AVA Capital Plc is registered and regulated by the Securities and Exchange Commission, Nigeria.

ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM, AND COUNTER-PROLIFERATION FINANCING POLICY

Policy Authors:	Compliance Department
Approval Authority	Board of Directors of AVA Capital Plc
Review Frequency	Annually or as needed

TABLE OF CONTENTS

PREAMBLE 4
1.0. DEFINITION OF TERMS 4
2.0 AML/CFT/CPF INSTITUTIONAL POLICY FRAMEWORK 10
2.1. SCOPE OF OFFENSIVE PROCEEDS 11
2.2 CUSTOMER DUE DILIGENCE (CDD) 13
2.3. HIGHER RISK CATEGORIES OF CLIENTS 17
2.4. Lower-Risk Clients and Transactions 17
2.5. TIMING OF VERIFICATION 19
2.6. FAILURE TO COMPLETE CDD 20
2.7. EXISTING CLIENTS 21
3.0. POLITICALLY EXPOSED PERSON (PEP) 21
4.0. NEW TECHNOLOGIES AND NON-FACE TRANSACTIONS 22
5.0. RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CDD FUNCTIONS 23
6.0 MAINTENANCE OF RECORDS ON TRANSACTIONS 23
7.0. ATTENTION ON COMPLEX AND UNUSUAL LARGE TRANSACTIONS 24
8.0 COMPLIANCE, MONITORING, AND RESPONSE TO SUSPICIOUS TRANSACTIONS 27
9.0. SANCTIONS FOR NON-COMPLIANCE 27
10.0 SHELL BANKS 28
11.0 SUSPICIOUS TRANSACTIONS “RED FLAGS” 28
13.0. MONITORING OF EMPLOYEE CONDUCT 30
14.0 PROTECTION OF STAFF WHO REPORT VIOLATIONS 30
15.0 ADDITIONAL AREAS OF AML/CFT RISKS 30
16.0. ADDITIONAL PROCEDURES AND MITIGANTS 31
17.0 TESTING FOR THE ADEQUACY OF THE AML/CFT COMPLIANCE 31
18.0 TERRORIST FINANCING OFFENCES 31
19.0 CULTURE OF COMPLIANCE 32
19.1 Guidance on KYC (Know Your Customer) 32
19.2 Duty to Obtain Identification Evidence 32
19.4 Apply Commercial Judgment 33
20.0 ESTABLISHING IDENTITY 33
20.1 Identification Evidence 33
20.2 What is Identity? 34

Address:
No. 1B, Professor Olagoke Olabisi Street, Lekki Phase 1, Lagos.

Tel:
+234 0700-0000-AVA

Website:
www.avacapitalplcgroup.com

20.3 When Must Identity be verified? 34
20.4 Whose Identity Must Be Verified? 34
20.6 Cancellation & Cooling-Off Rights 37
21.0 IDENTIFICATION PROCEDURES 37
21.1 General Principles 37
21.2 New Business for Existing Clients 38
21.3 Certification of Identification Documents 38
21.4 Recording Identification Evidence 39
21.5 Concession in Respect of Payments Made by Post or Electronic Transfer. 39
22.0 ESTABLISHING IDENTITY 40
22.1 Private Individual Clients 40
22.2 Documenting Evidence of Identity 42
22.3 Personal Identity Documents 42
22.4 Documentary Evidence of Address 42
22.5 Physical Checks on Private Individuals Resident in Nigeria 43
22.6 Electronic Checks 43
22.7 Private Individuals not resident in Nigeria 44
22.8. Private Individuals Not Resident in Nigeria: Supply of Information 45
22.9 Information to establish identity 45
22.9 Corporations/Partnerships 47
22.9.1. Information to Establish Identity 47
22.10 Other Types of Legal Arrangements and Non-Standard Entities 48
23.0 Low Risk Corporate Business 49
23.1 Public Quoted Companies 49
23.2 Private /Public unquoted Companies 50
24.0 Higher Risk Business Relating to Private/Public unquoted Companies 50
25. Policy Review 51

Address:
No. 1B, Professor Olagoke Olabisi Street, Lekki Phase 1, Lagos.

Tel:
+234 0700-0000-AVA

Website:
www.avacapitalplcgroup.com

PREAMBLE

AVA Capital Plc and all its subsidiaries' (AVA Global Asset Managers Limited, AVA Securities Limited, AVA Trustees, altogether hereinafter referred to as the "Group") are committed to maintaining the highest standards of integrity in the securities market and fully supporting the mandate of the Securities and Exchange Commission (the "Commission") to protect the market against all forms of abuse, including fraudulent and unfair trade practices.

In view of the increasing global significance of Anti-Money Laundering, Countering the Financing of Terrorism, and Counter-Proliferation Financing (AML/CFT/CPF) obligations, and the attendant risks they pose to the financial system in Nigeria and internationally, the need for robust, comprehensive, and effective preventive measures has become imperative.

Accordingly, the Group has developed this Know AML/CFT/CPF Policy in line with applicable Nigerian AML/CFT laws and regulations, the Investments and Securities Act 2025, the FATF Recommendations, and relevant international best practices. Economic and Financial Crimes Commission Act, Money Laundering Prevention and Prohibition Act 2022, and the Terrorism (Prevention and Prohibition) Act 2022.

This Policy is designed to reduce the risk of the Group being used as a conduit for money laundering or terrorist financing, while also protecting against fraud, reputational damage, and other financial and operational risks.

The Group is required to adopt a risk-based approach to the identification, assessment, and management of AML/CFT/CPF risks in accordance with applicable regulatory requirements. Non-compliance with these regulations and related AML/CFT/CPF laws may attract significant regulatory sanctions and penalties. It is therefore mandatory that the Group ensures full compliance with this Policy at all times, in line with the requirements set out herein.

1.0. DEFINITION OF TERMS

For the proper understanding of these Regulations, certain terms used are defined as follows: -

Accounts: a facility or an arrangement by which a financial institution: -

a) accepts deposits of currency;

b) allows withdrawals of currency or transfers into or out of the account;

c) pays cheques or payment orders drawn on a financial institution or cash dealer by a person or collects cheques or payment orders on behal21.5 Concession in Respect of Payments Made by Post or Electronic Transdeposit box.

Applicant for Business: the person or company seeking to establish a "business relationship' or an occasional client undertaking a 'one-off transaction whose identity must be verified.

Beneficiary: those natural persons, or groups of natural persons, who receive charitable, humanitarian, or other types of assistance through the services of the Non-Profit Organizations. They include all trusts (other than charitable or statutory permitted non-charitable trusts) that must have beneficiaries, who may include the settlor, and a maximum time, known as the perpetuity period,

Beneficial owner: the natural person(s) who ultimately owns or controls a client and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

BOFIA: Banks and Other Financial Institutions Act (as amended).

Business Relationship: is any arrangement between the Capital Market Operators 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.

Capital Market Operators: any person (individual or corporate) duly registered by the Commission to perform specific functions in the Capital Market.

Cooling off rights: the rights of an investor to return products purchased and get a refund if the individual changes his mind.

Cross-border transaction: any transaction where the originator and beneficiary Operators are located in different jurisdictions. This term also refers to any chain of transactions that has at least one cross-border element.

Designated categories of offences:

i. Participation in an organized crime group and racketeering;

ii. Terrorism, including terrorist financing;

iii. Trafficking in human beings and migrant smuggling; sexual exploitation, including sexual exploitation of children;

iv. Illicit trafficking in narcotic drugs and psychotropic substances; illicit arms trafficking;
v. Illicit trafficking in stolen and other goods; corruption and bribery; fraud;
vi. Counterfeiting currency;
vii. Counterfeiting and piracy of products; environmental crime;
viii. Murder, grievous bodily injury;
ix. Kidnapping, illegal restraint and hostage-taking; robbery or theft; smuggling; xix. extortion; forgery; piracy; and
x. Insider trading and market manipulation.

Designated non-financial businesses and professions:
I. Casinos (which also include internet casinos).
II. Real estate agency
III. Dealers in precious metals.
IV. Dealers in precious stones.
V, Legal practitioners, notary public, and accountants - means 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.

False disclosure: a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the disclosure or otherwise requested by the authorities. The FATF Recommendations means: The Forty Recommendations on Terrorist Financing.

Funds Transfer: any transaction carried out on behalf of an originator (both natural and legal) through Capital Market Operators by electronic means with a view to making an amount of money available to a beneficiary through another Capital Market Operator.
The originator and the beneficiary may be the same person.

ISA: The Investments and Securities Act, 2025

Legal persons: bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent client's relationship with Capital Market Operators or otherwise own property. Non-profit Organizations/Non-governmental.

Legal practitioners, notary public and accountants: 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;

MLPA: the Money Laundering Prevention and Prohibition Act, 2022

Nigerian Financial Intelligence Unit (NFIU): the central unit responsible for receiving, requesting, analyzing, and disseminating to the competent authorities disclosures of financial information concerning the suspected proceeds of crime and potential financing of terrorism.

One-off Transaction: any transaction carried out other than in the course of an established business relationship. It is important to determine whether a business applicant is undertaking a one-off transaction or whether the transaction is or will be a part of a business relationship, as this can affect the identification requirements.

Organizations: 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: the account holder, or where there is no account, the person (natural or legal) that places the order with the Capital Market Operators to perform the Capital Market Transaction.

Payable through account: correspondent accounts that are used directly by third parties to transact business on their own behalf.

Physical presence: meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

Politically exposed persons (PEPs) are individuals who are or have been entrusted with prominent public functions both in foreign countries and in Nigeria.

Proceeds: any property derived from or obtained, directly or indirectly, through the commission of an offence.

Property: assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.

Relevant authority: any person or organization that has a mandate over your activity as an individual.

Regulators: competent regulatory authorities responsible for ensuring compliance of Financial Institutions and Designated Non-Financial Institutions with requirements to combat money laundering and terrorist financing.

Risk: all references to risk in these regulations refer to the risk of money laundering and/or terrorist financing.

Settlor: persons or companies who transfer ownership of their assets to trustees by means of a trust deed. Where the trustees have some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter setting out what the settlor wishes to be done with the assets.

Shell bank: 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; and "physical presence" in relation to shell banks means: having structure and management located within a country and not merely the existence of a local agent or low-level staff;

Suspicious Transaction (For these regulations): a suspicious transaction may be defined as one which is unusual because of its size, volume, type, or pattern, or otherwise suggestive of known money laundering methods. It includes such a transaction that is inconsistent with a client's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.

TPA: The Terrorism (Prevention and Prohibition) Act, 2022

Terrorist: any natural person who

I. commits, or attempts to commit, terrorist acts by any means, directly or indirectly;

II. participates as an accomplice in terrorist acts;

III. organizes 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 to further the terrorist act or with the knowledge of the intention of the Group to commit a terrorist act.

Terrorist act: A terrorist act includes, but is not limited to: -

i. An act which constitutes an offence within the scope of, and as defined in one of the following treaties:

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

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

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

d. International Convention against the Taking of Hostages (1979),

Address:
No. 1B, Professor Olagoke Olabisi Street, Lekki Phase 1, Lagos.

Tel:
+234 0700-0000-AVA

Website:
www.avacapitalplcgroup.com

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

f. 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),

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

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

i. The International Convention for the Suppression of Terrorist Bombings (1997),

j. International Convention for the Suppression of the Financing of Terrorism (1999),

k. Convention on offences and certain other Acts committed on Board Aircraft, Convention on the Making of plastic Explosives for Detection (1991);

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

Terrorist financing (FT): includes the financing of terrorist acts, and of terrorists and terrorist organizations. Terrorist financing offence refers not only to the primary offence or offences, but also to ancillary offences.

Terrorist organization: any group of terrorists that:

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. organizes 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

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

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

Trust and Company Service providers: all persons or businesses that are not covered elsewhere under these Recommendations, and which, as a business, provide any of the following services to third parties;

i. acting as a formation agent of legal persons;

ii. acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

iii. providing a registered office;

iv. business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;

v. acting as (or arranging for another person to act as) a trustee of an express trust

vi. acting as (or arranging for another person to act as) a nominee shareholder for another person.

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

2.0 AML/CFT/CPF INSTITUTIONAL POLICY FRAMEWORK

A. General Guidelines on Institutional Policy

i. The Group shall adopt policies stating its commitment to comply with AML/CFT/CPF obligations under the law and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activity or terrorism.

ii. The Group shall formulate and implement internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations are always met.

B. AML/CFT/CPF Compliance Officer Designation and Duties

The Group shall designate its AML/CFT/CPF Compliance Officer with the relevant competence, authority, and independence to implement the institution's AML/CFT/CPF compliance programme.

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

I. Developing an AML/CFT/CPF Compliance Programme;

i. Rendering returns on Mandatory Disclosure and Suspicious Transactions

ii. Reports to the NFIU;

iii. Rendering returns on Foreign Exchange Transactions Reports to the SEC;

iv. Receiving and vetting suspicious transaction reports from staff;

v. Filing suspicious transaction reports with the NFIU;

vi. Rendering "nil" reports with the NFIU and the SEC, where necessary to ensure compliance;

vii. Ensuring that The Group's compliance programme is implemented;

viii. Coordinating the training of staff in AML/CFT/CPF awareness, detection methods, and reporting requirements; and

ix. Serving both as a liaison officer with the SEC and FIU and a point-of-contact for all employees on issues relating to money laundering and terrorist financing.

C. Cooperation with Relevant Authorities

The Group shall comply promptly and fully with all lawful requests for information issued by the Securities and Exchange Commission (SEC), the NFIU, and any other relevant regulatory or law enforcement authorities in relation to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) matters.

Where a request for information relating to suspected money laundering or terrorist financing is received, the Group shall:

i. Conduct an immediate search of its records to determine whether it maintains or has previously maintained any relationship, account, or transaction with the individual(s), entity(ies), or organisation(s) specified in the request;

ii. Promptly communicate the outcome of such search to the requesting authority in accordance with applicable legal and regulatory requirements;

iii. Maintain strict confidentiality and ensure the security of all such requests and related information, limiting access strictly to authorised personnel on a need-to-know basis.

2.1. SCOPE OF OFFENSIVE PROCEEDS

A. Identification and Reporting of Proceeds of Crime

The Group shall identify and report to the NFIU any transactions or activities suspected to involve proceeds of crime, including those arising from the following predicate offences:
i. Participation in an organized crime 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;
viii. Fraud;
ix. Counterfeiting currency;
x. Environmental crime;
xi. Murder, grievous bodily injury;
xii. Kidnapping, illegal restraint, and hostage taking;
xiii. Robbery or theft;
xiv. Smuggling;
xv. Extortion;
xvi. Forgery;
xvii. Piracy; and
xviii. Insider trading and market manipulation.
xix. Any other predicate offence as defined under applicable Nigerian AML/CFT/CPF legislation, including the Money Laundering (Prevention and Prohibition) Act and the Terrorism (Prevention and Prohibition) Act

B. Measures to Be Taken Against ML/TF

The Group recognises that obligations of confidentiality and professional secrecy shall not prevent the implementation of applicable Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT/CPF) requirements.
In this regard, and in accordance with applicable legislation, including the Economic and Financial Crimes Commission (Establishment) Act, the Money Laundering (Prevention and Prohibition) Act, and the Investments and Securities Act, the Group shall:
i. Ensure full cooperation with relevant competent authorities in the detection, investigation, and prevention of money laundering and terrorist financing;

ii. Facilitate lawful access to information by relevant authorities for the effective discharge of their statutory functions;
iii. Permit the sharing of information between competent domestic and international authorities, where required or permitted by law; and
iv. Share relevant information within the Group or with other regulated entities where necessary for compliance with AML/CFT/CPF obligations, subject to appropriate safeguards.

2.2 CUSTOMER DUE DILIGENCE (CDD)

i. The Group shall conduct Customer Due Diligence (CDD) in the following circumstances:
a. When establishing a business relationship;
b. When carrying out occasional transactions above the regulatory threshold as may be prescribed by the Securities and Exchange Commission from time to time, including single transactions or multiple transactions that appear to be linked;
c. When carrying out occasional wire transfers, whether domestic or cross-border, including transactions conducted through payment cards used for funds transfer purposes.
ii. For the avoidance of doubt, the following shall not be subject to wire transfer CDD requirements:

- Transactions arising from the use of credit or debit cards for payment of goods and services, ATM withdrawals, or cash advances;
- Transfers between Capital Market Operators where both the originator and beneficiary act on their own behalf;
- Any transaction where there is suspicion of money laundering or terrorist financing, in which case full CDD measures shall apply irrespective of thresholds;
- Situations where there are doubts regarding the accuracy, adequacy, or validity of previously obtained customer identification information.

iii. The Group shall not establish or maintain any relationship with shell banks. In line with applicable legislation, including the Banking and Other Financial Institutions Act (as amended), the Group shall also not enter into or continue correspondent relationships with foreign financial institutions that have no physical presence in any jurisdiction or that permit their accounts to be used by shell banks.
iv. The Group shall take reasonable measures to ensure that correspondent financial institutions do not allow their accounts to be used by shell banks. Where appropriate due

diligence has been completed, the Group shall not be required to repeat full identification and verification for every transaction unless triggered by risk indicators, changes in the relationship, or regulatory requirements.
v. The Group shall not open or maintain anonymous accounts or accounts in fictitious names. Where nominee arrangements are permitted, the Group shall ensure that the identity of the underlying beneficial owners is obtained, recorded, and made available to competent authorities upon lawful request

2.2.1 Customer Due Diligence (CDD) Measures

The Group shall implement appropriate Customer Due Diligence (CDD) measures to identify, verify, and understand its clients, their activities, and associated risks in accordance with applicable AML/CFT/CPF laws and regulations.

a. Customer Identification and Verification

The Group shall:
i. Apply the full range of CDD measures required under applicable laws and regulations;
ii. Identify all clients and verify their identities using reliable, independent sources, documents, or data;
iii. Obtain sufficient identification information for all clients. For legal persons and legal arrangements, this shall include, where applicable, the entity's legal name, registration details, registered address, nature of business, ownership structure, and authorised representatives.

b. Beneficial Ownership Identification

The Group shall:
i. Identify the beneficial owner(s) of every client and take reasonable measures to verify their identities using reliable and independent sources.
ii. Determine whether a client is acting on behalf of another person. Where a client acts on behalf of another person, the Group shall obtain sufficient identification information and verify the identity of the person for whom the client is acting.
iii. In relation to legal persons and legal arrangements, take reasonable measures to:

- Understand the ownership and control structure of the client;
- Identify the natural persons who ultimately own or control the client; and
- Verify the identities of such persons where required.

iv. The natural persons who ultimately own or control a client may include:

For Companies:

- Individuals who directly or indirectly own or control a significant ownership interest in the company; and
- Individuals who exercise ultimate effective control through management positions or other means.

For Trusts and Incorporated Trustees:

- The settlor or founder;
- Trustees;
- Protectors (where applicable);
- Beneficiaries or classes of beneficiaries;
- Individuals exercising ultimate effective control over the trust or incorporated trustee; and
- Any other natural person exercising ultimate ownership or control.

For Charitable Organisations, Foundations, Associations, and Non-Profit Organisations:

- Founders or promoters;
- Trustees, directors, or members of the governing council;
- Authorized signatories;
- Persons exercising significant influence or control over the organisation's activities, assets, or finances; and
- Any individual who ultimately controls or directs the organisation.

v. Where the client or the controlling shareholder is a publicly listed company subject to adequate regulatory disclosure requirements, the Group shall not be required to identify and verify individual shareholders of that public company.

c. Understanding the Business Relationship

The Group shall:

i. Obtain information on the purpose and intended nature of the business relationship before establishing the relationship.

ii. Understand the client's source of funds, source of wealth (where appropriate), expected transaction activity, and overall risk profile.

d. Ongoing Due Diligence and Monitoring

The Group shall:

i. Conduct ongoing monitoring of the business relationship to ensure that transactions are consistent with the Group's knowledge of the client, the client's business activities, risk profile, and source of funds, where applicable.

ii. Scrutinize transactions undertaken throughout the course of the relationship to identify unusual, complex, or suspicious activities.

iii. Ensure that customer identification documents, data, and information remain accurate, current, and relevant by conducting periodic reviews, particularly for higher-risk clients and business relationships.

iv. Monitor higher-risk clients and transactions more closely and on a risk-sensitive basis to detect suspicious or unusual activities.

e. Enhanced Monitoring and Risk Reclassification

Where a client's activities, transaction patterns, ownership structure, or other circumstances present a higher risk of money laundering, terrorist financing, or other financial crimes, the Group shall:

i. Apply Enhanced Due Diligence (EDD) measures proportionate to the identified risks.

ii. Assess all relevant circumstances before determining the client's risk rating and shall not automatically classify a client as high risk solely because additional caution is required.

iii. Reassess and, where appropriate, reclassify a client's risk rating if subsequent activity is inconsistent with the Group's understanding of the client.

iv. Consider filing a Suspicious Transaction Report (STR) where there are reasonable grounds for suspicion.

f. Failure to Complete Due Diligence

The Group shall not establish a business relationship, carry out a transaction, or continue an existing business relationship where it is unable to satisfactorily complete the required CDD measures. In such circumstances, the Group shall:

- Decline or terminate the business relationship, as appropriate;
- Consider whether a Suspicious Transaction Report (STR) should be filed with the relevant competent authority; and
- Maintain records of the decision and supporting rationale.

2.3. HIGHER RISK CATEGORIES OF CLIENTS

The basic principle of a risk-based approach is that the Group shall apply Enhanced Customer Due Diligence (CDD) for higher-risk clients, business relationships, and transactions, and Simplified CDD for lower-risk categories, in line with applicable AML/CFT/CPF regulations.

In assessing a client's risk profile, the Group shall treat the following as examples of higher-risk categories requiring enhanced caution at onboarding and during the course of the relationship.

a. Non-resident clients;

b. Clients from locations known for their high crime rate (e.g., drug production, trafficking, smuggling);

c. Clients from or in countries or jurisdictions which do not or insufficiently apply the FATF Recommendations (such as jurisdictions designated as Non-Cooperative Countries and Territories (NCCT) by the FATF or those known to the reporting institution to have inadequate AML/CFT/CPF laws and regulations);

d. Politically Exposed Persons (PEPs) and persons/ companies related to them;

e. Complex legal arrangements such as unregulated investment vehicles/special purpose vehicles (SPV);

f. Companies that have nominee-shareholders;

Upon determining clients as "high-risk", we shall undertake enhanced CDD process on the clients which shall include enquiries on:

a. the purpose for opening an account;

b. the level and nature of trading activities intended;

c. the ultimate beneficial owners;

d. the source of funds;

e. senior management's approval for opening the account;

We shall continue to undertake enhanced monitoring of the business relationship.

2.4. Lower-Risk Clients and Transactions

The Group may apply Simplified Due Diligence (SDD) or Reduced Customer Due Diligence (CDD) measures where it has determined, through a documented risk assessment, that a client, product, service, transaction, or business relationship presents a lower risk of money laundering, terrorist financing, or other financial crimes.

Simplified Due Diligence measures shall only be applied where permitted by applicable laws and regulations and shall be proportionate to the identified level of risk.

a. Circumstances Indicating Lower Risk

A client, transaction, or business relationship may be considered lower risk where:

i. The risk of money laundering or terrorist financing is assessed as low;

ii. Information relating to the identity of the client and beneficial owner is publicly available from reliable and independent sources;

iii. Adequate transparency, oversight, and regulatory controls exist within the relevant jurisdiction or sector; and

iv. The client, product, or transaction exhibits characteristics consistent with a lower risk profile as determined by the Group's risk assessment framework.

b. Examples of Lower-Risk Clients

Subject to a risk-based assessment, the following categories of clients may be considered lower risk:

i. financial institutions and regulated entities that are subject to AML/CFT/CPF requirements equivalent to applicable regulatory standards and are effectively supervised for compliance;

ii. Publicly listed companies whose securities are traded on recognized stock exchanges and which are subject to regulatory disclosure requirements;

iii. Government ministries, departments, agencies, parastatals, and government-owned enterprises;

iv. Life insurance policies where premiums fall within thresholds prescribed by the relevant regulatory authority;

v. Insurance policies established for pension or retirement schemes where there is no surrender value and the policy cannot be used as collateral;

vi. Pension, superannuation, retirement benefit, or similar employee benefit schemes funded through payroll deductions, provided the scheme rules do not permit the assignment or transfer of a member's interest; and

vii. Beneficial owners of pooled accounts maintained by regulated Designated Non-Financial Businesses and Professions (DNFBPs), provided such entities are subject to

AML/CFT/CPF obligations and supervision consistent with applicable laws and regulations.

c. Foreign Clients

Where Simplified Due Diligence measures are applied to clients' residents in foreign jurisdictions, the Group shall ensure that such jurisdictions have effectively implemented internationally recognized AML/CFT/CPF standards, including the recommendations of the Financial Action Task Force (FATF).

d. Risk-Based Application of Simplified Due Diligence

The Group shall apply Customer Due Diligence measures on a risk-sensitive basis and shall determine, on a case-by-case basis, whether Simplified Due Diligence is appropriate. In making this determination, the Group shall consider factors including:

- The nature and profile of the client;
- The ownership and control structure of the client;
- The products and services being utilized;
- The nature, size, and complexity of the transaction;
- The delivery channel used;
- The geographical location and jurisdiction of the client; and
- Any other relevant risk factors identified during the onboarding process or ongoing monitoring.

The application of Simplified Due Diligence shall not exempt the Group from its obligation to conduct ongoing monitoring, identify suspicious activity, or comply with any other applicable AML/CFT/CPF requirements.

2.5. TIMING OF VERIFICATION

We shall verify the identity of clients, beneficial owners, and occasional clients before or at the time of establishing a business relationship or conducting transactions on their behalf. In exceptional circumstances, the verification of a client's and beneficial owner's identity may be completed after the establishment of the business relationship, provided that:

a. Verification is carried out as soon as reasonably practicable thereafter;

b. Deferring verification is necessary so as not to interrupt the normal conduct of business; and

c. The associated money laundering and terrorism financing risks are effectively managed and mitigated.

Circumstances Where Deferred Verification May Be Permitted

Examples of situations where immediate verification may be impracticable due to the need to maintain normal business operations include:

a. Securities transactions: In the securities sector, transactions may need to be executed rapidly in response to prevailing market conditions at the time instructions are received. In such cases, execution may be required before completion of identity verification.

b. Non-face-to-face business relationships: Where clients are not physically present, verification may be completed after the establishment of the relationship, subject to appropriate risk controls.

Risk Management Controls for Pre-Verification Activity

Where clients are permitted to engage in transactions prior to completion of identity verification, appropriate risk management procedures shall be implemented. These shall include, at a minimum:

- Restrictions on the number, type, and/or value of transactions permitted before verification; and
- Enhanced monitoring of transactions, particularly those that are large, complex, or inconsistent with the expected profile of the business relationship

2.6. FAILURE TO COMPLETE CDD

i. Prospective clients who fail to comply with the Customer Due Diligence (CDD) requirements set out above shall:

a. Not be permitted to open an account, establish a business relationship, or carry out any transaction; and

b. Be reported by the Group through the filing of a Suspicious Transaction Report (STR) to the NFIU, where applicable.

ii. Where a business relationship has already been established, and the client subsequently fails to complete the required CDD measures, the Group shall:

a. Terminate the business relationship; and

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

2.7. EXISTING CLIENTS

i. The Group shall apply Customer Due Diligence (CDD) measures to existing clients on a risk-sensitive and materiality basis and shall continue to conduct ongoing due diligence on all established business relationships at appropriate intervals.

ii. The appropriate circumstances for undertaking or updating CDD on existing clients shall include, but are not limited to, the following:

a. Where a transaction of significant value is initiated or conducted;

b. Where there are substantial changes to the client's documentation or identification standards;

c. Where there is a material change in the manner in which the account or business relationship is operated; and

d. Where the Group becomes aware that it holds insufficient or incomplete information regarding an existing client.

iii. The Group shall ensure that clients are properly identified and verified in accordance with the above criteria. All client identification and verification records shall be maintained and made accessible to the AML/CFT/CPF Compliance Officer, relevant authorised personnel, and regulatory or law enforcement authorities, where required

3.0. POLITICALLY EXPOSED PERSON (PEP)

A. Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions both in foreign countries and in Nigeria. Examples of PEPs include, but are not limited to;

i. Heads of State or government;

ii. Governors;

iii. Local government chairmen;

iv. Senior politicians;

v. Senior government officials;

vi. Judicial or military officials;

vii. Senior executives of state-owned corporations;

viii. Important political party officials;

ix. Family members or close associates of PEPs; and
x. Members of Royal Families.

B. The Group, in addition to performing CDD measures, has established appropriate risk management systems to determine whether a potential client, existing clients, or the The beneficial owner is a politically exposed person.

C. Senior management approval shall be obtained before establishing business relationships with PEPs, and monthly returns on any transaction with PEPs shall be rendered to the NFIU.

D. Where a client has been accepted or has an ongoing relationship with The Group and the client or beneficial-owner is subsequently found to be or becomes a PEP, The Group is required to obtain senior management approval to continue the business relationship.

E Reasonable measures shall be taken to establish the source of wealth and the sources of funds of clients and beneficial-owners identified as PEPs, and all anomalies shall be reported immediately to the SEC and NFIU.

F. Where the Group is in a business relationship with PEPs, it shall conduct enhanced ongoing monitoring of that relationship. In the event of any transaction that is abnormal, the Group shall flag the account and report immediately to the NFIU.

4.0. NEW TECHNOLOGIES AND NON-FACE TRANSACTIONS

The Group shall put in place: -

a. policies or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes, such as internationally accepted Credit or Debit Cards.

b. policies and procedures to address any specific risks associated with non -face to face business relationships or transactions. These policies and procedures shall be applied automatically when establishing a client's relationships and conducting ongoing due diligence.

c. If the Group relies upon a third party, it shall immediately obtain the necessary information concerning property which has been laundered or which constitutes proceeds from instrumentalities used in and intended for use in the commission of money laundering and financing of terrorism or other predicate offences. The Group shall satisfy itself that copies of identification data and other relevant documentation relating to the CDD

requirements are made available by the third party upon request without delay.
d. The Group shall be satisfied that the third party is a regulated institution with measures in place to comply with the requirements of CDD.

5.0. RELIANCE ON INTERMEDIARIES AND THIRD PARTIES ON CDD FUNCTIONS

Where The Group relies on intermediaries or other third parties that are not operating under an outsourcing or agency arrangement, and where business relationships, accounts, or transactions are introduced through such third parties, The Group shall ensure that appropriate elements of the Customer Due Diligence (CDD) process are adequately performed in respect of the introduced business. In such cases, the following minimum requirements shall be met:
i. The Group shall promptly obtain from the third party all necessary information relating to relevant elements of the CDD process;
ii. The Group shall take reasonable steps to ensure that copies of identification data and any other relevant CDD documentation will be made available by the third party upon request, without delay;
iii. The Group shall satisfy itself that the third party is regulated in accordance with internationally recognised AML/CFT/CPF Core Principles and has appropriate systems and controls in place to comply with applicable CDD requirements; and
iv. The Group shall ensure that adequate Know Your Customer (KYC) provisions are applied to the third party to enable the timely provision of relevant account and customer information to competent authorities when required.
Notwithstanding any reliance on a third party, the ultimate responsibility for the identification and verification of clients shall remain with The Group.

6.0 MAINTENANCE OF RECORDS ON TRANSACTIONS

The Group shall;
a. Maintain all necessary records of transactions, both domestic and international, for at least six years following completion of the transaction (or longer if requested by the SEC and NFIU in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.
b. Maintain records of the identification data, account files, and business correspondence for at least six years following the termination of an account or business relationship (or longer if requested by the SEC and NFIU in specific cases).

Address:
No. 1B, Professor Olagoke Olabisi Street, Lekki Phase 1, Lagos.
Tel:
+234 0700-0000-AVA
Website:
www.avacapitalplcgroup.com

c. Ensure that all client transaction records and information are available on a timely basis to the SEC and NFIU.

Some of the necessary components of transaction records to be kept include clients' and beneficiaries' names, addresses (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

7.0. ATTENTION ON COMPLEX AND UNUSUAL LARGE TRANSACTIONS

The Group shall pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Such transactions or patterns of transactions include:

i. significant transactions relative to a relationship,

ii. transactions that exceed certain limits,

iii. very high account turnover, inconsistent with the size of the account balance, or

iv. transactions that fall out of the regular pattern of the account's activity.

The Group shall examine as far as possible the background and purpose for such transactions and set forth their findings in writing to the NFIU; such findings shall be kept available for SEC, NFIU, other relevant authorities, and auditors for at least five years.

8.0 COMPLIANCE, MONITORING, AND RESPONSE TO SUSPICIOUS TRANSACTIONS

The Group shall:

i. Establish and maintain a documented policy framework that enables employees to identify, monitor, investigate, and appropriately respond to suspicious transactions and activities that may be indicative of money laundering, terrorist financing, or other financial crimes.

ii. Designate a suitably qualified and independent AML/CFT/CPF Compliance Officer with responsibility for overseeing the monitoring, investigation, and reporting of suspicious transactions, as well as ensuring compliance with applicable AML/CFT/CPF laws, regulations, and internal policies.

iii. Remain vigilant to known indicators and typologies of money laundering, terrorist financing, and other predicate offences. The Group shall maintain and periodically update a list of red flags and suspicious transaction indicators and ensure that such guidance is communicated to all relevant employees.

iv. Where any employee identifies a red flag or suspects that a transaction or activity may be linked to money laundering, terrorist financing, or other criminal conduct, the matter shall be escalated immediately to the AML/CFT/CPF Compliance Officer for review and investigation. Where necessary, a review panel may be constituted under the supervision of the AML/CFT/CPF Compliance Officer to assess the matter. All actions, findings, and decisions arising from such investigations shall be properly documented and retained. The Group and its employees shall maintain strict confidentiality throughout the review process and in relation to any Suspicious Transaction Report (STR) filed with the relevant authorities. This requirement is intended to ensure compliance with applicable anti-tipping-off provisions under relevant AML/CFT/CPF laws and regulations.

v. Where The Group knows, suspects, or has reasonable grounds to suspect that funds or assets are the proceeds of criminal activity, are linked to terrorist financing, or are otherwise connected to unlawful conduct, it shall submit a Suspicious Transaction Report (STR) to the NFIU within the prescribed regulatory timeframe. All suspicious transactions, including attempted transactions, shall be reported regardless of the amount involved and irrespective of whether the suspicion relates to tax matters or any other predicate offence.

vi. The Group, its directors, officers, employees, and any other persons acting on its behalf, whether on a permanent, temporary, or contractual basis, shall not disclose to any client or unauthorized person that a Suspicious Transaction Report has been filed, is being considered, or that an investigation relating to money laundering, terrorist financing, or other financial crimes is being conducted.

vii. The Group shall ensure that all employees receive periodic training on the identification, escalation, investigation, and reporting of suspicious transactions and on their obligations under applicable AML/CFT/CPF laws and internal policies.

8.1 Internal controls, compliance, and audit

i. The Group shall establish, implement, and maintain effective internal policies, procedures, systems, and controls designed to prevent, detect, and mitigate the risks of money laundering, terrorist financing, and other financial crimes.

Such policies and procedures shall be communicated to all employees and shall, at a minimum, address:

a. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) requirements;

b. Record retention and retention periods;

c. The identification, monitoring, and investigation of unusual and suspicious transactions;

d. Internal escalation and reporting procedures;
e. Suspicious Transaction Reporting obligations; and
f. Any other measures necessary to ensure compliance with applicable AML/CFT/CPF laws, regulations, and regulatory guidelines.

The AML/CFT/CPF Compliance Officer and other authorized personnel shall have timely and unrestricted access to client identification data, CDD information, transaction records, and any other information necessary to effectively discharge their AML/CFT/CPF responsibilities.

ii. The Group shall establish and maintain a comprehensive AML/CFT/CPF compliance programme which shall include:

a. The development and implementation of internal policies, procedures, controls, and compliance management arrangements designed to effectively manage AML/CFT/CPF risks;
b. Appropriate employee screening and vetting procedures to promote high standards of integrity, competence, and professionalism in recruitment and ongoing employment;
c. An ongoing AML/CFT/CPF training programme to ensure that employees remain informed of emerging money laundering and terrorist financing risks, typologies, techniques, methods, and trends, as well as their obligations under applicable AML/CFT/CPF laws, regulations, and internal policies. Such training shall specifically cover customer due diligence requirements, ongoing monitoring obligations, and suspicious transaction identification and reporting procedures; and
d. An independent and adequately resourced audit function responsible for periodically reviewing and testing the effectiveness of The Group's AML/CFT/CPF policies, procedures, controls, and compliance programme and reporting its findings to senior management and, where appropriate, the Board of Directors.

iii. The Group shall establish and maintain governance arrangements that ensure the operational independence, authority, and effectiveness of the Chief Compliance Officer (CCO) and the AML/CFT/CPF Compliance Officer, enabling them to perform their duties objectively and without undue influence, interference, or conflicts of interest.

iv. The Board of Directors and Senior Management shall be responsible for providing adequate oversight, resources, and support to ensure the effective implementation and continuous improvement of The Group's AML/CFT/CPF compliance framework.

This version strengthens the governance and independence provisions and aligns the section with international AML/CFT/CPF best practices and regulatory expectations.

8.2 Employee Education and Training Programme

A. The Group shall design a comprehensive employee education and training program not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT/CPF tasks.

B. The timing, coverage, and content of the employee training program shall be tailored to meet the perceived needs of The Group. The Group shall render quarterly returns on their level of compliance to the SEC and NFIU.

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

i. AML/CFT/CPF regulations and offences;

ii. The nature of money laundering;

iii. Money laundering ‘red flags and suspicious transactions, including trade-based

iv. Money laundering typologies;

v. Reporting requirements;

vi. Clients’ due diligence;

vii. Risk-based approach to AML/CFT/CPF;

viii. Record keeping and retention policy.

D. The Group shall submit its Annual AML/CFT/CPF Employee training program to the SEC and NFIU not later than the 31st of December every financial year against the next year.

9.0. SANCTIONS FOR NON-COMPLIANCE

The sanctions set out under this Policy and applicable regulatory requirements are intended to be effective, proportionate, and dissuasive. Such sanctions may be imposed on The Group, its directors, senior management, officers, and employees, depending on the nature and severity of the breach.

Any failure by The Group to comply with, or any contravention of, the provisions of applicable AML/CFT/CPF laws, regulations, guidelines, or this Policy may result in regulatory, administrative, civil, or other sanctions imposed by the Securities and Exchange Commission (SEC) and/or any other competent regulatory or law enforcement authority.

Any director, officer, employee, or other responsible person within The Group who fails to take reasonable steps to ensure compliance with applicable AML/CFT/CPF requirements shall be subject to appropriate disciplinary, administrative, or regulatory sanctions.

Without prejudice to any other sanctions that may apply, any false declaration, misrepresentation, concealment of material information, or false disclosure made by The Group or any of its directors, officers, employees, or representatives shall constitute a serious breach and may result in regulatory investigation, administrative review, enforcement action, and the imposition of applicable sanctions by the relevant authorities.

10.0 SHELL BANKS

Shell banks are financial institutions that have no physical presence, management, or meaningful operations in the jurisdiction in which they are incorporated or licensed and are not affiliated with a regulated financial group subject to effective consolidated supervision.

In accordance with applicable laws and regulations, including the Banks and Other Financial Institutions Act (BOFIA), shell banks are prohibited from operating in Nigeria.

The Group shall not establish or maintain correspondent relationships with shell banks or other high-risk foreign financial institutions that lack a physical presence in any jurisdiction. The Group shall also not enter into or continue correspondent relationships with any financial institution that permits its accounts to be used, directly or indirectly, by shell banks.

11.0 SUSPICIOUS TRANSACTIONS “RED FLAGS”

A. Potential Transactions Perceived or Identified as Suspicious

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 activity involving monetary instruments such as traveler’s cheques, bank drafts, money orders, particularly those that are serially numbered.

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

B. Terrorist Financing “Red flags”

i. Persons involved in a transaction share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed);

ii. Securities transaction by a non-profit 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. Large volume of securities transactions through a business account, where there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations;
iv. The stated occupation of the clients is inconsistent with the type and level of account activity;
v. Multiple personal and business accounts or the accounts of non-profit organizations or charities that are used to collect and channel securities to a small number of foreign beneficiaries.

C. Other Unusual or Suspicious Activities

i. Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.
ii. Employee failure to comply with approved operating guidelines.
iii. Employee is reluctant to take a vacation.

D. Other forms of reporting. The Group is expected to comply with reporting all securities transactions in any currency above a threshold of N5, 000,000 for individuals and N10, 000,000 for corporate persons to the NFIU.

12.0. ATTENTION FOR HIGHER RISK COUNTRIES

A. The Group shall give special attention to business relationships and transactions with persons (including legal persons and other Capital Market Operators) from or in countries that do not or insufficiently apply the FATF recommendations.
B. The Group shall report, as stated below, transactions that have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined and written findings made available to assist competent authorities such as the SEC, NFIU, auditors, and law enforcement agencies (LEAs) to carry out their duties.
C. Where the Group conducts business with foreign institutions that have failed to apply or have insufficiently applied the provisions of FATF Recommendations, the Group is required to take measures such as the following:
i. Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories to The Group for identification of the beneficial

Address:
No. 1B, Professor Olagoke Olabisi Street, Lekki Phase 1, Lagos.
Tel:
+234 0700-0000-AVA
Website:
www.avacapitalplcgroup.com

owners before business relationships are established with individuals or companies from that jurisdiction;

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

iii. In considering requests for approving the establishment in countries applying the countermeasure of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant Capital Market Operator is from a country that does not have adequate AML/CFT/CPF systems;

13.0. MONITORING OF EMPLOYEE CONDUCT

The Group shall monitor its employees' accounts for potential signs of money laundering. They are also required to subject employees' accounts to the same AML/CFT/CPF procedures as applicable to other clients' accounts. This is required to be performed under the supervision of the AML/CFT/CPF Compliance Officer. The latter's own account is to be reviewed by the Internal Auditor or a person of adequate/similar seniority. Compliance reports, including findings, are to be rendered to the SEC /NFIU.

14.0 PROTECTION OF STAFF WHO REPORT VIOLATIONS

The Group shall direct its employees in writing to always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to them. They are also required to make it possible for employees to report any violations of the institution's AML/CFT/CPF compliance program to the AML/CFT/CPF Compliance Officer. Where the violations involve the Compliance Officer, employees are required to report such to a designated higher authority, such as the Internal Auditor. The Group shall inform its employees in writing to make such reports confidential and that they will be protected from victimization for making them.

15.0 ADDITIONAL AREAS OF AML/CFT/CPF RISKS

A. The Group shall review, identify, and record other areas of potential money laundering risks not covered by these Compliance Regulations and report the same quarterly to the NFIU.

B. The Group shall review its AML/CFT/CPF 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/CPF Compliance Regulations.

16.0. ADDITIONAL PROCEDURES AND MITIGANTS

Having reviewed the AML/CFT/CPF framework and identified new areas of potential money laundering vulnerabilities and risks, the Group shall design additional procedures and mitigations as a contingency plan in its AML/CFT/CPF Operational Regulations. These will provide how such potential risks will be appropriately managed if they crystallize. Details of the contingency plan are to be rendered to the SEC and NFIU as at 31st December every financial year.

17.0 TESTING FOR THE ADEQUACY OF THE AML/CFT/CPF COMPLIANCE

The Group shall make a policy commitment and to subject its AML/CFT/CPF Compliance Program to independent-testing or require its internal audit function to determine its adequacy, completeness, and effectiveness. A report of compliance is required to be rendered to the SEC and NFIU as 31st December every financial year. Any identified weaknesses or inadequacies shall be promptly addressed by The Group.

18.0 TERRORIST FINANCING OFFENCES

1. Any person or entity who, in or outside Nigeria –

a. solicits, acquires, provides, collects, receives, possesses, or makes available funds, property, or other services by any means to –

i. terrorists, or

ii. terrorist groups, directly or indirectly, with the intention or knowledge, or having reasonable grounds to believe that such funds or property will be used in full or in part to commit an offence under these regulations or in breach of the provisions of these regulations,

2. possesses funds intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act by a terrorist or terrorist groups, commits an offence under these regulations and is liable on conviction to imprisonment for life.

3. Any person who knowingly –

a. which facilitates the acquisition, retention, or control by or on behalf of another person of terrorist funds by concealment, removal out of jurisdiction, transfer to a nominee, or in any other way, or

b. as a result of which funds or other property are to be made available for terrorism or for the benefit of a specified entity or proscribed organization, commits an offence under these regulations and is liable on conviction for life imprisonment.

4. For an act to constitute an offence under this section, it is not necessary that the funds or property were actually used to commit any offence of terrorism.

19.0 CULTURE OF COMPLIANCE

The Group shall implement a comprehensive AML/CFT/CPF compliance program to guide its compliance efforts and to ensure the diligent implementation of its regulations.

19.1 Guidance on KYC (Know Your Customer)

The Group shall not establish a business relationship until all relevant parties to the relationship have been identified and the nature of the business that they intend to conduct is ascertained. Once an ongoing business relationship is established, any inconsistent activity can then be examined to determine whether or not there is an element of money laundering for suspicion.

19.2 Duty to Obtain Identification Evidence

I. The Group shall be satisfied that a prospective client is who they claim to be before establishing any business relationship or executing any transaction.

II. Where a client is acting on behalf of another person, including where funds are provided by a third party or where the investment is to be held in another person's name, The Group shall verify the identity of both the client and the agent, trustee, or intermediary. This requirement shall not apply where the client is itself a regulated Nigerian Capital Market Operator.

III. The Group shall obtain satisfactory identification evidence for all clients, except where otherwise provided under these regulations.

IV. The Group shall ensure that all relevant parties to a business relationship are identified and verified from the outset in accordance with applicable AML/CFT/CPF requirements.

19.3 Nature and Level of the Business

The Group shall obtain sufficient information on the nature of the business that their client

intends to undertake, including the expected or predictable pattern of transactions.
The information collected at the outset for this purpose shall include: -
a. purpose and reason for opening the account or establishing the relationship;
b. nature of the activity that is to be undertaken;
c. expected origin of the funds to be used during the relationship; and
d. details of occupation/employment/business activities and sources of wealth or income.
ii. The Group shall take reasonable steps to keep the information up to date as opportunities arise, such as when an existing client opens a new account. Information obtained during any meeting, discussion, or other communication with the clients shall be recorded and kept in the client's file to ensure, as far as practicable, that current clients' information is readily accessible to the Money Laundering Compliance Officers (MLCO) or relevant regulatory bodies.

19.4 Apply Commercial Judgment

The Group shall apply a risk-based approach to Know Your Customer (KYC) requirements and exercise appropriate commercial judgment in determining the extent, frequency, and nature of client verification during the course of the business relationship, including when additional checks are required.
For personal accounts, all joint account holders shall be identified and verified in accordance with applicable AML/CFT/CPF requirements. In the case of private companies or partnerships, the Group shall focus on identifying and verifying the principal owners and controllers.
The identification evidence obtained at the outset shall be assessed in light of the inherent risks associated with the client, product, service, and jurisdiction, and shall be supplemented with additional checks where necessary.

20.0 ESTABLISHING IDENTITY

20.1 Identification Evidence

i. The client's identification process shall not start and end at the point of establishing the relationship but continue as far as the business relationship subsists. The process of confirming and updating identity and address, and the extent of obtaining additional KYC

information collected is used by The Group.
ii. The general principles for establishing the identity of both legal and natural persons and obtaining satisfactory identification evidence set out in these regulations are by no means exhaustive.

20.2 What is Identity?

i. Identity generally means a set of attributes such as names used, date of birth and the residential address at which the clients can be located. These are features which can uniquely identify a natural or legal person.
ii. In the case of a natural person, the date of birth is required to be obtained as an important identifier in support of the name. It is, however, not mandatory to verify the date of birth provided by the clients.
iii. Where an international passport/national identity card is taken as evidence of identity, the number, date and place/country of issue (as well as expiring date in the case of international passport) are required to be recorded.

20.3 When Must Identity be verified?

i. Identity shall be verified whenever a business relationship is to be established, on account opening or during one-off transaction or when series of linked transactions take place. “Transaction” in these regulations is defined to include the giving of advice.
ii. Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that clients are complete and kept, no further evidence of identity is needed when another transaction or activity is subsequently undertaken.

20.4 Whose Identity Must Be Verified?

The Group shall obtain sufficient identification evidence to verify that each client is the person they claim to be. Where a person is acting on behalf of another, The Group shall obtain and verify the identity of both the client and the person acting on their behalf.
There is no obligation to look beyond the client where:
i. The latter is acting on its own account (rather than for a specific client or group of clients);
ii. A client is a bank, broker, fund manager or other regulated Capital Market Operators,

iii. Financial institutions and all businesses are to be undertaken in the name of a regulated Capital Market Operator or financial institution.
iv. In other circumstances, unless the client is a regulated Capital Market Operator or financial institution acting as agent on behalf of one or more underlying clients within Nigeria, and has given written assurance that it has obtained the recorded-evidence of identity to the required standards, identification evidence shall be verified for:
a. the named account holder/person in whose name an investment is registered;
b. any principal beneficial owner of funds being invested who is not the account holder or named investor;
c. the principal controller(s) of an account or business relationship (i.e. those who regularly provide instructions); and
d. any intermediate parties (e.g., where an account is managed or owned by an intermediary).
The Group shall take appropriate steps to identify:
i. directors and all the signatories to an account.
ii. Joint applicants/account holders - identification evidence shall be obtained for all the account holders.
iii. For higher risk business undertaken for private companies (i.e., those not listed on the stock exchange), sufficient evidence of identity and address shall be verified in respect of:
iii. the principal underlying beneficial owner(s) of the company with 5% interest and above; and
iv. Those with principal control over the company's assets (e.g., principal controllers/directors).
v. Trusts – We shall obtain and verify the identity of those providing funds for the Trust. They include the settlor and those who are authorized to invest, transfer funds, or make decisions on behalf of the Trust, such as the trustees and controllers who have the power to remove the Trustees.
vi. Savings Schemes and Investments in Third Parties' Names When an investor sets up a savings accounts or a regular savings scheme whereby the funds are supplied by one person for investment in the name of another (such as a spouse or a child), the person who funds the subscription or makes deposits into the savings scheme shall be regarded as the applicant for business for whom identification evidence must be obtained in addition to the legal owner.

vii. Personal Pension Schemes

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

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

20.5 Timing of Identification Requirements: -

An acceptable time-span for obtaining satisfactory evidence of identity will be determined by the nature of the business, the geographical location of the parties, and whether it is possible to obtain the evidence before commitments are entered into or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regard to the risk.

To this end, the Group 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. Discontinue any activity it is conducting for the client; and bring to an end any understanding reached with the client where the client does not supply the required information as stipulated above.

The Group shall observe the provisions in the timing of verification under the AML/CFT/CPF Directive of these regulations. We may, however, start processing the transaction or application immediately, provided that we:

a. promptly takes appropriate steps to obtain identification evidence;

b. do not transfer or pay any money out to a third party until the identification requirements have been satisfied.

The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time-frame without adequate explanation may lead to a suspicion that the depositor or investor is engaged in money laundering. The Capital Market Operator shall therefore make Suspicious transaction reports to NFIU based on the information in its possession before the funds involved are returned to the potential client or where they came from. We shall respond promptly to inquiries made by other persons relating to the identity of their clients.

20.6 Cancellation & Cooling-Off Rights

Where an investor exercises cancellation rights or cooling-off rights, the sum invested must be repaid, subject to some deductions, where applicable. Since cancellation/cooling-off rights could offer a readily available route for laundering money, The Group shall be alert to any abnormal exercise of these rights by an investor or in respect of business introduced through an intermediary. If abnormal exercise of these rights becomes apparent, the matter shall be treated as suspicious and reported to NFIU.

21.0 IDENTIFICATION PROCEDURES

21.1 General Principles

i. The Group shall take reasonable measures to verify that it is dealing with a genuine natural person, legal person, or legal arrangement by obtaining adequate and reliable identification and verification information. Where reliance is placed on a third party to conduct identification or verification, the ultimate responsibility for obtaining satisfactory identification evidence shall remain with The Group.

ii. In all cases, The Group shall obtain sufficient evidence to establish the identity of the customer, confirm the validity of the address provided, and, where applicable, identify the beneficial owners and authorized representatives of a corporate entity or legal arrangement.

iii. As no single form of identification can provide absolute assurance of identity, The Group shall adopt a risk-based and cumulative approach to customer identification and verification, utilizing multiple sources of information where appropriate.

iv. The methods used to verify the identity of individual customers, including whether identification was conducted face-to-face or through non-face-to-face channels, shall be documented and maintained in the customer file. The Group shall also document the reasonable measures taken to mitigate the risk of impersonation, fictitious identities, duplicate applications, or other forms of identity-related fraud.

v. A referral or introduction from an existing client, a director, senior management, or a member of staff may provide additional comfort regarding a customer's legitimacy, but shall not substitute for the Group's customer identification and verification requirements. Details of the individual who made and approved the introduction shall be retained in the customer's file together with all relevant supporting records. Directors and Senior Management shall ensure strict adherence to the prescribed customer identification procedures for all applicants without exception.

21.2 New Business for Existing Clients

i. When an existing client closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address of such a client unless the name or the address provided does not tally with the information in The Group's database.

However, procedures shall be put in place to guard against impersonation and fraud. The opportunity of opening the new account shall also be taken to ask the client to confirm the relevant details and to provide any missing KYC information. This is particularly important:

a. if there was an existing business relationship with the client and identification evidence had not previously been obtained; or

b. if there had been no recent contact or correspondence with the client within the past three (3) months; or

c. when a previously dormant account is re -activated.

ii. In the circumstances above, details of the previous account(s) and any identification evidence previously obtained or any introduction records shall be linked to the new account records and retained for the prescribed period in accordance with the provisions of these Regulations.

21.3 Certification of Identification Documents

i. To guard against the dangers of postal-interception and fraud, prospective client shall not be asked to send by post originals of their valuable personal identity documents, such as an international passport, identity card, driving license, etc.

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

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

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

b. a senior official within the account opening institution;

c. Notary public/court of competent jurisdiction

iv. Certified copies of identification evidence are to be stamped, dated and signed "original sighted by me" by a senior officer of The Group. We shall always ensure that a good production of the photographic evidence of identity is obtained. Where this is not possible, a copy of evidence certified as providing a good likeness of the applicant could only be acceptable in the interim.

21.4 Recording Identification Evidence

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

ii. Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence are required to be recorded to enable the documents to be obtained later. Confirmation is required to be provided that the original documents were seen by certifying either on the photocopies or on the record that the details were taken down as evidence.

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

21.5 Concession in Respect of Payments Made by Post or Electronic Transfer.

i. The Group may apply simplified verification measures for low-risk products and services, including long-term life insurance policies and personal investment products, where payment is received from an account held in the customer's name, either solely or jointly with one or more persons. In such circumstances, and subject to The Group's risk assessment, no additional evidence of identity may be required.

ii. The waiver of additional verification requirements for postal or electronic transactions shall not apply in the following circumstances:

a. Products or accounts that permit funds to be transferred to other products or accounts offering cheque issuance, payment, or money transfer facilities;

b. Situations where funds may be repaid or transferred to a person other than the original customer;

c. Investments or accounts whose features may subsequently be altered to permit payments or transfers to third parties.

iii. The postal concession shall not constitute an exemption from the requirement to obtain satisfactory evidence of a customer's identity. A payment debited from an account in the customer's name may, where appropriate, serve as identification evidence for the purposes of customer verification.

iv. The Group shall maintain adequate records showing how each transaction originated, including details of the account from which the cheque, electronic payment, or other remittance was made.

v. This concession may apply where an application is submitted directly to The Group or where payment is made through a regulated intermediary, subject to The Group's assessment of the associated money laundering and terrorist financing risks.

vi.In the case of investment funds, where an investment balance is transferred from one fund manager to another and the value of the transfer exceeds US$10,000, N5,000,000 for an individual, or N 10,000,000 for a body corporate, and customer identification evidence has neither been obtained nor confirmed by the original fund manager, The Group shall obtain and verify such identification evidence at the time of the transfer.

22.0 ESTABLISHING IDENTITY

Establishing identity under these regulations is divided into three broad categories:

a. Private individual clients;

b. Quasi corporate clients;

c. Pure corporate clients

22.1 Private Individual Clients

I. The Group shall obtain and independently verify the following information for all private individuals whose identities are required to be established:

a. The individual's full legal name, including any other names by which the individual is known; and

b. The individual's permanent residential address, including relevant landmarks and postal code, where available.

ii. The information obtained shall be sufficient to establish that the individual exists, resides at the address provided, and is the person presenting or applying for the product or service. Where an individual has recently changed residence, reasonable measures shall be taken to verify the previous residential address.

iii. The Group shall obtain the customer's date of birth, as this information may be required by law enforcement and regulatory authorities. While verification of the date of birth may not always be mandatory, the Group shall also ascertain the customer's nationality and country of residence as part of its customer risk assessment process.

iv. The Group shall apply a risk-based approach to customer identification and verification. The nature and extent of verification measures shall be determined by factors including the level of money laundering and terrorist financing risk associated with the customer, product, service, delivery channel, and geographic location. Applications submitted through non-face-to-face channels, such as telephone, post, or electronic platforms, may require enhanced verification measures where appropriate.

The source of funds, method of payment, origin of the funds, and the identity of the person making the payment shall be recorded and maintained to provide a clear audit trail. For higher-risk customers, products, or transactions, the Group shall take additional measures to establish and verify the customer's source of wealth and source of funds.

v. Notwithstanding the lower risk associated with certain transactions or simple investment products, the Group shall always satisfy itself as to the identity and residential address of the customer before establishing a business relationship or carrying out a transaction.

Private Individuals Resident in Nigeria (Foreign Nationals)

vi. For foreign private individuals' resident in Nigeria, confirmation of the customer's full legal name and residential address shall be established through reliable and independent sources. Verification shall be conducted by cross-checking the information provided against valid documentary evidence (including international travel or residence documentation where applicable), electronic databases, or a combination of both methods.

vii. The Group shall ensure that the identification evidence obtained is adequate, reliable, and sufficient to verify the customer's identity and residential status in Nigeria. The ultimate responsibility for ensuring that customer identification and verification requirements are satisfactorily fulfilled shall remain with the Group.

22.2 Documenting Evidence of Identity

In order to mitigate the risk of forged or counterfeit documentation, the Group shall take appropriate steps to ensure that all documents presented for identification purposes are original.

Where original documents are not immediately available, certified copies may be accepted on an interim basis. Such copies must be duly dated, signed, and endorsed as "original seen" by a senior public servant or an equivalent authorized officer within a reputable private organization. The original documents shall, however, be obtained and verified by the Group within a reasonable timeframe.

The following are examples of acceptable documentary evidence for Nigerian resident private individuals:

22.3 Personal Identity Documents

i. Current International Passport

ii. Residence Permit issued by the Immigration Authorities

iii. Current Driving License issued by the Federal Road Safety Commission (FRSC)

iv. Inland Revenue Tax Clearance Certificate

v. Birth Certificate/Sworn Declaration of Age

vi. National Identity card

vii. Permanent Voters Card

22.4 Documentary Evidence of Address

i. Record of home visit in respect of non-Nigerians

ii.Confirmation from the electoral register that a person of that name lives at that address

iii. Recent utility bill (e.g. PHCN, NITEL, etc.)

iv. Current driving licence issued by FRSC

v. Bank statement or passbook containing current address

vi. Solicitor's letter confirming recent house purchase or search report from the Land Registry

vii. Tenancy Agreement

viii. Search reports on prospective client's place of employment and residence signed by a senior officer of the Group

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

22.5 Physical Checks on Private Individuals Resident in Nigeria

I. It shall be mandatory for the Group to establish the true identity and residential address of all clients and to implement effective measures to prevent impersonation, substitution of identity, or identity fraud.

ii. Additional confirmation of the client's identity, and verification that the application has been made by the identified individual, shall be obtained through one or more of the following procedures:

a. Direct mailing of account opening documentation to a named individual at an independently verified residential address, with confirmation of receipt where appropriate;

b. Receipt of an initial deposit instrument (e.g., cheque or transfer) drawn from a personal account in the client's name held with another regulated Capital Market Operator or financial institution in Nigeria;

c. Telephone or electronic contact with the client prior to account activation, using an independently verified residential or business contact number, or a "welcome call" conducted prior to permitting transactions, using a minimum of two previously obtained personal identity data points for authentication;

d. Internet or electronic platform sign-on, following verification procedures where the client utilizes security credentials such as passwords, tokens, or other authentication mechanisms issued and delivered securely to the named individual at an independently verified address;

e. Card, account, or platform activation procedures requiring confirmation of identity prior to enabling transactional access.

iii. The Group shall ensure that additional information regarding the nature and expected level of business activity, as well as the source of funds to be used in the relationship, is obtained from the client at onboarding and periodically updated where necessary.

22.6 Electronic Checks

i. The Group shall implement appropriate measures to verify the identity of all clients and ensure safeguards are in place to prevent impersonation, identity fraud, and misuse of customer information.

ii. A risk-based approach shall be applied in determining the extent of verification required during onboarding and throughout the business relationship. The level of checks shall be commensurate with the client risk profile, product type, delivery channel, and transaction activity.

iii. Customer identity and onboarding authenticity may be verified using a combination of the following measures, as appropriate:

a. Verification against reliable government-issued identity systems and independent electronic databases;

b. Biometric verification tools, including national identity validation, facial recognition, or liveness detection;

c. Electronic confirmation of bank account ownership or regulated financial institution verification;

d. Multi-factor authentication methods such as OTPs, secure credentials, or token-based authentication;

e. Secure digital onboarding solutions incorporating document authentication, tamper detection, and automated validation checks;

f. Supplementary direct communication with the client using verified channels, where required for higher-risk cases.

iv. The Group shall obtain sufficient information on the nature and purpose of the business relationship, including source of funds and, where applicable, source of wealth, particularly for higher-risk clients.

v. All verification processes and supporting records shall be properly documented, retained in line with regulatory requirements, and subject to ongoing review to ensure continued effectiveness throughout the client lifecycle.

22.7 Private Individuals not resident in Nigeria

i. For prospective clients who are non-residents of Nigeria but who make face-to-face contact, the Group shall obtain valid identification documents such as an international passport or national identity card as evidence of identity. Relevant details including document number, date of issue, and issuing country shall be recorded and retained in the client file.

ii. The Group shall obtain independent and reliable evidence of the client's permanent residential address from appropriate sources. A P.O. Box address alone shall not be accepted as valid proof of residence. The residential address provided must be capable of physical verification where necessary.

iii. Identification and address verification may be obtained directly from the client or through reputable third parties, including regulated financial institutions or Capital Market Operators in the client's country of residence. Where foreign-issued documents or third-party verification are relied upon, enhanced due diligence shall be applied to confirm authenticity and validity. Copies of all relevant identification documents shall be obtained and retained.

iv. Where a foreign national has recently arrived in Nigeria, the Group may obtain supplementary verification evidence, including employment confirmation, educational institution records, or travel documentation, as part of the overall risk-based assessment of identity and address.

22.8. Private Individuals Not Resident in Nigeria: Supply of Information

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

ii. Documentary evidence of name and address can be obtained: -

a. by way of original documentary evidence supplied by the clients;

b. by way of a certified copy of the client's passport or national identity card and a separate certified document verifying address e.g. a driving licence, utility bill, etc; or through a branch, subsidiary, head office of a correspondent bank.

c. Where the client does not already have a business relationship with the foreign Capital Market Operators that is supplying the information, certified copies of relevant underlying documentary evidence must be sought, obtained and retained by the institutions.

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

22.9 Information to establish identity

a. Natural Persons For natural persons the following information shall be obtained, where applicable:

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

ii. Correct permanent address (full address shall be obtained and a Post Office box number is not sufficient);

iii. Telephone number, fax number, and e-mail address;

iv. Date and place of birth;

v. Nationality;
vi. Occupation, public position held and name of employer;
vii. An official personal identification number or other unique identifier contained in an
viii. Unexpired official document such as passport, identification card, residence permit, social
ix. Security records or driving licence that bears a photograph of the clients;
x. Signature.
xi. Confirmation of BVN via NIBSS
The Group shall verify this information by at least one of the following methods: -
i. Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records);
ii. Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
iii. Contacting the clients by telephone, by letter or e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e mail address shall warrant further investigation);
iv. Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public);
v. Such other documents of an equivalent nature may be produced as satisfactory evidence of clients' identity;
vi. We shall apply effective client identification procedures for non-face-to-face client as for those available physically; from the information provided, we shall be able to make an initial assessment of a client's risk profile. Particular attention needs to be focused on those clients identified as having a higher risk profile. Additional inquiries made or information obtained in respect of those clients shall include the following:
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 client of the same institution);
c. Prior client bank reference and contact with the bank regarding the client;
d. Source of wealth;
e. Verification of employment, public position held (where appropriate).
The client acceptance policy shall not be so restrictive to amount to a denial of access by the general public to Securities transactions, especially for people who are financially or

socially disadvantaged.

22.9 Corporations/Partnerships

a. For corporate entities and partnerships, the Group shall take reasonable measures to understand the ownership and control structure of the customer and identify the natural persons who ultimately own or control the entity, including those exercising ultimate effective control over its assets and operations.

b. For corporate customers, the Group shall pay particular attention to shareholders, authorised signatories, and other persons who provide significant financial support, exercise material influence, or otherwise have control over the management or decision-making of the entity. Where ownership or control is exercised through another regulated entity, trust, or Capital Market Operator, the Group shall take reasonable steps to identify and verify the natural persons behind such structures.

c. For this policy, “control” shall include individuals who have authority to manage accounts, funds, or investments without requiring further approval, or who are in a position to override established internal controls and governance mechanisms.

d. For partnerships, all partners shall be identified. The Group shall also consider identifying individuals who exercise significant control over the partnership, including where relevant, immediate family members with ownership or controlling interests.

e. Where the customer is a company listed on a recognised securities exchange, or a subsidiary of such a listed entity, simplified due diligence may be applied to the entity itself, provided that the Group remains satisfied that there is no effective control by an individual, small group of individuals, or another legal arrangement. Where such control exists, the controlling persons shall be identified and verified in accordance with beneficial ownership requirements.

22.9.1. Information to Establish Identity

For corporate entities (including companies and partnerships), the Group shall obtain sufficient information to establish the legal identity, ownership structure, and nature of business of the entity. Such information shall include:

i. Registered name of the entity;

ii. Principal place of business;

iii. Registered or correspondence address;

iv. Contact details, including telephone number and email address where available;

v. Official identification or registration number, where applicable (e.g., Tax Identification

Number);
vi. Evidence of legal incorporation or existence, such as Certificate of Incorporation and constitutional documents (e.g., Memorandum and Articles of Association or equivalent);
vii. Board resolution or equivalent authorisation confirming the opening of the account and identifying persons authorised to operate the account;
viii. Nature, purpose, and legitimacy of the business relationship.

Verification of Information

The Group shall verify the above information using a risk-based approach and one or more of the following methods:

a. Review of audited financial statements or annual reports, where available;

b. Confirmation through reputable business information services or verification by regulated professionals such as lawyers or accountants;

c. Corporate registry searches (e.g., Corporate Affairs Commission or equivalent) to confirm legal status, including whether the entity is active, dissolved, struck off, or in liquidation;

d. Use of reliable electronic databases or independent data verification tools;

e. Obtaining bank references, where appropriate and available;

f. Direct interaction with the corporate entity through site visits, telephone, email, or other secure communication channels, where necessary;

g. Verification of the identity, authority, and reputation of any third party or agent acting on behalf of the corporate entity, particularly where the agent is not a formally appointed officer of the entity.

22.10 Other Types of Legal Arrangements and Non-Standard Entities

i. For Retirement Benefit Programmes, mutual or friendly societies, cooperatives, provident societies, charities, clubs, associations, trusts, foundations, and professional intermediaries, the Group shall obtain additional information in addition to the standard customer identification requirements applicable to principals and authorised signatories.

ii. Such additional information shall include, as appropriate:

a. The registered or official name of the entity;

b. Registered or correspondence address;

c. Contact details, including telephone numbers and email address where available;

d. Official identification or registration number (such as tax identification number or equivalent);
e. A description of the entity's purpose, nature of activities, and governance structure, as set out in its constitutional or formation documents;
f. Evidence of legal existence and registration, such as incorporation documents, regulatory licences, trust deeds, or registration with relevant authorities (e.g., charity or cooperative registries).
iii. The Group shall apply a risk-based approach in assessing such entities and shall ensure that appropriate due diligence is conducted on controlling persons, trustees, and authorised representatives, as applicable.

23.0 Low Risk Corporate Business

23.1 Public Quoted Companies

i. corporate clients that are listed on a recognised securities exchange are generally considered lower risk due to the regulatory disclosure and governance requirements applicable to such entities. Accordingly, the Group is not required to verify the identity of individual shareholders in such listed entities.
ii. It is not required to identify all directors of a publicly listed company solely for customer due diligence purposes, provided the entity maintains adequate public disclosure and regulatory oversight.
iii. The Group shall, however, take reasonable measures to ensure that the listed entity or its officers are not being used for illicit purposes, including fraud, money laundering, or other financial crime. The Group shall obtain appropriate evidence of authority (such as a board resolution or equivalent mandate) for any individual acting on behalf of the entity. Where appropriate, the Group may conduct additional verification through direct communication with senior officers of the entity.
iv. Where the applicant is:
a. A company listed on a recognised securities exchange; or
b. A wholly owned subsidiary, or a subsidiary under the control of such a listed company, and this can be independently verified, the Group may apply simplified due diligence, subject to ongoing monitoring.
v. Notwithstanding the above, the Group shall apply enhanced due diligence where the nature of the account, transaction profile, or service requested presents a higher risk of money laundering or terrorist financing.

23.2 Private /Public unquoted Companies

i. Where the customer is a private or unlisted company and the principal directors or shareholders do not already maintain an established relationship with the Group, the Group shall obtain and verify sufficient documentation to confirm the legal existence, ownership structure, and control of the entity.

ii. Such verification shall include, as appropriate:

a. Evidence of incorporation or registration, including the company's registered address and details of directors and shareholders;

b. Independent confirmation through reliable sources such as the Corporate Affairs Commission (CAC) or reputable business information services;

c. Where appropriate, confirmation or certification from a qualified professional (e.g., lawyer or accountant) attesting to the authenticity of the submitted documents.

iii. The Group shall assess the reliability, origin, and integrity of all documents obtained, taking into account the jurisdiction of incorporation and associated risk factors.

iv. Where satisfactory documentary verification of the entity cannot be obtained, the Group shall conduct enhanced due diligence on the entity's beneficial owners and controllers in line with applicable risk-based procedures.

24.0 Higher Risk Business Relating to Private/Public unquoted Companies

i. For private or unlisted companies engaged in higher-risk business, the Group shall, in addition to verifying the legal existence of the entity, take reasonable measures to identify and verify the natural persons who ultimately own or control the company and its assets.

ii. The Group shall obtain identification evidence for shareholders with significant ownership or control, which, for this policy, shall generally include shareholding or interest of 5% or more, or any other threshold deemed material based on risk assessment and the nature of the entity.

iii. Control shall be deemed to include persons who have authority to manage accounts, funds, or investments without requiring additional approval and who are in a position to override internal governance or control mechanisms.

iv. The Group shall identify and verify all beneficial owners and other persons exercising ultimate control over the entity. Where ownership or control is exercised through another corporate entity, trust, or similar structure, the Group shall apply a "look-through" approach to identify and verify the ultimate beneficial owners, settlors, or controllers. Any change in beneficial ownership or control shall trigger updated verification in accordance with the Group's KYC requirements.

v. Directors who do not exercise ownership or controlling influence, as well as authorised signatories, shall be identified and assessed on a risk-based basis.

vi. Where there is a change in transaction patterns, account activity, or business profile that is unusual or inconsistent with the expected profile, the Group shall conduct further due diligence to determine the source and nature of such changes.

vii. Enhanced due diligence shall be applied to companies incorporated in offshore jurisdictions or International Business Companies (IBCs), with particular attention to transparency of ownership, control structures, and the legitimacy of the business activities.

25. Policy Review

i. This Policy shall be reviewed at least annually, or more frequently where required due to changes in applicable laws, regulations, regulatory guidance, or the Group's business operations.

ii. The Policy shall also be reviewed following any significant regulatory developments, internal audit findings, compliance breaches, or material changes in the Group's risk profile.

iii. All amendments to this Policy shall be subject to review and approval by the appropriate governance authority, including the Compliance Function and the Board or delegated committee, as applicable.

26. Approval

This Board of AVA Capital Plc adopts this AML/CFT/CPF Policy, consistent with the Group Governance Framework.

DR. ADEYINKA ADEDEJI
CHAIRMAN

DR. HAUWA BABAKOBI
DIRECTOR