either by the country or by the PSB);

ii. monitor the implementation of those controls and enhance them, where necessary; and

iii. take enhanced measures to manage and mitigate the risks where higher risks are identified.

g. Designation and duties of AML/CFT Compliance Officer

1. A PSB shall designate its AML/CFT Chief Compliance Officer with the relevant competence, authority and independence to implement the institution's AML/ CFT compliance programme;

2. The AML/CFT Chief Compliance Officer referred to in sub-section (1) of this section of the framework shall be appointed at management level and shall report directly to the Board on all matters under this framework;

3. The duties of the AML/ CFT Compliance Officer referred to in this sub-section (1) of this section of the framework shall include:

i. developing an AML/CFT Compliance Programme;

ii. receiving and vetting suspicious transaction reports from staff;

iii. filing suspicious transaction reports with the NFIU;

iv. filing other regulatory returns with the CBN and other relevant regulatory and supervisory authorities

v. rendering "nil" reports to the CBN and NFIU, where necessary to ensure compliance;

vi. ensuring that the PSB's compliance programme is implemented;

vii. coordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements; and

viii. 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.

h. Cooperation with Competent Authorities

1. A PSB shall give an undertaking that it shall comply promptly with all the requests made pursuant to the AML/CFT laws and regulations and provide information to the CBN, NFIU and other relevant competent authorities

2. A PSB's procedures for responding to authorized requests for information on money laundering and terrorist financing shall meet the following:

i. searching immediately the PSB'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;

ii. reporting promptly to the requesting authority the outcome of the search; and

iii. protecting the security and confidentiality of such requests.

3.2 OFFENCES, MEASURES AND SANCTIONS

a. Scope of Offences

(1) A PSB 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:

i. participation in an organized criminal group and racketeering;

ii. terrorism, including terrorist financing;

iii. trafficking in human beings and migrant smuggling;

iv. sexual exploitation, including sexual exploitation of children;

v. illicit trafficking in narcotic drugs and psychotropic substances;

vi. illicit arms trafficking;

vii. illicit trafficking in stolen and other goods;

viii. corruption;

ix. bribery;

x. cybercrime and other fraud;

xi. counterfeiting currency;

xii. counterfeiting and piracy of products;

xiii. environmental crime;

xiv. murder;

xv. grievous bodily injury;

xvi. kidnapping, illegal restraint and hostage-taking;

xvii. robbery or theft;

xviii. smuggling, including smuggling done in relation to customs and excise duties and taxes);

xix. tax crimes, related to direct taxes and indirect taxes;

xx. extortion;

xxi. forgery;

xxii. piracy; or

xxiii. insider trading and market manipulation or any other predicate offence as contained in section 15 of Money Laundering (Prohibition) Act, 2011 (as amended) and provisions of the Terrorism Prevention Act, 2011 (as amended).

b. Terrorist Financing Offence

i. Terrorist 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 section1 of TPA 2011 (as amended).

ii. Terrorist financing offences are predicate offences for money laundering. They 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.

c. Targeted Financial Sanctions Related to Financing and Proliferation

i. A PSB shall report to 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, 2011 and any amendments that may be reflected by the competent authorities.

ii. The reports in sub-section (1) of this section of the framework shall include all transactions involving attempted and concluded transactions in compliance with the Money Laundering (Prohibition) Act MLPA, 2011 (as amended), Terrorism Prevention Act (TPA) 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.

iii. The administrative sanctions contained in Schedule I of this framework or in the Terrorism Prevention (freezing of International Terrorist Funds and Other Related

Issues) Regulation, 2013 (as amended) shall be imposed by the CBN on institutions under its regulatory purview.

d. Limitation of Secrecy and Confidentiality Laws

i. PSB secrecy and confidentiality laws shall not in any way, be used to inhibit the implementation of the requirements in this section of the framework and other relevant Regulations pursuant to the provisions of Section 38 of EFCC Act, 2004; 13 of MLP Act, 2011(as Amended) and Section 33 of the CBN Act, 2007.

ii. The relevant laws cited in this sub-section (12)(1) of this section of the framework have given the relevant authorities the power required to access information to properly perform their functions in combating money laundering and financing of terrorism, the sharing of information between competent authorities, either domestically or internationally, and the sharing of information between PSBs necessary or as may be required.

iii. Banking secrecy or preservation of customer confidentiality shall not be invoked as a ground for objecting to the measures set out in this section of the framework and other relevant Regulations or for refusing to be a witness to facts likely to constitute an offence under ML and TF laws, Regulations or any other law.

3.3 CUSTOMER DUE DILIGENCE, HIGHER RISK CUSTOMERS AND POLITICALLY EXPOSED PERSON

a. Customer Due Diligence ('CDD') measures

1) A PSB shall undertake Customer Due Diligence ('CDD') measures when –

a) business relations are established;

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

c) carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between PSBs and when credit or debit cards are used as a payment system to effect money transfer.

d) The measures in paragraphs (a), (b) and (c) 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 PSBs acting on their own behalf.

e) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in this section of the framework and other relevant Regulations; or

f) there are doubts on the veracity or adequacy of previously obtained customer identification data.

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

b. CDD Measures – Identification and Verification of Identity of Customers

1) A PSB 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.

2) A PSB shall carry out the full range of the CDD measures contained in this framework.

3) PSBs 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 Appendix A (schedule II) to this section of the framework.

5) Where the customers are a legal persons or legal arrangements, the PSB 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.

c. Verification of Beneficial Ownership

1) A PSB 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 it that it knows who the beneficial-owner is through methods including:

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 they may be no natural persons (whether acting alone or together) 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, the PSB 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 other types of legal arrangements PSBs shall identify and verify persons in equivalent or similar positions.

2) PSBs shall in respect of all customers, determine whether or 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 PSB 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 PSB 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;

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 PSB shall obtain information on the purpose and intended nature of the business account of its potential customers.

8) A PSB shall conduct on-going due diligence on a business account.

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 account to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, its business, risk profiles and the source of funds.

10) A PSB 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-accounts or customer categories.

d. Higher risk customers and activities

A PSB shall perform enhanced due diligence for higher-risk customer, business account or transaction including:

1) non-resident customers;

2) legal persons or legal arrangements; and

3) Politically Exposed Persons ('PEPs'),

4) Any other business, activities or professionals as may be prescribed by the regulatory, supervisory or competent authorities

e. Politically Exposed Person (PEP)

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) PSBs are required, in addition to performing CDD measures, to put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial owner is a PEP.

4) PSBs are also required to obtain senior management approval before they establish business accounts with PEP and to render monthly returns on all transactions with PEPs to the CBN and NFIU.

5) Where a customer has been accepted or has an ongoing account with a PSB 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 account.

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

f. New technologies and non-face-to-face transactions

(1) A PSB 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.

(2) PSBs are to ensure that any risk assessment to be undertaking 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 PSB shall have policies and procedures in place to address any specific risk associated with non-face to face business accounts or transactions.

(4) The policies and procedures required to be taken shall be applied automatically when establishing customer accounts 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.

g. Money or Value Transfer (MVT) Services

(1) All natural and legal persons performing Money or Value Transfer Service ('MVTS operators') shall be subject to the provisions of this section of the framework and other relevant Regulations.

(2) MVTS Operators shall maintain a current list of their agents and quarterly returns rendered to the CBN.

(3) In addition to the requirement specified in this regulation, MVTS 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) MVTS Operators shall:

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

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

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

h. Wire Transfers

(1) For every wire transfer of USD 1,000 or more, the ordering PSB shall obtain and maintain the following information relating to the originator of the wire transfer –

(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 USD 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 this section of the framework and other relevant Regulations.

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

(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 PSB 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 of 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 PSBs 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) PSBs are accordingly required to report wire transfers with incomplete originator's information to the NFIU.

(12) The beneficiary PSB shall restrict or even terminate its business account with the financial institution that fails to meet the standards specified in this regulation.

(13) Cross-border and domestic transfers between PSBs 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 provide 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 PSBs where both the originator person and the beneficiary person are PSBs acting on their own behalf.

3.4 LOWER RISK CUSTOMERS, PERIOD OF VERIFICATION AND RELIANCE ON INTERMEDIARIES

a. Simplified Due Diligence Applicable to Lower risk customers, transactions or products

(1) Where there are low risks, PSBs 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, PSBs shall apply the simplified or reduced CDD measures when identifying and verifying the identity of their customers and the beneficial-owners.

(4) The circumstances which the simplified or reduced CDD measures referred to in sub-section (3) of this section of the framework are applicable include in 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 this section of the framework and the relevant AML/CFT 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) Government ministries and parastatals; and

(d) Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions ('DNFBPs') provided that they are subject to the requirements for combating money laundering and terrorist financing consistent with the provisions of the Money Laundering (Prohibition) Act and designations made by the Minister of Trade and Investment

(5) PSBs that apply simplified or reduced CDD measures to customers that are resident abroad shall limit the application of the measures to customers in countries that have effectively implemented the FATF Recommendations.

(6) PSBs shall not apply the simplify 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.

(7) PSBs 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.

(8) Without prejudice to the above functions, PSBs shall consider the principles of consumer protection and data confidentiality as spelt out by the Consumer Protection Department of the CBN and Federal Competition and Consumer Protection Commission (FCCPC)

b. Timing of verification

(1) A PSB shall obtain and verify the identity of the customer, beneficial-owner and occasional customers following the establishment of the business account or conducting transactions for them.

(2) PSBs are permitted to complete the verification of the identity of the customer and beneficial owner following the establishment of the business account, 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 and others; or

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

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

(4) The procedures contemplated under sub-section (4) of this section of the framework include a set of measures such as:

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

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

c. Failure to complete CDD

(1) A PSB that fails to comply with the CDD measures pursuant to these sections of the framework and other relevant 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 PSB that has commenced the business account shall terminate the business account and render Suspicious Transaction Report to the NFIU.

(3) Where, a PSB suspects that transactions relate to money laundering or terrorist financing, during the establishment or course of the customer account, 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 PSB 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.

(5) A PSB shall ensure that their employees are aware of, and sensitive to the issues mentioned under this section of the framework.

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

(7) PSBs 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.

d. Existing Customers

(1) A PSB shall apply CDD requirements to existing customers on the basis of materiality and risk and continue to conduct due diligence on such existing accounts at appropriate times.

(2) The appropriate time to conduct CDD by PSBs is when:

(a) a transaction of significant value takes place;

(b) a customer documentation standard 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 PSB shall properly identify the customer in accordance with the criteria contained in this section of the framework and other relevant Regulations and the customer identification records shall be made available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

e. Reliance on intermediaries and third parties on CDD function

(1) A PSB that relies upon a third party to conduct its CDD shall:

i. 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

ii. 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 PSB 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 this section of the framework and other relevant Regulations.

(3) PSBs relying on intermediaries or other third parties who have no outsourcing, agency, business accounts, accounts or transactions with it for 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 PSB referred to in sub-section (3) of this section of the framework are to -

i. immediately obtain from the third party the necessary information concerning certain elements of the CDD process;

ii. 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;

iii. satisfy themselves that the third party is regulated and supervised in accordance with Core Principles of AML/CFT and has measures in place to comply with the CDD requirements set out in this section of the framework and other relevant Regulations; and

iv. ensure that adequate 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 PSB relying on the third party.

3.5 MAINTENANCE OF RECORDS, MONITORING, INTERNAL CONTROLS, PROHIBITIONS AND SANCTIONS

a. Maintenance of records on transactions

(1) A PSB 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 may be required by the CBN and NFIU provided that this requirement shall apply regardless of whether the account or business account is on-going or has been terminated.

(2) The components of records of transaction to be maintained by PSBs include the –

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

ii. nature and date of the transaction;

iii. type and amount of currency involved; and

iv. type and identifying number of any account involved in the transaction.

(3) PSBs 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 account or such longer period as may be required by the CBN and NFIU.

(4) A PSB shall ensure that all customer-transaction records and information are available on a timely basis to the CBN and NFIU.

(5) Without prejudice to the above, PSBs shall consider the principles of consumer protection and data confidentiality as spelt out by the Consumer Protection Department of the CBN and Federal Competition and Consumer Protection Commission (FCCPC)

b. Attention on complex and unusual large transactions

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

(2) For the purpose of sub-section (1) of this section of the framework, 'complex or unusually large transaction or, 'unusual pattern of transactions' include significant transactions relating to an account transaction 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.

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

c. Suspicious transaction monitoring

(1) Where a transaction -

i. involves a frequency which is unjustifiable or unreasonable;

ii. is surrounded by conditions of unusual or unjustified complexity;

iii. appears to have no economic justification or lawful objective; or

iv. in the opinion of the PSB involves terrorist financing or is inconsistent with the known transaction pattern of the account or business account;

that transaction shall be deemed to be suspicious and the PSB 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 PSB suspects that the funds mentioned under sub-section (1) of this section of the framework:

i. are derived from legal or illegal sources but are intended to be used for an act of terrorism;

ii. are proceeds of a crime related to terrorist financing; or

iii. 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 PSB shall immediately and without delay but not later than within 24 hours in the case of the circumstances mentioned in sub-section (1) and (2) of this section of the framework -

i. 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;

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

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

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

(5) A PSB that fails to comply with the provisions of:

i. sub-section (1) of this section of the framework is liable to a fine of N1, 000,000 for each day the offence subsists; or

ii. sub-section (2) of this section of the framework is liable to sanction as stipulated under the TPA, 2011 (as amended).

(6) Any person who being a director or employee of a PSB 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 on conviction to a time of not less than N10,000,000 or banned indefinitely or for a period of 5 years from practicing his profession.

(7) The directors, officers and employees of PSBs 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.

d. Compliance monitoring and response to suspicious transactions

(1) A PSB 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 **Appendix C** to this section of the framework and other relevant Regulations.

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

(4) When any staff of a PSB detects any "red flag" or suspicious money laundering 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 PSB and its staff shall maintain confidentiality in respect of any investigation conducted in pursuance of this section of the framework and other relevant 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 shall not say anything that might tip off someone else that he is under suspicion of money laundering.

(6) A PSB 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) PSBs, 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.

e. Internal controls, compliance and audit

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

(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) PSBs 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) an 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, 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 PSB shall put in place a structure that ensures the operational independence of the Chief Compliance Officer ('CCO')

f. Sanctions

1) Any individual, being an official of a PSB, who fails to take reasonable steps to ensure compliance with the provisions of this section of the framework and other relevant Regulations shall be sanctioned accordingly based on the extant administrative sanction regime issued or directed by the Attorney-General of the Federation.

2) A PSB, its officers or employees shall not benefit from any violation of extant AML/CFT laws and Regulation.

3) Criminal cases shall be referred to the Economic and Financial Crimes Commission ('EFCC') or other law enforcement agencies for prosecution and the

offender liable to forfeit any pecuniary benefit obtained as a result of the violation or breach.

4) Incidence of false declaration, false disclosure, non-declaration or non-disclosure of returns to be rendered under this section of the framework and other relevant Regulations by a PSB 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.

g. Prohibition of numbered or anonymous accounts, accounts in fictitious names and shell banks

(1) Notwithstanding the provisions of section 11.3 of the Guidelines for licensing and regulation of Payment Service Banks in Nigeria and Section 44.2 of this Framework, a PSB shall not keep anonymous accounts or accounts in fictitious names;

(2) A PSB, corporate body or any individual that contravenes the provisions of this section of the framework and other relevant Regulations is liable to a fine of not less than N10,000,000 and in addition to:

i. the prosecution of the principal officers of the corporate body, and

ii. the winding up and prohibition of its re-constitution or incorporation under any form or guise.

h. Other forms of reporting

(1) A PSB shall report in writing any single transaction, lodgment or transfer of funds in excess of N5,000,000 and N10,000,000 or their equivalent made by an individual and corporate body respectively to the NFIU in accordance with section 10(1) of the MLPA, 2011 (as amended).

(2) In compliance with section 2(1) of the MLPA, 2011(as amended) PSBs 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 Central Bank of Nigeria (CBN) and the NFIU within 7 days from the date of the transaction.

(3) In compliance with the Terrorism (Prevention) Act (TPA) 2011 (as amended), PSBs are also required to, within a period of not more than 24 hours, forward to the NFIU, reports of suspicious transactions relating to:

i. fund derived from illegal or legal sources are intended to be used for any act of terrorism; or

ii. proceeds of a crime related to terrorism financing; or

iii. proceeds belonging to a terrorist, terrorist entity or organization.

(4) A PSB shall not be statutorily liable for violation of confidentiality rules for every lawful action taken in furtherance of its obligations under this section of the framework and other relevant Regulations.

(5) Details of a report sent by the PSB to the appropriate authority shall not be disclosed by the institution or any of its officers to any other person.

i. Attention for High Risk Countries

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

(2) A PSB 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.

j. AML/CFT employee-education and training programme

(1) A PSB shall design comprehensive employee education and training programs, 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.

(2) The timing, coverage and content of the employee training program shall be tailored to meet the needs of the PSB to ensure compliance with the requirements and provisions of this section of the framework and other relevant Regulations.

(3) A PSB shall provide comprehensive training programs for staff covering compliance officers and as part of the orientation program for new staff and those posted to the front office, operations, account opening, mandate, and marketing/customer service/call center staff, internal control and audit staff and managers.

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

(5) An employee training program 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 program of PSBs shall include:

i. AML regulations and offences;

ii. the nature of money laundering;

iii. money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies;

iv. reporting requirements;

v. customer due diligence;

vi. risk-based approach to AML/CFT; and

vii. record keeping and retention policy.

(7) A PSB shall submit their annual AML/CFT Employee training program for the following year to the CBN and NFIU not later than the 31st of December of the current year.

k. Monitoring of employee conduct

(1) A PSB shall monitor their employees' accounts for potential signs of money laundering.

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

(3) The requirement specified in sub-section (2) of this section of the framework 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.

l. Protection of Staff Who Report Violations

(1) A PSB shall make it possible for employees to report any violations of the institution's AML/CFT compliance program to the AML/CFT Compliance Officer.

(2) A PSB shall direct their employees in writing to always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to the NFIU.

(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 PSB shall inform their employees in writing to make their reports confidential and to assure employees of protection from victimization as a result of making any report.

m. Additional areas of AML/CFT risks

(1) A PSB shall review, identify and record other areas of potential money laundering risks not covered by this section of the framework and other relevant Regulations and report the risk quarterly to the CBN and NFIU.

(2) A PSB shall review their AML/CFT frameworks from time to time with a view to determining their adequacy and identifying other areas of potential risks not covered by the AML/CFT Regulations.

n. Additional procedures and mitigants

After carrying out the review of the AML/CFT framework and identified new areas of potential money laundering vulnerabilities and risks, the PSB 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 every financial year.

o. Testing for the adequacy of the AML/CFT compliance

(1) A PSB shall make a policy commitment and to subject their AML/CFT Compliance Program to independent-testing or require their internal audit function to determine the adequacy, completeness and effectiveness of the program.

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

p. Formal Board approval of the AML/CFT compliance

(1) The ultimate responsibility for AML/CFT compliance is placed on the Board or top Management of every licensed PSB in Nigeria.

(2) The board of a PSB 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 Policy and Procedure referred to in sub-section (2) of this section of the framework are to be forwarded to the CBN and NFIU within six months of the release of this framework.

(4) Quarterly reports on the AML/CFT-compliance status of a PSB are to be presented to the board for its information and necessary action.

(5) PSBs shall submit to the Director, Payments System Management Department CBN, not later than seven (7) days after the end of each quarter, returns on their compliance with AML/CFT provisions.

r. Culture of compliance

Every PSB 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, reputational and financial risks.

3.6 GUIDANCE ON KNOW YOUR CUSTOMER (KYC)

a. Three Tiered KYC Requirements.

(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-section 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 PSB;

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

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

(g) such accounts may cover Mobile Banking products, issued in accordance with the CBN Regulatory Framework for Mobile Payments Service 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 N50,000 and maximum cumulative balance of N300,000 at any point in time

(m) international funds transfer is prohibited; and

(n) accounts are strictly savings;

(3) Tier two for which—

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

ii. items in paragraph (a) of this section of the framework may be forwarded electronically or submitted on-site in banks' branches or agents' offices;

iii. 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;

iv. 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;

v. evidence of basic customer information is required at this level and identification, verification and monitoring by PSBs are also required;

vi. accounts may be contracted by phone or at the institution's website;

vii. accounts may be linked to a mobile phone;

viii. may be used for funds transfers within Nigeria only;

ix. no amount is required for opening of the accounts;

x. such accounts cover Mobile Banking products (issued in accordance with the CBN Regulatory Framework for Mobile Payments Services in

Nigeria);

xi. maximum single deposit of ₦200,000 and a maximum cumulative balance of ₦500,000 are allowed at any time; and

xii. 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—

(i.) a PSB shall obtain, verify and maintain copies of all the required documents for opening of accounts in compliance with the KYC requirements contained in this framework;

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

(iii.) maximum single deposit of ₦5,000,000 and there is no limit on cumulative balance and

(iv.) KYC requirements shall apply.

b. Duty to Obtain Identification Evidence

i. PSBs shall not establish a business account until relevant parties to the account have been identified, verified, and the nature of the business they intend to conduct ascertained.

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

iii. 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.

iv. PSBs shall not engage any financial business or provide advice to a customer or potential customer unless the PSBs are certain as to who that person actually is.

v. PSBs shall obtain evidence of identification of their customers.

vi. A PSB shall identify all relevant parties to the account from the outset in accordance with general principles of obtaining satisfactory identification evidence set out in this section of the framework and other relevant Regulations.

c. Nature and Level of the Business

(1) A PSB shall obtain sufficient information on the nature of the business that their customer intends to undertake, including expected or predictable pattern of transactions.

(2) The information collated at the outset for this purpose should include:

i. purpose for opening the account or establishing the account;

ii. nature of the activity that is to be undertaken;

iii. expected origin of the funds to be used during the account; and

iv. details of occupation, employment or business activities and sources of wealth or income.

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

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

d. Application of commercial judgment

(1). A PSB shall take a risk-based approach to 'Know Your Customer ('KYC') requirements.

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

(3). For private company or partnership, focus should be on the identification of the principal owners or controllers whose identities shall also be verified.

(4). The identification evidence collected at the outset of a business should be viewed against the inherent risks in the business or service.

e. Identification

(1) The customer identification process shall subsist throughout the duration of the business account.

(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 PSB 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 this section of the framework and other relevant Regulations are not exhaustive.

f. Factors to consider in identification

(1).In determining a customer's identity under this section of the framework the following shall be considered-

a) the names used,

b) date of birth and

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.

e) Where an international passport or national identity card is taken as evidence of identity, the number, date and place or country of issue (as well as expiring date in the case of international passport) shall be recorded.

g. Time for verification of identity.

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

(2) In this section of the framework, "transaction" include the giving of advice and "advice "under this section of the framework shall not apply where information is provided about the availability of products or services and when a first interview or discussion prior to establishing an account takes place.

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

h. Verification of identity

(1) PSBs shall obtain sufficient evidence of the client's identity to ascertain that the client is the person he claims to be.

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

i. Exceptions

(1) 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; and

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

j. Identification of directors and other signatories

A PSB shall take appropriate steps to identify directors and all the signatories to an account.

k. Joint Account holders

Identification evidence shall be obtained for all applicants for a joint account.

l. Verification of identity for high risk business

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 -

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

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

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

A PSB shall –

i. be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly; and

ii. to observe the additional provisions for High Risk Categories of Customers under AML/CFT Directive in this section of the framework and other relevant Regulations.

n. Savings schemes and investments in third parties' names

Where an investor sets up a savings accounts or a regular savings scheme whereby the funds are supplied by one person for investment in the name of another (such as 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 and purpose, the applicant for the business and such person identification evidence shall be obtained in addition to the part of the legal owner.

o. Timing of identification requirements

(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.

(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 section of the framework, the PSB shall discontinue any activity it is conducting for the client and bring to an end any understanding reached with the client.

(3) A PSB shall also observe the provision in the Timing of Verification under the AML/CFT Directive of this framework.

(4) A PSB may however start processing the business or application immediately, provided that it promptly takes appropriate steps to obtain identification evidence ; and does not transfer or pay any money out to a third party until the identification requirements have been satisfied.

p. Consequence of failure to provide satisfactory identification evidence

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

(2). A PSB under this situation shall immediately make a Suspicious Transaction Report 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 PSB shall have in place written and consistent policies closing a account or unwinding a transaction where satisfactory evidence of identity cannot be obtained.

(4). PSBs are also required to respond promptly to inquiries made by competent authorities on the identity of their customers.

q. Identification Procedures

(1) A PSB shall ensure that it is dealing with a real person or organization (natural, corporate or legal) by obtaining sufficient identification evidence.

(2) Where reliance is being 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 of that name lives at the given address 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 or substitution (impersonation) fraud shall be stated also by the financial institution.

r. New Business for Existing Customers

(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 it does not tally with the information in the PSB's records, provided that procedures are put in place to guard against impersonation or fraud.

(2) The opportunity of opening the new account in sub-section (1) of this regulation shall be utilized to ask the customer to confirm the relevant details and to provide any missing KYC information. This is particularly important where:

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

(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-section (2) of this section of the framework, 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 provision of this section of the framework and other relevant Regulations.

s. Certification of Identification Documents

(1) 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, 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, where necessary.

(2) 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:

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

ii. a senior official within the account opening institution; or

iii. 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 PSB.

(5) A PSB 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.

t. Recording Identification Evidence.

(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 account ended.

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

(3) Confirmation of evidence in sub-section (2) of this section of the framework, shall be sufficient 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.

u. Additional verification requirements

(1) 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.

(2) Additional verification requirements for 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.

(3) 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.

(4) 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.

v. Term Deposit Account ('TDA').

Term Deposit Accounts ('TDA') can be broadly classified as a one-off transaction provided that a PSB 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. The identity verification requirements will therefore differ depending on the nature and terms of the TDA.

w. Investment Funds

In circumstances 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 neither been taken nor confirmation obtained from the original fund manager, such evidence shall be obtained at the time of the transfer.

x. Establishing Identity

Establishing identity under this section of the framework and other relevant Regulations is divided into three broad categories:

(a) private individual customers;

(b) quasi corporate customers; and

(c) pure corporate customers.

GENERAL INFORMATION

3.7 Private Individuals - General Information

(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 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.

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

(4) 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.

(5) 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.

(6) For low-risk accounts or simple investment products such as deposit or savings accounts or automated money transmission facilities, the PSB shall satisfy itself as to the identity**.**

a. Private Individuals Resident in Nigeria.

(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

The confirmation of name and address shall be established by reference to more than one source.

(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 PSB opening the account or providing the product or service.

b. Documenting Evidence of Identity.

(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 Schedule II to this section of this framework

c. Physical Checks on Private Individuals Resident in Nigeria

(1) A PSB shall establish the true identity and address of its customer and carryout effective checks to protect the institution against substitution of identities by applicants.

(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) 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;

(b) 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

(c) card or account activation procedures.

(3) A PSB 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 account are obtained from the customer.

d. Electronic Checks.

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

(2) A PSB shall use a combination of electronic and documentary checks to confirm different sources of the same information provided by a customer. Physical and electronic checks of the same statement of account are the different sources.

(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 also needs to 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 section of the framework shall assist PSBs 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.

3.8 FINANCIAL EXCLUSION FOR THE SOCIALLY OR FINANCIALLY DISADVANTAGED APPLICANTS

a. Refugees or Asylum Seekers.

(1) Where a refugee or asylum seeker requires a basic account without being able to provide evidence of identity, authentic references from the Ministry of Internal Affairs or an appropriate government agency 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.

b. Students and Minors

(1) When opening accounts for students or other young people, the normal identification procedures set out in this section of the framework and other relevant Regulations shall be followed as far as possible and where such procedures may not be relevant or do not provide satisfactory identification evidence, verification may be obtained through:

(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 or passport of the child provided that strict monitoring shall be undertaken since this type of account may be open to abuse.

3.9 UNINCORPORATED AND CORPORATED ORGANIZATIONS

a. Unincorporated Business or Partnership

(1) Where the applicant is an un-incorporated business or a partnership whose principal partners or controllers do not already have a business account with the PSB, 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.

(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 a the transaction shall be obtained.

b. Limited Liability Partnership

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

c. Pure Corporate Customers

(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.

(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”.

d. General Principles.

(1) The identity of a corporate company comprises:

i. registration number;

ii. registered corporate name and any trading names used;

iii. registered address and any separate principal trading addresses;

iv. directors;

v. owners and shareholders; and

vi. 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) In all cases, 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 account 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.

e. Public Registered Companies

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

(2) Identify the directors of a quoted company may not be identified.

(3) PSBs shall make appropriate arrangements to ensure that an officer or employee, past or present, is not using the name of the company or its account 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 and phone calls may be made to the Chief Executive Officer of such a company to intimate him of the application to open the account in the financial institution.

(5) 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.

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

f. Private Companies.

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 –

(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 Corporate Affairs Commission (CAC) or an enquiry via 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 PSB shall pay attention shall be paid 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.

g. Higher Risk Business Applicant

Where a higher-risk business applicant is seeking to enter into a account where third party funding and transactions are permitted, the following evidence shall be obtained either in documentary or electronic form –

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

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

iii. 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

iv. the Memorandum and Articles of Association of the company.

h. Higher Risk Business Relating to Private Companies

(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.

(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, the objective is to undertake measures that look behind that company or vehicle and verify the identity of the beneficial-owner or settlers and where PSBs become aware that the principal-beneficial owners or controllers have changed, they are required to verify the identities of the new owners.

(5) PSBs are required to also identify directors who are not principal controllers and signatories to a account for risk based approach purpose.

(6) PSBs 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 accounts, 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 "Know Your Customer" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

i. Designated Non-Financial Businesses and Professions (DNFBPs)

(1) As part of KYC documentation for designated non-financial businesses and professions, the certificate of registration with the Federal Ministry of Trade and Investment Special Control Unit Against Money Laundering, shall be obtained including identities of at least two of the directors.

(2) Where applications made on behalf of clubs or societies, a PSB 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** when signatories change, PSBs shall verify the identity of at least two of the new signatories.

(3) Where the purpose of the club or society is to purchase the shares of 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.

j. Registered Charity Organizations

(1) A PSB 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 are required to be operated 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, the financial institution is required to obtain and confirm the name and address of the organization concerned.

(4) Where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate, a PSB is required to send a letter

to the official correspondent, informing him of the charity organizations' application before it and the official correspondent shall is required to 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 this section of the framework and other relevant 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.

k. Religious Organizations (ROs)

A Religious Organization shall have a CAC registered number 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.

3.10 INTRODUCTIONS, APPLICATIONS AND FOREIGN INTERMEDIARIES

a. Introductions from Authorized Financial Intermediaries

(1) Where an intermediary introduces a customer and then withdraws from the ensuing account altogether, then the underlying customer has become the applicant for the business shall be identified in line with the requirements for personal, corporate or business customers as appropriate and an introduction letter shall be issued by the introducing financial institution or person in respect of each applicant for business.

(2) To ensure that product-providers meet their obligations, that satisfactory identification evidence shall be obtained and retained for the necessary statutory period, each introduction letter shall either be accompanied by certified copies of the identification evidence that has been 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.

b. Corporate Group Introductions

(1) Where a customer is introduced by one part of a financial sector group to another, it is not necessary for identity to be re-verified or for the records to be duplicated 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 account;

(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, 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 PSB has day-to-day access to all the Group's "Know Your Customer" information and records, there is no need to identify an introduced customer or obtain a group introduction letter where the identity of that customer has been verified previously.

(3) Where the identity of the customer has not previously been verified, then any missing identification evidence will need to be obtained and a risk-based approach taken on the extent of KYC information that is available on whether or not additional information shall be obtained.

(4) A PSB 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 but where such restrictions apply, copies of the underlying records of identity shall, wherever possible, be sought and retained.

(5) 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 this section of the framework and other relevant Regulations.

c. Business Conducted by Agents

(1) Where an applicant is dealing in its own name as agent for its own client, a PSB shall, in addition to verifying the agent, establish the identity of the underlying client.

(2) A PSB can regard evidence as sufficient where it has established that the client –

(a) is bound by and has observed this section of the framework and other relevant Regulations or the provisions of the Money Laundering (Prohibition) Act, 2011 (as amended); and

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

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

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

(b) where 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) Where 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 relevant money laundering legislation, then each case shall be treated on its own merits. The knowledge of the agent shall inform the type of the due diligence standards to apply. Risk-based approach shall also be observed by the financial institution.

d. Acquisition of one financial institution and business by another

(1) Where a PSB acquires the business and accounts of another PSB/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 in this section of the framework and other relevant 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 this section of the framework and other relevant Regulations;

(b) procedures shall be checked; or

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

3.11 LINKED TRANSACTIONS, FOREIGN ACCOUNTS AND INVESTMENT

a. Sanctions for non-compliance with KYC

Failure to comply with the provisions contained in this section of the framework will attract appropriate sanction in accordance with the provisions of the Principal Act, existing laws and as provided for under the offences and penalties of this section of the framework and other relevant Regulations.

b. Interpretation

In this section of the framework and other relevant Regulations –

'Applicant for Business' means a person or company seeking to establish a 'business account' 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 institutions, but may/may not be ultimately intended for different persons;

'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 Account' means any arrangement between the PSB and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset;

'Cross-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' include:

i. participation in an organized criminal group and racketeering;

ii. terrorism, including terrorist financing;

iii. trafficking in human beings and migrant smuggling;

iv. sexual exploitation, including sexual exploitation of children;

v. illicit trafficking in narcotic drugs and psychotropic substances;

vi. illicit arms trafficking;

vii. illicit trafficking in stolen and other goods;

viii. corruption and bribery;

ix. fraud;

x. counterfeiting currency;

xi. counterfeiting and piracy of products;

xii. environmental crime;

xiii. murder, grievous bodily injury;

xiv. kidnapping, illegal restraint and hostage-taking;

xv. robbery or theft;

xvi. smuggling (including in relation to customs and excise duties and taxes;

xvii. tax crimes (related to direct taxes and indirect taxes);

xviii. extortion;

xix. forgery;

xx. piracy;

xxi. insider trading and market manipulation; and

xxii. all other predicate offences as contained in Section 15 of Money Laundering (Prohibition) Act, 2011 (as amended).

'Designated non-financial businesses and professions includes:

(a) casinos which also includes internet casinos;

(b) real estate agents;

(c) dealers in precious metals;

(d) dealers in precious stones;

(e) lawyers, notaries, other independent legal professionals – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering;

'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 Recommendations' means the revised FATF Recommendations issued by the Financial Action Task Force.

'Financing of terrorism' means financial support in any form, of terrorism or of those who encourage, plan or engage in the act of terrorism;

'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 PSB 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 account with a PSB 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 Organizations mean 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 where there is no account, the person natural or legal that places the order with the financial institution to perform the wire transfer;

'A one-off transaction' means any transaction carried out other than in the course of an established business account.

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 account 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 derived from or obtained, directly or indirectly, through the commission of an offence;

'Risk' All references to risk in this section of the framework and other relevant Regulations means the risk of money laundering and/or terrorist financing;

'Shell bank' means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision;

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

'Terrorist' means any natural person who:

(i) commits or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully,

(ii) participates as an accomplice in terrorist acts,

(iii) organises or directs others to commit terrorist acts, or

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

'Terrorist act' includes:

(a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties –

(i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970),

(ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971),

(iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973),

(iv) International Convention against the Taking of Hostages (1979),

(v) Convention on the Physical Protection of Nuclear Material (1980),

(vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988),

(vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988),

(viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and

(ix) the International Convention for the Suppression of Terrorist Bombings (1997); and

(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population or to compel a Government or an international organization to do or to abstain from doing any act;

'Terrorist financing (FT) offence' includes both the primary and ancillary offences;

'Terrorist organization' includes any group of terrorists that –

(a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully,

(b) participates as an accomplice in terrorist acts,

(c) organizes or directs others to commit terrorist acts, or

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

'Terrorist 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;

'Unique identifier' means any unique combination of letters, numbers or symbols that refer to a specific originator.

'Wire transfer' means any transaction carried out on behalf of an originator **both natural and legal person** through a PSB 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.

3.12 INFORMATION TO ESTABLISH IDENTITY

a. Natural Persons

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

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

(b) correct 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 account; and

(i) signature.

(2) The PSB shall verify the information referred to in paragraph 1 of this Schedule 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.

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.

3) PSBs shall apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.

(4) A PSB shall be able to make an initial assessment of a customer's risk profile from the information provided and particular attention shall to 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 (i.e. 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, public position held (where appropriate).

(5) 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.

b. Institutions.

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.

c. Corporate Entities

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

i. name of the institution;

ii. principal place of the institution's business operations;

iii. mailing address of the institution;

iv. contact telephone and fax numbers;

v. some form of official identification number, if available such as tax identification number;

vi. the original or certified copy of the certificate of incorporation and memorandum and articles of association;

vii. the resolution of the board of directors to open an account and identification of those who have authority to operate the account; and

viii. nature and purpose of business and its legitimacy.

(2) The PSB 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 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) utilizing 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.

d. Corporation or Partnership

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

(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.

e. Other Types of Institution

(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, Mutuals/Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, Trusts and Foundations and Professional Intermediaries –

(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/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 PSB shall verify the information referred to in paragraph 9(1) of this Schedule by at least one of the following –

(a) obtaining an independent undertaking from a reputable and known firm of lawyers confirming the documents submitted;

(b) obtaining prior bank references; and

(c) accessing public and private databases or official sources.

f. Mutual/Friendly, Cooperative and Provident Societies

Where these entities are 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.

g. Charities, Clubs and Associations

(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. This includes 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. Independent confirmation shall also be obtained of the purpose of the institution.

h. **Professional Intermediaries**

(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 where 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 PSB 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 them:

(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 account such as fund administrator or manager.

(3) 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.

(4) 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.

3.13 MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS"

a. Suspicious Transactions "Red Flags"

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 traveller'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.

(a) 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.

(b) 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 movement 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) 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 takes place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations.

(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;

(ix) where embassy accounts directly fund personal expenses of foreign nationals.

7.0 SHARED SERVICES

i. PSBs shall with the approval of the CBN enter into shared services agreement with its parent company or subsidiary, provided that the recipient entity does not have the expertise and capacity to carry out these services.

ii. PSBs shall establish policies and procedures to ensure that shared services with its parent/subsidiary companies are conducted at arm's length.

iii. PSBs shall submit its shared policies and procedures, as approved by the Board to the Central Bank of Nigeria.

iv. The board shall be responsible for the oversight of shared service arrangement and ensure the reasonableness of fees charged for the service.

v. A shared service agreement shall be executed between the recipient institution and the provider company

vi. All shared services agreements involving cross-border arrangements (parent and subsidiary) shall include a provision for capacity building.

vii. The shared service agreement, along with the validation by an independent firm shall be submitted to the CBN for approval.

viii. The Report of an Independent third-party review of the fees and services rendered shall be submitted annually to the Director, Payments System Management Department.

ix. PSBs shall comply with FIRS Income Tax (transfer pricing) Regulation. In addition, shared service fees shall be documented for all transactions between the service provider and the recipient in the same manner as if they were between unrelated parties.

x. A PSB that provides shared services to other entities in a group shall be responsible for the payment of salaries and allowances of the staff used to provide such services.

xi. All services shared within the group shall be disclosed by the PSB in their annual report and website.

xii. PSBs shall comply with all provisions of the Guidelines for Shared Services Arrangements for Banks and Other Financial Institutions advised from time to time by the CBN.

8.0 PRUDENTIAL RATIOS

a. Capital adequacy ratio

The capital adequacy ratio for Payment Service Banks shall be as provided in the extant Guidelines for Licensing and Regulation of Payments Service Banks or as may be determined by the Central Bank of Nigeria from time to time.

b. Liquidity Ratio

The liquidity ratio for Payment Service Banks shall be as provided in the extant Guidelines for Licensing and Regulation of Payments Service Banks or as may be determined by the Central Bank of Nigeria from time to time.

c. Cash Reserve Ratio

The cash reserve ratio for Payment Service Banks shall be as provided in the extant Guidelines for Licensing and Regulation of Payments Service Banks or as may be determined by the Central Bank of Nigeria from time to time.

9.0 DATA INFRASTRUCTURE AND CYBER SECURITY

A PSB shall comply with the provisions of the Nigerian Financial Services Industry IT Standard Blueprint and the Risk Based Cyber Security Framework as well as all other regulations the Bank may issue regarding ICT infrastructure for banks.

In line with the Nigerian Financial Services Industry IT Standard Blueprint, a PSB shall maintain level 3 maturity where IT Standards are defined; documented; Integrated into organizational practices via policy and procedures; Communicated through training and ensure that automation and tools are not used in a limited and fragmented way.

A PSB shall also comply with the following standards:

SN	IT PROCESS AREA		STANDARDS	
1	Strategic IT Alignment		IT Infrastructure Library (ITIL)	Control Objectives for Information and related Technologies (COBIT)
2	IT Governance		COBIT	ISO 38500
3	Architecture & Information Management	Interfaces	ISO 8583	ISO 20022
		Reporting	eXtensible Business Reporting Language (XBRL)	
		Enterprise Architecture	The Open Group Architecture Framework (TOGAF)	
4	Solutions Delivery	Applications Development	Capability Maturity Model Integration (CMMI)	ISO 15504
		Project Management	Project Management Body of Knowledge (PMBOK)	PRojects IN Controlled Environments version 2 (PRINCE2)
5	Service Management & Operations	Service Management	ITIL	
		Data Center	Tier 3 Standards	
		Health, Safety, Environment (HSE)	OHSAS 18001	
		Business Continuity	Business Continuity Institute Good Practice Guidelines (BCI GPG)	BS25999 / ISO 22301
6	Information & Technology Security		Payment Card Industry Data Security Standard (PCI DSS)	ISO 27001/27002
7	Workforce & Resource Management		Skills Framework for the Information Age (SFIA)	

A PSB is also required to put in place a Cybersecurity programme that shall meet the minimum requirement laid out in the Risk Based Cybersecurity Framework. The requirement is in 4 key areas as summarized below:

i. Cybersecurity Governance and Oversight: This sets the agenda and boundaries for cybersecurity management and controls through defining, directing and supporting the security efforts of the PSBs. It spells out the responsibilities of the Board of Directors, Senior Management and Chief Information Security Officer (CISO). This entails the development and enforcement of policies, procedures and other forms of guidance that the PSBs and their stakeholders are required to follow.

ii. Cybersecurity Risk Management System: Effective Risk Management serves to reduce the incidence of significant adverse impact on an organization by addressing threats, mitigating exposure, and reducing vulnerability. PSBs shall incorporate cyber-risk management with their institution-wide risk management framework and governance requirements to ensure consistent management of risk across the institution. The Risk Management programme shall be based on an understanding of threats, vulnerabilities, risk profile and level of risk tolerance of the organization. The process shall also be dynamic in view of the constantly changing risk landscape. The Board and Senior Management shall support and be involved in the cyber-risk management process by ensuring that resources and capabilities are available, and roles of staff properly defined in management of risks.

iii. Cybersecurity Operational Resilience: PSBs are required to build, enhance, and maintain their cybersecurity operational resilience which will ultimately contribute to reducing cybercrime in Nigeria and strengthen the banking sector cyber defense.

iv. Metrics, Monitoring & Reporting: A PSB shall put in place metrics and monitoring processes to ensure compliance, provide feedback on the effectiveness of control and provide the basis for appropriate management decisions. The metrics should be properly aligned with strategic objectives and provide the information needed for effective decisions at the strategic, management and operational levels.

A PSB shall comply with all other regulations the Bank may issue regarding ICT infrastructure for banks.

10.0 INTEROPERABILITY

A PSB shall comply with the provisions of the Guidelines on Transactions Switching in Nigeria and any other relevant guidelines.

11.0 BUSINESS CONTINUITY MANAGEMENT SYSTEM

11.1 Rights and Responsibilities of PSBs

i. A PSB shall assume the roles and responsibilities of acquirers/acquiring bank and/or issuer/issuing bank as stipulated in all regulations on electronic payments, depending on the function they may perform at any point in time within the electronic payment ecosystem.

ii. Acquiring PSBs whose transactions are switched shall maintain databases that can handle information relating to cardholders, merchants and their transactions for a minimum period of seven (7) years.

iii. Information on usage, volume and value of transactions and other relevant information shall be forwarded to the CBN as and when due and in the format required by the CBN.

iv. Each PSB shall settle fees charged for the services provided by the switching company in relation to the operation of the switching network, in accordance with the agreed tariff.

v. The issuing PSB shall be held liable (where proven) for frauds with the card arising from card skimming or other compromises of the issuing PSB's security system

vi. An acquiring PSB shall be responsible for ensuring that merchants put in place reasonable processes and systems for confirming payee identity and detecting suspicious or unauthorized usage of electronic payment instruments, both where customer/card is physically present at point of sale or in cases where customer/card is not physically present, like in Internet/web and telephone payment systems/portals.

vii. PSBs shall be deemed as partner institutions to the Nigeria Central Switch or any other Switch. Each Partner Institution shall undertake to satisfy and ensure continued compliance with the eligibility criteria and conditions for admission, as outlined in the operational rules and regulations of the Nigeria Central Switch (NCS) and the technical requirements as specified in the Guideline for Transaction Switching in Nigeria.

viii. A PSB shall not perform the role of a Switch

ix. PSBs are mandatorily required to establish secure connectivity to the Nigeria Central Switch and must be capable of providing secure hardware encryption/decryption of customer's PINs and messages for onward transmission to the NCS with respect to their card operated devices.

x. In addition to the above, any other responsibilities as may be defined within the

switching guidelines or by the Bank with respect to transaction switching shall be applicable to PSBs.

11.2 Prohibition of Anti-competition Agreements

A PSB who is a party to Switching Services in Nigeria shall not enter into any agreement in respect of any switching service that shall cause or is likely to cause adverse effect on competition. Any agreement entered in contravention of this provision shall be null and void and of no effect.

a. Any agreement entered between PSBs on Switching Services or decision taken by any association of switching companies or association of persons, including cartels engaged in identical or similar provision of switching services, which:

i. Limits or controls markets, technical development, investment or provision of Switching Services;

ii. Shares the market or provision of services by way of allocation of geographical area of market, or number of customers in the market or any other similar way; shall be considered an anti-competition agreement.

b. Any agreement amongst parties to Switching Services, in respect of switching services, including:

i. Tie-In Agreement;

ii. Exclusive Service Agreement; and

iii. Refusal to deal

shall be considered an agreement in contravention of anti-competition agreement if such agreement causes or is likely to cause adverse effect on competition in Nigeria.

11.3 Prohibition of Abuse of Dominant Position

1. A PSB who is a party to Switching Services shall not abuse its dominant position by directly or indirectly imposing unfair or discriminatory condition and fees in the provision of its services.

2. Equally, a PSB who is a party to Switching Services shall not limit or restrict the provision of switching services or market thereof or technical or scientific development relating to switching services to the prejudice of consumers.

3. A PSB shall not indulge in practice or practices resulting in denial of market access.

12.0 REGULATORY RENDITION

Payment Service Banks shall render regular reports to the Central Bank of Nigeria in a format and frequency prescribed by the Bank.

13.0 INTEGRATION TO THE GLOBAL STANDING INSTRUCTION (GSI) PLATFORM

For their role as Participating Institutions in the GSI scheme, PSBs shall execute the GSI Mandate Agreement with the Nigeria Inter-Bank Settlement System (NIBSS) in line with the provisions of the Guidelines on Global Standing Instruction (2020) or the Extant Regulation.

For their role as Participating Institutions in the GSI scheme, PSBs shall comply with the provisions of the Guidelines on Global Standing Instruction (2020) or the Extant Regulation.

13.1 Roles and responsibilities

Particularly, a PSB shall:

i. Execute the GSI Mandate Agreement with NIBSS and forward a copy to the CBN.

ii. Ensure all qualifying accounts are properly maintained and visible to NIBSS on the Industry Customer Accounts Database (ICAD) or by any other service created or provisioned for this purpose.

iii. Ensure that accounts in NIBSS' ICAD are correctly tagged with correct BVN.

iv. Ensure and maintain connectivity to the Nigeria Central Switch.

v. Honour **ALL** balance enquiries and debit advices received from NIBSS for GSI Trigger in accordance with master agreement, including GSI recall instructions.

vi. Have adequate IT infrastructure to meet **ALL** the connectivity and protocol requirements at NIBSS and CBN.

vii. Provide access to customers' NUBAN accounts.

13.2 Reporting requirements

Every PSB shall provide reports of GSI activities as may be required by the Bank

(Soft copies of the reports shall be submitted to ***GSI-Returns@cbn.gov.ng*** no later than the 8th day after each month end; in alignment with routine monthly update of CRMS records' outstanding balances).

13.3 Accountability in PSBs

To ensure completeness, integrity, accuracy and timeliness of the GSI processes consistently, the:

i. The **Chief Risk Officer (CRO)** shall be accountable for the appropriateness of the entire GSI process.

ii. The **Chief Information/Technology Office (CIO or CTO)** shall ensure continuous connectivity to the GSI platform and availability of all internal systems to honour all GSI instructions and protocols (including the tagging of "Unavailable Accounts" for audit log/trail purposes. This does not absolve the PSB's MD/CEO of the overall responsibility over activities of the bank.

iii. CBN shall ensure adequate training for PSBs on GSI related processes and settlement procedures.

iv. The CBN shall apply the prescribed penalties to the erring PSBs and impose additional sanctions for grievous violations, malfeasance by a PSB. Disputes arising from other incidents not described herein may be settled by an Arbitrator.

14.0 COMPLIANCE WITH EXTANT LAWS AND REGULATIONS

Payment Service Banks shall comply with other relevant extant regulations for CBN licensed financial institutions and/or service providers. These include but are not limited to:

a) Cyber Security Framework issued by the CBN;

b) Nigeria Payment System Risk & Information Security Management Framework issued by the CBN;

c) Nigeria Financial Services Industry IT Standards Blueprint Version 2.1;

d) Data Protection Regulations;

e) CBN Consumer Protection Regulations;

f) Guidelines on Operation of Electronic Payment Channels in Nigeria;

g) Regulation on Agent Banking;

h) Regulations on Mobile Money Operations in Nigeria;

i) Guidelines on card issuance and usage in Nigeria;

j) Real-Time Gross Settlement (RTGS) rules and regulations, and S4 Business rules; and

k) All other regulations issued by the Bank as applicable.

15.0 MONITORING AND EVALUATION

Without prejudice to the provisions of section 12.0, to ensure effective monitoring and enforcement, Payment Service Banks shall be required to render monthly returns indicating the following:

a. Number of financially excluded/unbanked customers on-boarded during the month to which the returns relate;

b. Number of access points deployed in the month, as well as active access points and the cumulative access points deployed.

16.0 SANCTIONS

To ensure strict compliance with extant regulations, appropriate financial and administrative sanctions shall be imposed on erring Payment Service Banks and/or their principal officers, as provided for in relevant laws, regulations and guidelines.

Glossary

Business Continuity Plan (BCP) – also known as a Resolvability and Ever-Green Will is a plan to manage the continued operations of a business or the core elements of a business during a major incident or an event of a disaster. BCP ensures banks are more accountable for their crisis resolution preparedness and should be designed to make resolution more transparent, better understood, and lead to a successful outcome.

ICT – Information and Communication Technology.

IT – Information Technology

On-boarding – the integration of unbanked individuals into the banking system through a process of registering/opening bank accounts for them, as well as familiarizing them with financial services they can access via the bank or financial service provider.

Resolution authorities – An administrative national authority or authorities responsible for exercising the resolution powers over firms within the scope of the resolution regime e.g. resolution regime for financial institutions.

Unbanked / financially excluded – individuals or a sub-set of the economy (adults), with no/limited access to financial services of a bank or similar financial institutions such as accounts, access to credit etc.