EUROCOMM SECURITIES LIMITED

(MEMBER OF THE NIGERIAN STOCK EXCHANGE)

COMPLIANCE / ANTI MONEY LAUNDERING POLICY

COMPLIANCE AND ANTI-MONEY LAUNDERING/COUNTER TERRORIST FINANCIAL MANUAL

Contents

COMPLIANCE AND **ANTI-MONEY LAUNDERING/COUNTER TERRORIST FINANCIAL** MANUAL

1.0 INTRODUCTION

As a very highly ethical and professional institution and to ensure safe and sound business practices in line with regulatory requirements, Eurocomm Securities Limited developed and adopted this KYC and Anti-Money Laundering (AML) and Combating of Financing of Terrorism (CFT) policy.

The Anti-Money Laundering (AML), Know Your Customer (KYC) and Combating of Financing of Terrorism (CFT) policy was formulated by the company in line with the following guidelines:

Eurocomm Securities Limited business strategy

Industry practices

SEC Rules

SEC AML/CFT Compliance Manual for Capital Market Operators and Other

Financial Institutions in Nigeria

NDLEA, EFCC, NFIU and other Law Enforcement Agencies regulations
GIABA
Financial Action Task Force (FATF)

To abide by minimum international ethical standard and comply with regulatory requirements, the policy outlined in this manual represents the minimum acceptable standard and controls that guides KYC and Anti-Money Laundering (AML)/ Combating of Financing Terrorism (CFT) activities within the company.

The AML/CFT/KYC policy stipulates basic ethical principles and effective procedures to identify clients, decline and report suspicious transactions and co-operate with iaw enforcement agencies

2.0 ESTABLISHING CLIENTS' IDENTITY

2.1 Identification Evidence

The company's client's identification process should not start and end at the point of establishing the relationship but continue as far as the business relationship subsists. The process of confirming and updating identity and address, and the extent of obtaining additional KYC information may differ depending on the type of client involved.

The general principles for establishing the identity of both legal and natural persons and the guidance on obtaining satisfactory identification evidence are by no means exhaustive and will also be guided by other requirements that may be released to capital market operators from time to time by regulators and applicable laws.

2.2 What is identity?

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

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

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

2.3 When Must Identity be verified?

Identity is required to 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 this Policy and Procedure Manual is defined to be the giving of advice. The "advice" here does not apply to when information is provided about the availability of services nor applies to when a first interview/discussion prior to establishing a relationship takes place.

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

2,4 **Redemptions/Surrenders**

When an investor finally realizes his investment (wholly or partially), if the amount payable is US $10,000 or above or its equivalent thereof; or /45,000,000 for an individual or ff10,000,000 for a body corporate, r such other monetary amounts as may, from time to time, be stipulated by any

applicable money laundering legislation or regulation, the identity of the investor must be verified and recorded if it had not been done previously.

In the case of redemption or surrender of an investment (wholly or partially), the company will take reasonable measures to establish the identity of the investor where payment is made to.

The legal owner of the investment by means of a cheque crossed "account payee only"

A bank account held in the name of the legal owner of the investment by any electronic means effective for transfer of funds.

2.5 Whose Identity Must Be Verified?

Client's sufficient evidence of the identity must be obtained to ascertained that the client is the very person he/she claims to be.

The person acting on behalf of another-The Company has the obligation to obtain sufficient evidence of identities of the two persons involved.

There is no obligation to look beyond the client where:

- He trades on its own account (rather than for a specific client or group of clients);
- The client is a broker, fund manager or other regulated financial institutions; and
- All the businesses are to be undertaken in the name of a regulated financial institution.

A. The company should take appropriate steps to identify directors and all the signatories to an account.
B. Joint applicants/account holders- identification evidence should be obtained for all the account holders.
C. For higher risk business undertaken for private companies (i.e. those not listed on the stock exchange NGX, NASD and any other trading platform. sufficient evidence of identity and address should be verified in respect of:

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

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

D. The company should be alert to circumstances that might indicate any significant change in the nature of the business or its ownership and make enquires accordingly and to observe the additional provisions for Higher Risk Categories of Clients under AML/CFT in this Manual.
E. Trust — The Company shall obtain and verify the identity of those providing funds for the Trust. .They include the settler and those who are authorized to invest, transfer funds or make decisions on behalf of the Trust such as the principal trustees and controllers who have power to remove the Trustees.
F. Savings Schemes and Investments in Third Parties' Names:
When an investor sets up an account whereby the funds are supplied by one person for investment in the name of another (such as a spouse or a child), the company should regard the person who funds the subscription or makes deposits into the account as the applicant for business for whom identification evidence must be obtained in addition to the legal owner.

2.6 Personal Pension Schemes:

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

2.7 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 and must be approved by the Managing Director.

To this end, the company is required to:

(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 transaction; and
(b) Where the client does not supply the required information as stipulated in (a) above, the company will discontinue any activity it is conducting for the client; and bring to an end any understanding reached with the client.

The company shall observe the provision in the Timing of Verification as contained in this AML/CFT Policy and Procedure Manual.

The company may however start processing the business or application immediately, provided that it:

(a) Promptly takes appropriate steps to obtain identification evidence and
(b) Does not transfer or pay any money until the identification requirements have been satisfied.

3.0 CLIENT IDENTIFICATION PROCEDURES

3.1 Client Acceptance Procedures

The basic client acceptance policies and procedures of Eurocomm Securities Ltd will require the account officer to obtain all relevant information necessary to establish relationship with client which will not likely pose any risk to the company considering the following factors:

a. -Client's background
b, -Purpose and intended nature of business relationship
c. -Nature and type of transactions (cash, cheque, funds transfer, etc)
d. -Sources of funds
e. -Country of origin

The relationship officer must adhere strictly to the minimum account opening documentations requirements for the various types of accounts.

Extensive due diligence is essential for an individual with a high net worth whose source of funds is unclear.

Decisions to enter into business relationships with higher risk clients, such as Politically Exposed Persons (PEPs) must be approved by the MD and reported to the Board.

3.2 Procedures to Establish Identity of all Clients

Eurocomm Securities Limited will view client identification as an essential element of the KYC standards.

The client identification process will apply at the outset of the relationship. All existing clients must have their mandate documents reviewed and updated when it is necessary to do so.

Eurocomrn Securities Ltd will establish a systematic procedure for identifying new clients and should not establish any relationship until the identity of a new client is satisfactorily established.

Any transactions from client that appear to be illegitimate must be promptly investigated and declined if need be. In addition, regular checks must be undertaken by relationship officers to ensure that clients do not engage in trade on any prohibition list.

All accounts (personal and corporate) are to be regularly monitored especially as it affects the threshold limit or amount defined by the Money Laundering (Prohibition) Act 2004.

In any case of suspicious transaction, prompt report (with full disclosures) should be made to the Chief Compliance Officers notwithstanding the veil of client's right of confidentiality.

The company must never agree to open an account or conduct ongoing business with a client who insists on anonymity or who gives a fictitious name.

For all suspected drug-related or Money Laundering Cases, the establishment of a satisfactory audit trail is a necessity.

3.3 Responsibility of Members of Management

Management staffs are to provide inputs on new means by which illegitimate money are being laundered to enable the Chief Compliance Officer advice the appropriate authorities.

Staffing: There will be proper and adequate staffing screening procedures to ensure high standards when hiring new employees. •

3.4 Responsibility of the Chief Compliance Officer (CCO)

He must ensure that the company is in full compliance with the provisions of the Money Laundering (Prohibition) Act 2004.

b. He should ensure that there is ongoing employee training programme to adequately create awareness in KYC procedures. The CCO should arrange necessary AML/CFT training awareness for staff at all level.

C. He should align the company's AML policy and procedures with evolving

Statutory and regulatory directives of NDLEA, EFCC and other relevant international laws and standards e.g. FATF.

d. He should represent the company at all Law Enforcement Agencies and

Regulatory Bodies (National Drug Law Enforcement Agency and EFCC)

meetings.

e. He should ensure that the company complies with laid down AML policies.

f. He should regularly undertake internal review of all suspicious transactions and returns with a view to determining whether or not such suspicious transactions have substance and require disclosure to EFCC and NIFU.

g. He should ensure that the company makes routine reports to NIFU and NDLEA in respect of weekly returns or any specific suspicious reports.

h. To serve as liaison officer with SEC, NGX, NFIU as well as contact for all staff on issues of money laundering.

3.5 Responsibility of all Employees.

a. All staff must be vigilant, at all times, to the possibility of money laundering activities.

b. They must comply fully with all Money Laundering procedures in respect of client identification, account monitoring and record keeping.

C. They must report promptly to the Compliance Officer all suspicious deposits and transactions or collusion in respect of Money Laundering activities.

d. They must conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions conducted are consistent with the company's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

e. When an account has been opened, but problems of verification arise in the stock broking relationship which cannot be resolved, the account should be closed and the funds returned to the source from which they were received.

4.0 INTERMEDIARIES OR OTHER THIRD PARTIES TO VERIFY IDENTITY OR INTRODUCE BUSINESS

4.1 Who to rely upon and the circumstances

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

- Undertake the identification procedure when introducing a client and to obtain any additional KYC information from the client; or
- Confirm the identification details if the client is not resident in Nigeria; or
- Confirm that the verification of identity has been carried out (if an agent is acting for underlying principals).

4.2 Introduction from Authorized Financial Intermediaries

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

4.3 Written Applications

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

If these procedures are followed, the company will be considered to have fulfilled its own identification obligations. However, if the letter is not forthcoming from the intermediary, or the letter indicates that the

Intermediary has not verified the identity of the applicant, the company will satisfy its obligation by applying its own direct identification procedures.

4.4 Non-written Applications

Where the company receives non-written applications from financial intermediaries (where a deal is placed over the telephone or by other electronic means), it has an obligation to verify the identity of clients and ensure that the intermediary provides specific confirmation that identity has been verified. A record must be made of the answers given by the intermediary and retained for a minimum period of five years after severance of relationship. These answers constitute sufficient evidence of identity in the hands of the company.

4.5 Introductions from Foreign Intermediaries

Where introduced business is received by the company from a regulated financial intermediary who is outside Nigeria, the reliance that can be placed on that intermediary to undertake the verification of identity-check must be assessed by the Money Laundering Compliance Officer or some other competent persons within the company on a case by case basis based on the knowledge of the intermediary. In any case, such business and client must be approved by the MD and reported to the Board.

CLIENT DUE DILIGENCE (CDD)/KNOW YOUR CLIENT (KYC)

The company should undertake client due diligence measures, including identifying and verifying the identity of its clients, when:

- Establishing business relations
- carrying out occasional transactions above the applicable designated threshold
- there is a suspicion of money laundering or terrorist financing
- the company has doubts about the veracity or adequacy of previously obtained client identification data.

The client due diligence (CDD) measures to be undertaken by the company will require the relationship manager to adopt the following:

- identify the client and verify the client's identity using reliable, independent source documents, data or information
- identify the beneficial owner of account to be opened and taking reasonable measures to verify the identity of the beneficial owner
- take reasonable measures to understand the ownership and control structure of the client

- obtain information on the purpose and intended nature of the business relationship
- conduct ongoing due diligence on the business relationship and monitoring of transactions undertaken throughout the course of the relationship

5.0 PERSONAL CLIENTS - VERIFICATION OF IDENTITY

The internal process on new accounts opening will require that a two level verification process be carried out. The account officer will be in charge of the first level while the Compliance officer will carry out second level verification before account is opened. First and foremost, account-opening forms (comprehensive information and KYC forms) are filled by the client detailing all required information.

A good form of verification of identity will be by way of personal introduction from known and reputable/respected clients.

a. Positive identification should be obtained from documents issued by reputable sources and file copies (certified true copy of the original by the account officer) should be retained while reference numbers and other relevant details should be recorded as required by the Act and Financial Action Task Force (FATF) standards.
b. The following information should be obtained from all prospective clients:
   True name and/or names used;
   Occupation/Business;
   Detailed and verifiable permanent address;
   - Date of birth;
   - Nationality; Bank Verification Number
   - Relationship with other stock broking firms;
   Mother's maiden name;
   - National ID, International Passport, Driver's License etc

The best identification documents possible should be obtained from the prospective client (i.e. those that are the most difficult to obtain illicitly). However, it must be appreciated that no form of identification can be fully guaranteed as genuine or representing correct identity. Identification documents sought should be pre-signed and preferably bear a photograph. The following documents are acceptable under existing regulations:

Current valid International passport.
Valid National Driver's License.
National Identity card.
Voter's card

The company may however in exceptional circumstances accept a Notary Certificate or Identification by a prominent member of the community of the

Prospective client in cases where the aforementioned forms of identification required by existing regulation is unobtainable.

In addition, the name and permanent address should be verified through one or more of the following:

Requesting sight of a recent utility bill;
Confirmation letter from employer;
Physical visit to the address given by the prospective client and a duly signed visitation report form completed by the account officer.

5.1' **Non-Nigerian Resident Clients**

For prospective clients who are not normally resident in Nigeria and where verification of identity cannot be obtained through a Nigerian-based account, an international passport or national identity card and Resident Permit should be sought to verify their identity.

5.2 Corporate Clients

Corporate accounts are some of the most likely vehicles used for money laundering, particularly when fronted by a legitimate trading company. It is therefore important to identify the directors, major shareholders, account *signatories* and nature of the corporate business.

In order to prevent Eurocomm Securities Limited from being used by natural persons as a method of operating anonymous corporate accounts, account officer must ensure proper understanding of the structure of the company, determine the source of the funds, and identify the beneficial owners and those who have control over the funds.

5.3 Companies Registered In Nigeria

The following relevant documents must be obtained in respect of new accounts for companies incorporated in Nigeria:

- Memorandum and Articles of Association.
  Certificate of Incorporation or Certificate of Registration of Trade.
  Signed application form, or an account opening authority containing specimen signatures.
  Form CO7 (List of Directors)
  Form CO2 (Statement of Share Capital)
  Board Resolution authorizing opening of the Account.

a. In order to ensure compliance with requirements on client's identification, the company's Operations Manager must review all account opening packages to confirm completeness.
b. Verification of Sources of Funds: In addition to client's identification, the company as a matter of prudence and in fulfillment of AML regulations, must take steps to know the business of its clients to ensure that not only the initial funds but also subsequent funds in the account are not proceeds of illegal activities.

   Before an account opened, independent verification of the nature of business and source of revenues must be undertaken by the account officer. This will form part of the basis upon which the company will be able to fulfill obligations on Suspicious Transactions Reporting (STR) under the Money Laundering (Prohibition) Act 2004.

   In addition, the company through the account officer should verify that the business of the client is not connected to the items on any import prohibition list.

5.4 **Accounts** Opened **on behalf of a Third Party/Trust Accounts**

Where an account is being opened on behalf of a minor or other third party, for example by a trustee or a nominee, care must be taken to check the identity of all parties to the account in line with account opening procedures for other personal or Corporate accounts (See section 3 of this document).

The identification of a trust account should include the trustees, settlers/grantors and beneficiaries.

6.0 RISK CATEGORISATION OF CLIENTS

6.1 High Risk Categories of Clients

The company shall perform Enhanced Due Diligence (EDD) for higher-risk categories of client, business relationship or transaction. Examples of higher-risk client categories include:

a) Non-resident clients;
b) Legal persons or legal arrangements such as trusts that are personal-assets-holding vehicles;
c) Companies that have nominees-shareholders or shares in bearer form;
d) Politically Exposed Persons (PEPs), cross-border business relationships and
e) Financially Exposed Persons (FEPs), etc.

Where there are low risks, the company will apply reduced or simplified Measures. There are low risks in circumstances where the risks of money laundering or terrorist financing is lower, where information on the identity of the client and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in national systems. In circumstances of low-risk, capital market operators are required to apply the simplified or reduced CDD measures when identifying and verifying the identity of their clients and the beneficial-owners.

Note: You are advised to be weary of clients that are known friends, relatives or even colleagues as you be apprehended and detained pending when investigations is concluded.

6.2 Medium Risk Clients

This category takes care of those clients that may not be easily categorized as either low or high-risk customers.

6.3 Low-Risk Clients, Transactions or Services

Low risk clients include the following:

a. Financial Institutions — provided they are subject to requirements for combat of money laundering and terrorist financing which are consistent with the provisions of the relevant laws and are supervised for compliance with them;
b. Public companies (listed on a stock exchange or similar situations) that ate subject to regulatory disclosure requirements;
C. Government ministries and parastatals /enterprises;
d. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by NAICOM;
e. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;
f. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the, scheme rules do not permit the assignment of a member's interest under the scheme, and
g. Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBPs) provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the provisions of Money Laundering (Prohibition) Act 2004.

6.4 If the company applies simplified or reduced CDD measures to clients' resident abroad, it is required to limit such to clients in countries that have effectively implemented the FATF Recommendations.

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

6.6 The company will adopt CDD measures on a risk sensitive-basis. Examples of higher categories are indicated above and the company will determine in each case whether the risks are lower or not, having regard to the type of client, product, transaction or the location of the client. Where there is doubt, the company will seek clarification with the NFIU.

7.0 TIMING OF VERIFICATION

7.1 Company will verify the identity of the client before or during the course of establishing a business relationship or conducting transactions for them.

The company is permitted to complete the verification of the identity of the client and beneficial owner following the establishment of the business relationship, only when:

(a) This can take place as soon as reasonably practicable;
(b) It is essential not to interrupt the normal business conduct of the client; and
(c) The money laundering risks can be effectively managed.

Examples of situations where it may be essential not to interrupt the normal conduct of business are: Non face-to-face business such as Securities transactions: In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the client is contacting them and the performance of the transaction may be required before verification of identity is completed,

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

7.2 Failure to Complete CDD

If the company fails to comply with the above, it should;

a. Not open the account, commence business relations or perform the transaction; and

b. Be required to render a suspicious transaction report to the NFIU.

If the company has already commenced the business relationship (e.g. as stated above), it should terminate the business relationship and render suspicious transaction reports to the NFIU.

7.3 Existing Clients

The company is required to apply CDD requirements to existing clients on the basis of materiality and risk and to continue to conduct due diligence on such existing relationships at appropriate times.

The appropriate time to conduct CDD by the company is when

a. a transaction of significant value takes place,
b. a client's documentation standards change substantially,
C. there is a material change in the way that the account is operated, and
d. the company becomes aware that it lacks sufficient information about an existing client.

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

8.0 EXEMPTION FROM IDENTIFICATION PROCEDURES

8.1 where a customer's identity was not properly obtained as contained in this Manual and Requirements for Account Opening Procedure, the company shall re-establish the client's identity in line with the contents of this Manual as under no circumstance should any client be exempted from identification procedure.

9.0 DEFINITION OF POLITICALLY EXPOSED PERSONS (PEPs)

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

- Heads of State or government
- Governors;
- Local government chairmen;
- Judicial or military official;
- Senior politicians;

- Senior government officials;
- Senior executives of state owned corporations;
- Important political party officials;
- Members of Royal families; and
- Family members or close associates of PEPs.

9.2 The company shall, in addition to performing CDD measures, put in place appropriate risk management systems to determine whether a potential client or existing client or the beneficial-owner is a politically exposed person.

9.3 The officer of the company shall obtain senior management approval before establishing business relationships with a PEP and to render monthly returns on their transactions with PEPs to the NFIU.

9.4 Where a client has been accepted or has an ongoing relationship with the company and the client or beneficial-owner is subsequently found to be or becomes a PEP, M.D's approval should be obtained in order to continue the business relationship.

9.5 The company will take reasonable measures to establish the source of wealth and the sources of funds of client and beneficial-owners identified as PEPs and report all anomalies immediately to the NFIU and other relevant authorities.

9.6 Where the company is in a business relationship with a PEP, it is required to conduct enhanced ongoing monitoring of that relationship. In the event of any transaction that is abnormal, the company will flag the account and report immediately to the relevant authorities such as EFCC/NFIU.

10.0 NEW TECHNOLOGIES AND NON-FACE-TO-FACE TRANSACTIONS

10.1 The company shall have policies in place or take such measures as may be needed t prevent the misuse of technological developments in money laundering or terrorist financing schemes.

10.2 The company should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures shall be applied automatically when establishing client relationships and conducting ongoing due diligence.

Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face clients.

10.3 where the company relies upon a third party, it shall immediately obtain the necessary information concerning properly 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 company shall satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.

10.4 The company shall satisfy itself that the third party is a regulated and supervised institution and has measures in place to comply with requirements of CDD and reliance on intermediaries and other third parties on CDD as contained in this Manual and other relevant laws.

11.0 NON-COOPERATIVE COUNTRIES AND TERRITORIES (NCCT) OR HIGHER RISK COUNTERIES

11.1 The company shall pay special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF recommendations.

11.2 The company shall report, as stated below, transactions that have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined and written findings made available to assist competent authorities such as NFIU, auditors and law enforcement agencies (LEAs) to carry out their duties.

11,3 Where the company does business with foreign institutions which, do not continue to apply or insufficiently apply the provisions of FATF Recommendations, it shall take measures such as the following:

- Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories to financial institutions for identification of the beneficial owners before business relationships are established with individuals or companies from that jurisdiction;
- Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

- In considering requests for approving the establishment in countries applying the counter-measures of subsidiaries or branches or representative offices of financial institutions, taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;
- Warning non-financial sector businesses that transactions with natural or legal persons within that country might run the risk of money laundering;
- Limiting business relationships or financial transactions with the identified country or persons in that country.

12.0 WHISTLE-BLOWING AND MONITORING OF EMPLOYEE CONDUCT

12.1 Observation of Whistle-Blowing

Eurocomm Securities Limited has whistle-blowing policies and procedures which is developed in furtherance of the company's aspiration to strengthen its corporate governance and risk management framework, which will result in enhanced stakeholders' value. The whistle-blowing policy sets forth the company's policy and procedures for reporting to the company instances of ostensible unethical activities that relate to the business of the company, with a view to enabling the company to appropriately address such incidents,

As an institution, Eurocomm Securities Limited is committed to achieving the highest possible standards of service and ethical standards in its business. The company therefore encourages all of its stakeholders to raise legitimate concerns about any ostensible unethical and/or illegal acts and/or omissions by the company or its personnel so as to enable the company to appropriately address such concerns. The company encourages raising the concerns to the company rather than the concerned stakeholder overlooking the problem, thereby causing avoidable damage to the company in particular and the society in general.

12.2 Monitoring of Employee Conduct

The company shall monitor its employees' conduct for potential signs of money laundering. The company is also required to subject employees' stockbroking accounts to the same AML/CFT procedures as applicable to other clients' accounts.

This is required to be performed under the supervision of the AML/CFT Chief Compliance Officer. The latter's own stock broking account, if any, is to be

reviewed by a person of adequate/similar seniority. Compliance reports including findings are to be rendered to the NFIU on periodic basis.

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

13.0 PROTECTION OF STAFF WHO REPORT VIOLATIONS

13.1 The company shall direct it's employees in writing to always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to them. The company shall also make it possible for employees to report any violations of the institution's AML/CFT compliance program to the AML/CFT Compliance officer. Where the violations involve the Chief Compliance Officer, employees are required to report such to a designated higher authority of the company.

13.2 The company shall inform their employees in writing to make such reports confidential and that they will be protected from victimization for making them.

14.0 EMPLOYEES AML/KYC/CFT EDUCATION AND TRAINING PROGRAMMES

14.1 The Need for Staff Awareness

a. Staff must be aware of their own personal obligations under the Money Laundering (Prohibition) Act 2004 as they can be personally held liable for failure to report information to the authorities. It is crucial that all staff fully understands the need for and implements the KYC policies consistently.

b. Staff must co-operate fully with the NFIU and NDLEA as well as provide prompt reports of suspicious transactions on Money Laundering matters.

14.2. Training/Education Packages

a) Eurocomm Securities Limited will have an on-going employee training programme to adequately train staff in KYC procedures. The timing and content of the programme as well as the requirement will depend on the staff need.

b) Regular refresher training shall be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all staff fully understands the need for and implement KYC policies consistently.

14.3 New Employees

a. A general appreciation of the background to the basic requirements in the KYC and anti-money laundering policies and subsequent need for reporting of any suspicious transactions to the Compliance officer, must be provided to all new employees who deal with clients or their transactions irrespective of the level of seniority.

b. Staff should be aware of the importance that the company placed on reporting of suspicious transactions and the legal requirement to report as well as statutory personal obligation in this respect.

c. Staff members who are in a position to deal with the public are the first point of contact with potential money-launderers and their efforts are therefore vital to the company's strategy and key success factors in combating money laundering.

d. As such, they should be aware of their legal responsibilities and the company's reporting system for such transactions.

e. Training would regularly be provided on quarterly basis by the company on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious as spelt out in the Money Laundering (Prohibition) Act 2004.

14.4 Management Staff

a. A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility of supervising or managing staff.

b. Instructions should include the offences and penalties entrenched in the Money Laundering (Prohibition) Act 2004 for non-reporting and aiding money launderers; procedure relating to restraint orders; and the requirements for retention of records.

c, The employee training program is required to be developed under the guidance of the AML/CFT Chief Compliance Officer in collaboration with the tip Management.

d. The basic elements of the employee training program ae expected to include:

- AML regulations and offences
- The nature of money laundering
- Money laundering ‘red flags’ and suspicious transactions

- Reporting requirements
- Risk based approach to AML/CFT
- Customer due diligence
- Record keeping and retention policy.

15.0 RECORD KEEPING, MAINTENANCE AND RETENTION

To ensure that record remain up-to-date and relevant, there must be regular reviews of existing records when substantial transaction take place, or when client documentation standards change substantially or when there is a material change in the way the client's account is operated.

The company will ensure that the clear standards developed on records to be maintained on customer's identification and individual transactions and their retention period is adhered to strictly.

15.1 The investigating authorities need to ensure a satisfactory audit trail for suspected drug related or other laundered money and to be able to establish a financial profile of the suspect account. To satisfy these requirements, the following information may be sought:

15.2 The volume of money flowing through the account:

For selected transactions:

The origin of the funds (if known);
The form in which the funds were offered or withdrawn i.e. cheques, online transfer, etc.
The identity of the person undertaking the transaction;
The destination of the funds;
The form of instruction and authority.

Thus, all record and documents as they pertain to all accounts and transactions done in the company must be kept and adequately secured to aid any investigating authorities desirous to satisfy itself in respect of section 15.1.1 to 15.1.2 above.

16.0 RETENTION OF RECORDS "

16.1 The client's identification documents, accounts opening records and business correspondences of all clients will be obtained and should be kept for at least 6 years after the closure of account or the severance of relations with the customer.

16.2 All individual financial transaction records should be kept for at least 6 years* after the transaction has taken place.

*Note

Statutes of Limitation Act — 6 years

Money Laundering (Prohibition) Act 2004 — 5 years

17.0 RECOGNITION, COMPLIANCE MONITIRING AND REPORTING OF SUSPICIOUS TRANSACTIONS

17.1 Recognition of Suspicious Transactions

As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction is one, which is inconsistent with a client's known legitimate business or personal activities or the normal business inconsistent with that type of account.

a. The first key to recognition of whether a transaction is suspicious or not, is to have sufficient information about the client and his/her business.

b, Examples of Suspicious Transactions
These are not intended to be exhaustive but only provide the basic ways by which money may be laundered. The only limit as to how money might be laundered is the imagination of those attempting to change the identity of illegally obtained money.

c. Identification of any of these transaction types listed below (17.4) should prompt further investigation and be a catalyst towards making at least initial enquiry about the source of funds.

d. Monitoring of suspicious transactions: Suspicious transactions should be continually reviewed by a senior officer responsible for ensuring the day-to-day consideration of money laundering techniques.

17.2 Reporting of Suspicious Transactions to Regulators

All suspicious transactions must be reported promptly through the company's Chief Compliance Officer to the Economic and Financial Crimes Commission (EFCC), and Nigerian Financial Intelligent Unit (NFIU) within 7 days.

a. In addition to acting as the national points for receipt of transactions disclosures, the SEC, NDLEA, EFCC and NFIU also act as national and international advisors on Money laundering matters. Therefore, Eurocomm

Securities Limited should constantly review and seek clarifications from the SEC, NDLEA, EFCC, and NFIU on matters relating to money laundering.

b. To guard against money laundering, it is important to provide an audit checklist for suspicious funds. Copies of relevant identification documents should be retained.

17.3 Feedback of Suspicious Transactions

The commission (EFCC) could provide feedback at the instance of the disclosing company. Eurocomm Securities Limited will always seek for feedback on reported cases.

17.4 Examples of Suspicious Transactions

a. Reluctance to provide normal information when opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the company to verify.

b. Clients who appear to have accounts with several stockbroking firms within the same locality, especially when the firms are aware of a regular consolidation process from such accounts prior to a request for onward payment of cheque on account.

C. Buying and selling of stocks with no discernible purpose or in circumstance which appear unusual.

d. Money laundering by off-shore international activity

e. Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bonafide transactions to or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs.

f. Building of large balances, not consistent with the known turnover of the customer's business and subsequent transfer to account(s) held overseas.

g. Unexplained electronic funds transfers by clients on an in and out basis or without passing through an account.

h. Change in employee characteristics e.g. lavish life styles or avoiding going on annual leave.

i. Any dealing with an agent where the identity of the ultimate beneficiary or counter party is undisclosed, contrary to normal procedure for the type of business concerned.

18.0 INTERNAL CONTROLS, COMPLIANCE AND AUDIT

18.1 The company will establish and maintain internal procedures, policies and controls to prevent money laundering and financing of terrorism and will communicate these to the employees. These procedures, policies and controls will cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

18.2 The AML/CFT compliance officer and appropriate staff should have timely access to customer identification data, CDD information, transaction records and other relevant information. The company will therefore develop programs against money laundering and terrorist financing that include:

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

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

iii. Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.

18.3 The company is required to put in place a structure that ensures the operational independence of the Chief Compliance Officer (CCO).

18.4 These measures are meant to deter money laundering and terrorist financing. They include measures on sanctions and other forms of reporting, special attention for higher risk countries and foreign branches and subsidiaries of the company.

19.0 CURRENT LEGAL PROVISION AND PENALTIES

19.1 Personal obligations of members of management and staff.

19.2 Money laundering regulations cover proceeds of all criminal activities such as armed robbery, tax evasion, smuggling, proceeds of drug trafficking, advance fee fraud, official corruption and bribery, etc.

19.3 It is an offence for any person to be involved in money laundering, aid or collaborate with a money launderer,

19.4 A director or employee of the company who warns or in any way intimates the owner of funds involved in transaction to reported to the NDLEA or refrains from making the report as required, destroys or removes official records or employs a false identity is guilt and liable on conviction.

19.5 An employee who accepts or makes cash payment in excess of amounts authorized by the Decree and fails to make a report of international transfer of funds or securities is guilty of an offence and liable on conviction.

19.6 The company's employee's oversight or flaw in internal control, which makes it impossible for him to discharge his responsibilities under the Decree, is liable to SEC disciplinary action.

19.7 The company's employees who conspire, abet or aid any person to commit offence under the Act are guilty if convicted for such untoward acts.

19.8 NDLEA is empowered to demand, obtain and inspect the books or records of the company on money laundering related cases. Willful obstruction of the NDLEA or its authorized officers is an offence.

19.9 It is a criminal offence for the capital market operator in Nigeria not to have in place adequate procedures to combat money laundering.

19.10 These procedures include:

- Identification of old and new clients

- Special surveillance of certain transactions

-Preservation of records

-Arousing and stepping up awareness among company's employees.

-Rendition of appropriate returns.

19.11 **PENALTIES**

19.12 Offence: Assistance-.

It is an offence to assist a person who converts or transfers resources or profit derived directly or indirectly from illicit traffic in narcotic drugs or psychotropic substances or any other criminal activity, with the aim of either concealing or disguising the illicit origin, or collaborates in concealing or disguising the genuine nature, origin, location or ownership of the resources.

Penalty: Imprisonment of not less than 2 years and not more than 3 years.

19.14 Offence: Tipping Off:

It is an offence for a director or employee of a capital market institution to warn or in any other way intimate the owner of funds under an investigation about the report he is required to make or action take on it or who destroys or removes a register or record required to be kept.

Penalty: Imprisonment of not less than 2 years and not more than 3 years,

19.15 Offence by Body Corporate:

Where an offence, under this Act, is proved to have been committed on the instigation or with the connivance of or attributable to any neglect on the part of a Director, Manager, Secretary or other similar officer.

Penalty: On conviction, the body corporate will be wound up and all its assets and properties forfeited to the Federal Government.

19.16 Obstruction of the Commission (EFCC) or Agency or any authorized officer:

It is an offence for a person to willfully obstruct the Commission, National Drug Law Enforcement Agency or any authorized officer of the Agency in the exercise of the powers conferred on the Agency.

Penalty: Imprisonment of not less than 2 years and not more than 3 years for individuals and fine of f41,000,000.00 for body corporate.

20.0 TESTING, FOR ADEQUACY OF AML/KYC/CFT COMPLIANCE

20.1 The company is required to make a policy commitment and to subject its AML/CFT Compliance program to independent-testing or require its internal audit function to determine its adequacy, completeness and effectiveness.

20.2 FORMAL BOARD APPROVAL OF THE AML/CFT COMPLIANCE POLICIES AND PROCEDURS MANUAL

The ultimate responsibility for AML/CFT compliance is placed on the Board/Top Management of the company. The Board ensures that a comprehensive operational AML/CFT Compliance Manual is formulated by Management and presented to the Board for consideration and formal approval.

Copies of the approved Manual above are to be provided to the SEC and NFIU on request.

20.3 CULTURE OF COMPLIANCE

The company should have comprehensive AML/CFT —compliance program to guide its compliance efforts and to ensure the diligent implementation of its Manual. Indeed, entrenching a culture of compliance would not only minimize the risks of the company being used to launder the proceeds of crime but also provide protection against fraud, reputation and financial risks.

20.4 SPECIAL RECOMMENDATIONS

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

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

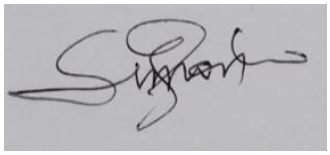
c) Terrorist financing offences are predicated offences for money laundering:

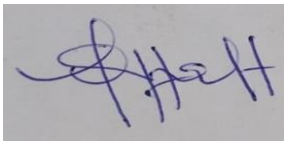
Terrorist financing offences therefore apply, regardless of whether the person alleged to have committed the offence is in the same country or a different country from the one in which the terrorist/terrorist organization is located or the terrorist act occurred or will occur.

21.0 SANCTIONS FOR NON-COMPLIANCE WITH AML/KYC/CFT LAWS AND REGULATIONS

21.1 Failure to comply with the provisions contained in this Manual and applicable laws and regulations will attract appropriate sanction(s) fr6m the regulatory body or bodies against the company or officer responsible for the infraction(s) in accordance with existing Laws and as detailed in the KYC/AML/CFT Compliance Policies and Procedures section of this Manual or other policies or provisions as may be prescribed by the company or regulators or relevant laws.

APPROVED BY THE BOARD OF DIRECTORS





---------- ----------

Managing Director Director