AGRICULTURAL DEVELOPMENT BANK LIMITED

ANTI-MONEY LAUNDERING POLICY AND MANUAL

Author:	**Anti-Money Laundering Unit**
Recommended By:	**Executive Management Committee**
Approved By:	**Board of Directors**
Date:	**March 2020**

TABLE OF CONTENTS

ACRONYMS

AML	Anti-Money Laundering
AMLRO	Anti-Money Laundering Reporting Officer
BCBS	Basel Committee on Banking Supervision
BCEAO	Central Bank of West African States
BIS	Bank for International Settlements
CFT	Combating Financing of Terrorism
CTR	Cash Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
ECOWAS	Economic Community of West Africa States
FATF	Financial Action Task Force
FT	Financing of Terrorism
GIABA	Inter-Governmental Action Group against Money Laundering and Terrorism Financing in West Africa
HKMA	Hong Kong Monetary Authority
KYC	Know Your Customer
ML	Money Laundering
MLCO	Money Laundering Compliance Officer
PEP	Politically Exposed Person

STR	Suspicious Transaction Report
WAEMU	West African Economic and Monetary Union.

PART 1
POLICY

ADB ANTI-MONEY LAUNDERING POLICY AND MANUAL

Preamble

The purpose of our AML Policy is to establish the general framework for the fight against money laundering, terrorism, corruption and other financial crimes. Successful participation in this fight by the financial sector requires an unprecedented degree of global cooperation between governments and financial institutions. Our institution is committed to reviewing our AML strategies and objectives on an ongoing basis and to maintaining an effective AML programme. We are committed to high standards of AML compliance and require management and employees to adhere to these standards in preventing the use of our products and services for money laundering purposes. Adherence to this policy is absolutely fundamental for ensuring that all of our entities, regardless of geographical location, comply with applicable anti-money laundering legislation. We are required and committed to adhere to minimum standards of anti-money laundering compliance based on the applicable anti-money laundering laws and regulations and any additional standards from our regulatory supervisors and the Financial Action Task Force (FATF) which clarify the main statutory duties imposed on our institution. Our AML programme is formulated and directed by the Anti-Money Laundering Unit under the auspices of the Board of Directors. However, it is the responsibility of all employees to keep ill-gotten funds out of our institution.

.

1.0 Purpose and Overview of The Policy and Manual

This Policy and Manual has been formulated by the Bank to reinforce the broad AML/CFT legal requirements and more importantly, to provide best-practice guidance to the Bank's staff on how to implement the relevant legal provisions.

Money laundering (ML) has been defined as the process whereby criminals attempt to or conceal the illegal origin of illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. It is, thus, a derivative crime. Financing of Terrorism (FT) is a reverse form of money laundering and may involve both legitimate and illegitimate money. It is characterized by concealment of the origin or intended criminal use of the funds.

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

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

This Manual covers the following key areas:

- design of AML/CFT policy;
- Compliance Officer's designation and duties;
- the need to co-operate with the competent/supervisory authorities;
- customer due diligence;
- monitoring and responding to suspicious transactions;
- reporting requirements;

- record keeping;
- AML/CFT employee training programme;
- Appendices defining and listing financial and designated non-financial businesses and professions; money laundering 'red flags'; and other resource materials

1.1 Money Laundering

Money laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. Simply put, money laundering is the process of making dirty money look clean.

1.**2** Stages of Money Laundering

Traditionally, it has been accepted that Money Laundering occurs in three separate/fundamental stages:

i. **Placement of Cash**-how the criminal proposes to introduce the dirty money into the system.

ii. **Layering**-utilizing multiple transaction e.g. purchase of commodities, payment of false invoices to partner companies, foreign investment etc., which confuses the audit trail and separates the money from its origin.

iii. **Integration**-inserting the criminal proceeds into legitimate business so as to give the appearance of normal business funds.

1.3 Terrorist Financing

Terrorism can be defined as the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in the furtherance of political or social objectives. Terrorist acts are criminal in nature and constitute a serious threat to the individuals' lives and freedom.

Terrorist funding relates to provision or collection of funds to carry out an act of killing or seriously injuring a civilian with the objective of intimidating a section of the people or compelling a government to do or to abstain from doing any act.

1.4 Difference Between Money Laundering and Terrorist Financing

The most basic difference between money laundering and terrorist financing involves the origin or source of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. It could be from a genuine source as well. On the other hand, money laundering always involves the proceeds of illegal activity or a predicate offense committed.

1.5 Anti-Fraud

Agricultural Development Bank (ADB) Limited will continually strive to ensure that all of its products, services and payment processes are carried out and reported honestly, accurately, transparently and accountably and that all decisions are taken objectively and free of personal interest. The bank will not condone any behaviour that falls short of these principles. All staff of the bank have a responsibility for putting these principles into practice and for reporting any breaches they discover.

This document applies to any irregularity, or suspected irregularity, involving employees as well as Directors, shareholders, vendors, consultants, contractors, outside agencies doing business with employees of such agencies, and /or any other parties with a business relationship with the Agricultural Development Bank Limited.

2.0 AML/CFT Institutional Policy Framework

2.1 General Guidelines

Agricultural Development Bank (ADB) Limited is committed to complying with AML/CFT obligations in order to actively prevent any transaction that otherwise facilitates criminal activity or terrorism. The Bank will, therefore, formulate and implement internal controls and other procedures to deter criminals from using its facilities for money laundering and terrorist financing, thus ensuring that it meets its obligations under the law.

The internal control measures include:

- Programmes to assess the risks related to money laundering and terrorist financing;
- The formulation of control policy concerned with issues of timing, degree of control, areas to be controlled, responsibilities and follow-ups, to combat money laundering and terrorist financing;
- Monitoring programmes in relation to unusually large transactions; enhanced due diligence with respect to persons and businesses carrying high risks, including politically exposed persons;
- Enhanced due diligence on persons in jurisdictions that do not have adequate AML/CFT regimes;
- Providing employees, including the Compliance Officer, with training on customer due diligence and the recognition and handling of suspicious transactions, etc; and
- Making the employees to be aware of the provisions of the AML/CFT laws and regulations and the manual of compliance formulated by the Bank, pursuant to those laws.

3.0 Anti-Money Laundering Reporting Officer's Designation and Duties

The Bank shall appoint a responsible official as an Anti-Money Laundering Reporting Officer (AMLRO) who shall be a key management personnel of the accountable institution and who will operationally report to the Board in accordance with section 41(1) (b) of the Anti-Money Laundering Act, 2008 (Act749) as amended, Regulation 5(1) of L.I. 1987 and Part A 1.0 of the Bank of Ghana and Financial Intelligence Centre AML/CFT & P Guideline for Banks and Non-Bank Financial Institutions in Ghana July 2018. He shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme.

He or she shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme.

The duties of the AML Reporting Officer shall include but not limited to the following:

(i) Developing an AML/CFT Compliance Programme;
(ii) Receiving and vetting suspicious transaction reports from staff;
(iii) Filing suspicious transaction reports with the competent/supervisory authority;
(iv) Filing of other statutory reports timeously with the competent/supervisory authority;
(v) Ensuring that the compliance programme is implemented;
(vi) Coordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements; and
(vii) Serving both as a liaison with relevant competent/supervisory authorities and a point-of-contact for all employees on issues relating to money laundering and terrorist financing.

4.0 Co-operation with Competent Authorities for Information

The Bank shall comply promptly with requests, and pursuant to the law, provide information to the competent authority or other relevant government agency. The Bank's procedures for responding to authorized requests for information on money laundering and terrorist financing shall include:

(a) immediately searching institutional records to determine whether or not it maintains or has maintained any account for, or has engaged in any transaction with each individual, entity, or organization named in the request;

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

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

4.1 Conditions for Acceding to Such Request

The formal request so made shall not be acceded to unless:

a. With the prior approval of the Managing Director, the Deputy Managing Director, the General Counsel or a Key Management Personnel of the bank.
b. With the express written permission of the customer or individual involved
c. It is an Order from a Court of competent Jurisdiction.
d. It is request from the Law Enforcement Agencies, eg, EOCO

e. It is a directive from Bank of Ghana.
f. It is a request from the Financial Intelligence Centre, Ghana
g. It is a request from the Securities and Exchange Commission.

4.2 Data Protection

The Agricultural Development Bank (ADB) Limited is registered under the Data Protection Act of Ghana, Act 2012 (Act 843). To this end, the bank is mindful of and shall be guided by all the eight thematic areas of the Act.

i. **Accountability**. A person who processes personal data shall ensure that the personal data is processed without infringing the privacy rights of the data subject, in a lawful manner and in a reasonable manner.
ii. **Lawfulness of Processing Minimality**. Personal data may only be processed if the purpose for which it is to be processed is necessary, relevant and not excessive.
iii. **Specification of Purpose**. A data controller who collects personal data shall collect the data for a purpose which is specific, explicitly defined and lawful and is related to the functions or activity of the person.
iv. **Compatibility of Further Processing With Purpose of Collection**. Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data shall be for that specific purpose.
v. **Quality of Information**. A data controller who processes personal data shall ensure that the data is complete, accurate, up to date and not misleading, having regard to the purpose for the collection or processing of the personal data.
vi. **Openness**. The bank shall ensure that the data subject is aware of the nature, purpose and consequences of breach of data usage. Where the said data is already in the Public domain, the data subject is not protective of it and that the bank bears no liability for its usage. Certain privileged governmental institutions by the nature of their set up can request for and use data without recourse to the data subject. For example, the Bank of Ghana, Law Enforcement Agencies, The Financial Intelligence Centre, a Court of Competent Jurisdiction, etc.
vii. **Data Security Safeguards**. The bank shall take appropriate security measures to prevent unauthorized access, alteration, disclosure or destruction of personal data. It shall include adopting enhanced security measures to ADB data processors.
viii. **Data Subject Participation**. The bank may disclose information to our agents, advisors, service providers for the following reasons:
    - Processing and assessing application(s)
    - Verifying personal data
- Conducting credit searches against the applicants prior to and during the term of any loan.

5.0 Know Your Customer (KYC)/Client Programme (Due Diligence Procedure)

5.1 What is ‘’Know Your Customer’’ Requirement?

‘’Know Your Customer’’ (KYC) requirement entails obtaining full particulars of the identity of a customer and having adequate knowledge of the purpose for which the customer desires to establish a business relationship with a financial institution. Having adequate knowledge of a customer and applying it to all transactions initiated by the customer is an effective way of avoiding being used to launder the proceeds of crime and recognizing suspicious activities.

Thus, the Bank shall establish clear and written procedures for verifying the identity of persons who open new accounts. The procedures should state the types of information the institution will collect from customers and how it will verify each customer’s identity.

5.2 Customer Acceptance Policy

The Bank will not establish a business relationship until all relevant counterparties to the relationship have been identified and the nature of the business they intend to conduct has been duly ascertained. Once an on-going business relationship has been established and the normal operation confirmed, any inconsistent activity would be investigated to determine whether there is a suspicion of money laundering.

5.3 The Requirement to Obtain Identification Evidence

The first requirement of knowing your customer for money laundering purposes is that the Bank should be satisfied that a prospective customer is who he/she claims to be. The Bank shall not carry out, or agree to carry out, any financial business or provide advice to a customer or potential customer, unless the Bank is certain about who that person actually is. If the customer is acting on behalf of another, e.g. the funds are being supplied by someone else, or the investment is to be held in the name of someone else, we have an obligation to verify the identity of both the customer and the agent/trustee unless the customer is itself a regulated financial institution within the country.

5.4 The Nature and Level of the Business to be Conducted

Adequate information should be obtained on the nature of the business that the customer intends to undertake, including the expected or predictable pattern of transactions. The information collected at the outset for this purpose should include:

- Purpose and reason for opening the account or establishing the relationship;
- Nature of the activity that is to be undertaken;
- Expected origin of the funds to be used during the relationship; and
- Details of occupation/business activities and sources of wealth or income.

Adequate steps should be taken to keep the information up to date as the opportunities arise, e.g. when an existing customer opens a new account. Such information obtained during any contact with the customer should be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily available to the Compliance Officer or relevant regulatory bodies.

5.5 Risk-based Approach to KYC

The Bank shall adopt a risk-based approach in implementing its KYC policy in respect of categorizing customers into a three-tier risk rating. The bank will rely on an objective risk rating template in achieving this results. The factors to be used in the risk rating shall include geographical location of the customer or where the entity business is situate, object of the entity, nationality of the customer, customer type, and the product or service being offered the customer among others. Customers or accounts to be classified as high risk shall be subjected to enhanced due diligence and constant monitoring of its transactions thereof. They shall include but not limited to:

- private or executive banking customers;
- correspondent banking;
- non-face-to-face customers (eg. home link);
- Politically Exposed Persons (PEPS)

For such high risk entities, the KYC approach should involve customer risk profiling and assignment of specific risk rates, and the resort to Enhanced Customer Due Diligence techniques (ECDD). The ECDD techniques should include but not limited to:

i) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information (otherwise known as identification data);

ii) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the Bank is satisfied that it knows who the beneficial owner is;

iii) Obtaining information on the purpose and intended nature of the business relationship;

iv) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customers, their business and risk profile, including where necessary, the source of funds.

5.6 Third Party Payments

Pursuant to Section 23 (7) of the Anti-Money Laundering Amendment Act 2008 (Act749), all third parties making transactions (deposits and withdrawals) on another person's bank account, as well as walk-in-customers seeking to make Banker's Draft and Telegraphic Transfers shall be required to provide a valid photo ID. The following are the acceptable photo IDs by the bank:

- ✓ voters Identity card
- ✓ national passport
- ✓ driver's license or
- ✓ SSNIT biometric card.

All cards to be accepted shall be verifiable. A photo ID that cannot be verified shall not be accepted in any form unless the customer could furnish an officer of the bank with some other valid photo ID to support the initial one.

5.7 Financial Inclusion

The bank believes that access to banking facilities and other financial services is a necessary requirement for most adults. As such, socially and financially disadvantaged applicants resident in Ghana should not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence to identify themselves.

Where a financial institution has reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, the institution may accept as identification evidence, a letter or statement from a person in a position of responsibility who knows the client and can confirm that the client is who he/she says he/she is, including confirmation of his permanent address. The ID of the guarantor shall be obtained and verified.

5.8 Source of Wealth and Source of Funds

Source of Wealth refers to the total wealth or the majority of the wealth of a customer, the activities which have generated or contributed to a customer's accumulation of funds and assets. Source of wealth therefore describes how a customer acquired their total wealth over time i.e. the source(s) through which the wealth was generated. All legitimate assets that can be confirmed are valued and included within the individual's net worth summary.

Source of Funds nonetheless refers to the origin of the particular funds or assets which are the subject of the business relationship between the bank and its client. The transactions the bank is required to undertake on behalf of the client - the amounts being invested, deposited or remitted. The information obtained should be substantive, relevant and be able to establish the fund's origin and the method and or circumstances under which the funds were acquired.

A prospective customer who wishes to open account with the bank shall at the onboarding stage, be obliged to furnish the bank with the Source of his or her Wealth and or Source of his or her Funds before business relationship is established.

The Bank, as part of conducting Enhanced Due Diligence (EDD) on its high risk customers – individuals and entities or its business partners, shall collect and verify information relating to their Source of Wealth and or Source of Funds.

PART II
MANUAL

6.0 Leading Issues on Identity

6.1 Definition of Identity

Identity is defined as a set of attributes, including names used, date of birth, physical features, and the residential address at which a customer may be located, all of which can uniquely identify a natural or legal person. For a natural person, the date of birth should be obtained as an important identifier in support of the name. However, it is not mandatory to verify the date of birth provided by the customer.

6.2 Timing of Verification of Identity

Identity must be verified whenever a business relationship is to be established and an account opened, or a one-off transaction or series of linked transactions is undertaken. For the purpose of this manual, the definition of transactions includes the giving of advice. However, advice does not include the provision of information about the availability of products of services or to a first interview/discussion prior to establishing a relationship. Once identification procedures have been satisfactorily completed, and the business relationship established, as long as contract or activity is maintained and records concerning that customer are kept, no further evidence of identity is needed when any transaction or activity is subsequently undertaken.

6.3 Persons whose Identities should be verified

a Customers: Sufficient evidence of the identity must be obtained to ascertain that a customer is who he/she claims to be.

b A person acting on behalf of others: The obligation is to obtain sufficient evidence of their identities. This requirement is, however, subject to some exceptions, e.g. in consortium lending where the lead Manager/Agent supplies the normal confirmation letter.

c Furthermore there is no obligation to look beyond the client where:

- It is acting on its own account (rather than for a specific client or group of clients);
- The customer is a Bank, broker, fund Manager or other regulated financial institution;
- All the business is to be undertaken in the name of a regulated financial institution.

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

- The named account holder/person in whose name an investment is registered;
- Any principal beneficial owner of funds being invested who is not the account holder or named investor;
- The principal controller(s) of an account or business relationship (i.e. those who regularly provide instructions); and
- Any intermediate parties (e.g. where an account is managed or owned by an intermediary).

e Appropriate steps should also be taken to identify directors and all signatories to an account.

f Joint applicants/account holders: Identification evidence should be obtained for all the account holders.

g Higher risk businesses undertaken for private companies (i.e. those not listed on the stock exchange): Adequate evidence of identity and address should be verified in respect of:

- The principal underlying beneficial owner(s) of the company; and
- Those with principal control over the company's assets (e.g. principal controllers/directors).

h Officers of the Bank should be alert to circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly.

i Trusts: Bank Officials should obtain and verify the identity of those providing funds for the trust, i.e. the settler(s) and those who are authorized to invest or transfer funds, or make decisions on behalf of the trust, i.e. the principal trustees and controllers who have power to remove the trustees.

7.0 Regular Savings Schemes and Savings Accounts

7.1 Investments in The Names of Third Parties

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

7.2 Timeframe for Obtaining Verification Requirements

The appropriate timeframe for obtaining satisfactory evidence of identity depends on various relevant factors and circumstances, such as the nature of the business, the geographical location of the parties and whether it is possible to verify identify before any commitments could be made or transactions executed.

A Branch staff may start the processing of account opening as soon as a documented request is received, provided that such staff takes diligent steps to verify the customer's identity and does not transfer or pay out funds to a third party until the verification requirements have been duly met.

8.0 Identification Procedures

8.1 General Requirements

a Every official should at all times satisfy itself that he/she is dealing with a real person or organization (natural, corporate or legal), by obtaining adequate identification evidence. Where reliance is being placed on a third party to identify or confirm the identity of an applicant, the overall legal responsibility for obtaining satisfactory identification evidence rests with the account-holding branch.

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

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

d In verifying the identity of natural persons officers should state whether identification was done face to face or remotely. Adequate steps should be taken to avoid single or multiple fictitious applications or substitution (impersonation) fraud.

e An introduction from a respected customer, personally known to a Director or Manager, or from a member of staff, will often provide some comfort but should not replace the need for identification evidence set out in this manual. Details of who initiated and authorized the introduction should be kept in the customer's mandate file together with other records. Branch Managers and Heads of Department should insist on normal identification procedures for every applicant.

9.0 Certification of Identification Documents

9.1a Postal

To guard against the dangers of postal interception and fraud, prospective customers should not be requested to send originals of valuable personal identity documents (such as international passport, identity card, driver's licence. etc.) by post.

9.1b Face to Face Contact

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

9.1c Foreign Nationals

With respect to foreign nationals, the copy of international passport, national identity card or documentary evidence of address, should be certified by:

- An Embassy, Consulate or High Commission of the country of issue; or
- A senior official within the Bank; or
- A Lawyer, Attorney or Notary Public.

9.1d Certified Copies

Certified copies of identification evidence should be duly stamped, dated and signed: ''original sighted by me'', by a senior officer of the Bank. Officers should always ensure that a good reproduction of photographic evidence of identity is obtained and failing that a copy of the evidence certified as providing a good likeness of the applicant.

9.2 Establishing Identity

(a) Before opening an account, the account opening officer should request the applicant to provide the following information which should be certified by the applicant by signing the application form and also independently validated by the officer.

- Full Name (including all other names used).
- Permanent home address, including landmarks and postcode, where available.
- Telephone and fax numbers and e-mail address.
- Date and place of birth.
- Nationality.
- Occupation, public position held (if any) and/or name of employer.

- Any official personal identification number or other unique identifier contained in anunexpired official document that bears a photograph of the applicant, such as international passport, driver's license, identification card, tax identification number, etc.

(b) The information obtained should clearly establish that a person of that name exists at the address given and that the applicant is that person. Where an applicant has recently changed residence, the previous address should be validated.

(c) A risk-based approach should be adopted in verifying the identity of each customer. Thus, the extent and number of checks will vary, depending on the perceived riskiness of the service or business sought and whether the application is made in person or through a remote medium, such as telephone, post or the internet. Furthermore, the actual or anticipated source of funds, i.e. how the payment was made, from where and by whom, should always be recorded to provide an audit trail.

10.0 Establishing Identity for Politically – Exposed Persons (PEPs)

10.1 Who are Politically-Exposed Persons?

These are persons who are or have occupied high public office (See Appendix IV for a comprehensive list of PEPs). There is, thus, a possibility that such persons may abuse their public powers for unjust and illicit personal gain through the receipt of bribes, frauds, etc. Business relationship with such PEPs or entities associated with them may expose the Bank to significant reputational and/or legal risks. Accepting and managing funds from corrupt PEPs will seriously damage the Bank's reputation and could erode confidence in the financial system. Furthermore, the legal repercussions could be costly since, in certain circumstances, the Bank and/or its officers and staff may be liable to criminal sanctions against money laundering if they know, or should have known, that the funds in question derived from corruption or other predicate offences. Thus, all the relevant AML laws and regulations, including suspicious transaction reporting, tipping off, etc., apply.

Heavy fines have been imposed on financial institutions for conducting business with PEPs without adequate KYC and enhanced due diligence procedures. Even in the absence of an explicit legal requirement, it is undesirable and unprofessional for a financial institution to accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets. In the circumstances, it is imperative on Officers representing the Bank when entering into a relationship with a person who is suspected of being a PEP to identify that personality fully as well as persons and entities that are clearly related to the PEP.

10.2 Due Diligence Procedures In Respect Of PEPs

To enable the Bank guard against inadvertently dealing with PEPs, in addition to the standardized KYC procedures, Officers should adopt the following processes:

- Gather adequate information from any new customer and check publicly available information or a credible checklist or database in order to establish whether or not the customer is a PEP.
- Determine the source of funds and ensure that it does not derived from a corrupt or other criminal source before accepting a PEP as a customer.
- Take a heightened scrutiny approach to the account opening process by referring it for approval by the Compliance Officer and Senior Management.
- Carry out on-going monitoring of accounts and transactions of PEPs and additional controls.

10.3 Other Higher Risk Accounts

For other higher risk accounts or customers, similar steps should be taken to ascertain the source of wealth/funds.

10.4 Lower Risk Accounts

Even for lower risk accounts or simple investment products, e.g. deposit or savings accounts without cheque book or any of the Bank's automated money transmission facilities, there is an overriding requirement for all Officers to satisfy themselves on the identity and address of the customer.

11.0 **Establishing Identity of Natural Persons Resident in Ghana**

11.1 Trusts, Nominees and Fiduciaries

The confirmation of name and address should be established by reference to a number of sources. The checks should be undertaken by cross validation that the applicant exists at the stated address either through the sighting of actual documentary evidence, or by undertaking electronic checks of suitable databases, or by a combination of the two. The primary responsibility for ensuring that the identification evidence is satisfactory rests with the Officers/Branch opening the account or providing the product/service.

11.2 Documentary Evidence of Identity

Care should be taken to ensure that documents submitted are originals in order to avoid the acceptance of forged documents. Copies of documents dated and duly signed, 'original seen' by a senior public servant or a person of comparable status in a reputable private organization may be accepted, pending the submission of the original documents.

11.3 Checklist of Acceptable Documentary Evidence of Identity

Personal Identity Documents

- Current international passport.
- Residence permit issued by the immigration authorities.
- Current driver's licence issued by competent agency.
- Official tax identification number or tax clearance certificate.
- Birth certificate/sworn declaration of age.
- National identity card.
- Documentary evidence of address.
- Recent utility bill.
- Bank statement or passbook containing current address.
- Tenancy agreement.
- Search report on prospective customer's place of employment and residence, duly signed by a senior officer of the Bank.

11.4 Physical Checks On Natural Persons Resident in Ghana

The Bank should have systems that enable it to establish the true identity and address of a customer and effective checks that protect against the substitution of identity by an applicant.
For example, the officer should demand and examine independent source data like water and electricity bills of the prospective customer to confirm proof of residential address.

11.5 Additional checks to verify identity

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

- Mailing of account opening documentation direct to a named individual at an independently verified address;

- Having satisfactory evidence of an initial deposit cheque drawn on a personal account in the applicant's name in another financial institution in the country;

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

- Using card or account activation procedures.

11.6 Electronic Checks

Where feasible, electronic checks may be used to verify evidence of identity and address through other different original sources as an alternative or supplement to the documentary evidence provided.

11.7 Special Note On Non-Face-To-Face Identification

Non-face-to-face customers, whether resident or non-resident, pose increased potential risk of false identities and impersonation. Thus, extra care should be exercised in such cases by supplementing documentary or electronic evidence with additional checks to ascertain that each customer in the above category is actually who he claims to be. This is particularly so in cases where the prospective customer requests for a Bank account or service that provides money transfer facilities or payment to third parties.

In cases where financial intermediaries or agents undertake the processing of account opening requests on behalf of prospective customers, Officers should ensure that such intermediaries are subject to AML controls and that the prescribed identification procedures have been complied with. Documentary evidence of such verification should be obtained and kept with other account-opening documents.

11.8 Refugees and Asylum Seekers

In circumstances in which a refugee or asylum seeker applies to open a Bank account without being able to provide the usual evidence of identity, reliance should be placed on certification provided by the relevant or competent government authority confirming the identity of the person in question. As is required for such exceptional circumstances,

accounts of this type should be closely monitored to prevent their possible misuse given that such refugees could be PEPs.

12.0 Establishing Identity: Legal Persons Trusts, Nominees and Fiduciaries Cautionary Note

Trusts, nominee companies and fiduciaries conduct a wide variety of commercial activities and often play important and legitimate roles in the global economy. However, the unique features of trusts which attract genuine operators and the anonymity and complexity of structures which they often provide, all tend to make them attractive for criminal activity. Accordingly, there have been general concerns about the misuse of corporate vehicles by criminals to disguise and convert the proceeds of their illegal activities and the use of trusts and other quasi-corporate entities to facilitate such misuse.

Given that trusts and other quasi-corporate entities take different forms and are pervasive, the money laundering risk should be identified and managed on a service-by-service basis. Thus, customer identification procedures should be established to reflect the

perceived risk. Branch officials, when opening accounts for trusts, nominees and fiduciaries, should verify the identity of the trustee(s), the settler(s), i.e. the provider of the funds, the controllers (who have the power to remove the trustees) beneficiaries, and signatories. The underlying evidence of identity should be kept together with the account-opening records.

12.1 Receipt and Payment of Funds On Behalf Of Trusts

Branch officials should check monies received or payments made on behalf of trusts to identify the source of the funds and the nature of the transactions and ensure that adequate due diligence has been observed by the remitting Bank on the underlying client and the origin of the funds.

12.2 Powers of Attorney and Third-Party Mandates

Branch officials should obtain and verify identification evidence on holders of powers of attorney and third-party mandates in addition to those of the customers. Furthermore, the reason for granting the power of attorney should be determined and all records of transactions executed pursuant to the power of attorney should be kept.

12.3 Executorships Accounts

Branch officials should verify the identity of the executor(s)/administrator(s) of the estate when a Bank account is to be opened for the purpose of winding up the affairs of a deceased person. Payments to the underlying named beneficiaries on the instructions of the executor or administrator of an estate may be made without additional verification requirements. However, if a beneficiary seeks to transact business in his/her own name, identification evidence should be obtained. Where there is any suspicion about the nature or origin of assets comprising an estate that is being wound up, a report should be made to the Compliance Officer who would file a suspicious transaction report with the competent authorities.

12.4 Client Accounts opened by Professional Intermediaries

Where a professional intermediary, such as a Solicitor, Fund Manager, Accountant, Stockbroker, or estate agent, holds funds on behalf of its clients in client accounts opened with financial institutions, the professional intermediary is taken as the customer. Where such an intermediary is covered by the anti-money laundering regulations, verification of identity may not be necessary. However, where the intermediary is not subject to anti-money laundering regulations, Branch officials should verify both the identity of the professional intermediary and that of the person on whose behalf he is acting.

The Branch Management should monitor transactions executed on client accounts and report those transactions that give reasonable cause for suspicion to the competent authorities.

12.5 Unincorporated Businesses/Partnerships

Identification evidence should be obtained in respect of the principal beneficial owners /controllers where the applicant is an unincorporated business or a partnership whose principal partners/controllers do not already have a business relationship with the Bank. This procedure entails identifying the main signatories who are vested with significant measure of control by the principal beneficial owners/controllers.

Evidence of the trading address of the business or partnership should be obtained. Where a current account is being opened, a visit to the place of business may be necessary to ascertain the true nature of the business activities. Also, where appropriate, a copy of the latest report and accounts should be obtained.

The nature of the business or partnership should be ascertained to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from

the partnership authorizing the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained.

12.6 Limited Liability Partnership

A Limited Liability Partnership should be treated as a corporate customer for verification of identity and ‘’KYC’’ purposes.

13.0 Identification Procedures for Corporate Entities

13.1 General Principle

There is particular concern over the ease with which corporate entities could be created and dissolved in some jurisdictions which facilitates the use of these vehicles not only for legitimate purposes but also for criminal activities, such as money laundering. Given the potential risk of misuse of corporate vehicles and the AML protection afforded by factors such as the quality of available information, knowledge of the ultimate beneficial owners as well as the assets and their business objectives, Branch officials should obtain beneficial ownership information and perform customer due diligence at the commencement, and during the course, of a business relationship. This is particularly the case at the account-opening stage.

Furthermore, Branch Management should painstakingly verify the legal existence of the company from official documents or sources and that those persons claiming to act on behalf of the company are duly authorized.

13.2 Identification Requirements

The underlying principles of customer identification for natural persons also apply to corporate entities, especially where the identification and verification of natural persons is involved in the relationship with corporate entities.

For corporate entities, the following information should be obtained:

- Registered corporate name and any trading names used;
- Registration or incorporation number;
- Principal place of business operations;
- Mailing address;

- Contact telephone and fax numbers;
- Names of Directors and secretary as specified in Form 3;

- Original or certified copy of the certificate of incorporation and the Regulations.
- The nature of the company's business and its legitimacy; and
- The resolution of the Board of Directors to open an account and identification of the signatories to the account.

Branch Management should verify the information obtained by, at least, one of the following methods:

- Reviewing a copy of the latest report and accounts (audited, if available) for established companies;
- Conducting an enquiry through a business information service or an undertaking from a reputable and known firm of lawyers or accountants certifying the documents submitted;
- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- Utilising as and when available independent information verification processed, such as accessing public and private databases;
- Obtaining prior bank references;
- Visiting the corporate entity, where feasible; and
- Contacting the corporate entity by telephone, mail or e-mail.

13.3 Due Diligence Procedures for High Risk Business

For private companies and other legal entities undertaking higher risk business, Branch Management should, in addition to the usual requirements for companies, seek to lift the corporate veil and identify those who have ultimate control over the business and the company's assets. Identification evidence is required for those shareholders who have significant shareholding (as defined by competent authority) and those who are mandated to manage funds, accounts or investments without further authorization and are thus in a position to override internal procedures and control measures.

In keeping with a risk-based approach, identification evidence should be obtained not only for the principal beneficial owners and those who exercise control over the assets of the company but also the non-executive directors. Branch Management should undertake a visit to the place of business if the volume is large enough not only to confirm the existence of the business and the nature and purpose but also its legitimacy.

An international business company which is registered in an offshore jurisdiction but operates out of a different jurisdiction requires particular attention. Accordingly, such companies should be subjected to rigorous customer due diligence procedures.

13.4 Identification Procedure for Foreign Financial Institutions

Confirmation of existence and regulated status of a foreign financial institution should be carried out by checking with, at least, one of the following sources:

- The home country Central Bank or relevant supervisory body; or
- Another office, subsidiary, branch, or correspondent bank in the same country; or
- A local correspondent bank of the overseas institution; or
- Evidence of its licence or authorization to conduct financial and/or banking business.

International publications and directories or any of the international business information services may also be used to reinforce any of the above sources.

14.0 Identification Procedures for Other Institutions and Bodies

14.1a Clubs and Societies

With respect to applications made on behalf of **clubs or societies**, Branch Management should be satisfied about the legitimate purpose of each organization by sighting its constitution. The identification requirements prescribed for natural persons apply to the key officers of clubs and societies.

14.1b Charity

When processing an application by **a charity** to open an account, Branch Management should satisfy itself that the charity is registered and has a legitimate purpose by sighting its constitution. Satisfactory evidence of the identity of the authorized signatories if they are not already known to the institution, in keeping with the due diligence requirements for natural persons, should be obtained.

14.1c Religious Organization

Branch Management should verify the identity of **a religious organization** by confirming its status with the company registry. The identity of the signatories to its account should also be duly verified.

14.1d Government and its agencies

For **Governments and their Agencies**, Officers should establish the status of the applicant before opening an account. A certified copy of the resolution or other document authorizing the opening of the account or undertaking the transaction should be obtained in addition to evidence that the official representing the agency has the relevant authority to act.

14.1e Foreign Embassies and Consulates

In respect of **Foreign Consulates**, there is need to verify the status of applicants requesting to open accounts or undertake transactions in the names of resident Foreign Consulates and any supporting documents by reference to the relevant Government Ministry or competent authority.

14.2 Correspondent Banking

It is incumbent on the Bank to manage its correspondent banking transactions proactively by taking a risk-based approach. Accordingly, it would have to be ensured that correspondent banks are effectively regulated for Anti-Money

Laundering control and have effective customer acceptance and KYC policies.

The Bank would not enter into or continue correspondent banking relationships with banks incorporated in jurisdictions which are identified as high risk because they have poor KYC standards or have been designated as being non-co-operative in the fight against money laundering.

The Bank would guard against receiving funds through its accounts without Treasury or Trade Finance officers taking adequate measures to satisfy themselves that sufficient due diligence had been undertaken by the remitting bank on the underlying client and the origin of the funds. The Bank would consider terminating its relationship with correspondent

Banks that do not respond adequately to customer due diligence and suspicious transactions queries.

15.0 One-Off Cash Transactions

Cash remittances and wire transfers (whether inward or outward) or other monetary instruments that are undertaken against payment in cash for customers who do not have an account or other established relationship with the Bank (i.e. walk-in customers) represent a high risk money laundering category. Thus, adequate procedures should be established to record the transactions and take relevant identification evidence where necessary. Limits for requiring identification evidence should be set at a significantly lower level than that for normal transactions.

15.1 Reinvestment of Income

Where the proceeds of a one-off transaction are to be payable to a customer, but are then to be invested on his behalf and can only be further reinvested or paid directly to him, and for which a record is to be kept, the identification requirement should be carried out in keeping with the procedure set out for natural persons.

16.0 Monitoring, Recognising and Responding to Suspicious Transaction

All transactions of customers – both permanent and walk-in, including remittances, electronic transactions and e-banking products (card transactions and virtual channels like mobile money, mobile banking and cash management) shall be monitored to ensure that they are consistent with the bank's knowledge of the customer(s) involved, their businesses and risk profile performed on them during the onboarding stages. Continuous monitoring of high risks accounts shall be risk-based in line with FATF Recommendation 10.

When any staff of the Bank detects any "red flag" or suspicious money-laundering activity, the staff is required to promptly report to the AML Reporting Officer who shall commence an immediate investigation. Upon the establishment of a prima facie case, a Suspicious Transaction or Activity Report shall be filed with the Financial Intelligence Centre within twenty-four hours of knowledge of same by the AML Reporting Officer

16.1 Definition of a Suspicious Transaction

There are numerous types of suspicious transactions, reflecting the various ways in which money launderers operate. For the purpose of this manual, 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, such as a transaction that is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.

16.2 Training in respect of suspicious transactions

The AML Reporting Officer would train staff to a level that would enable them to monitor, recognize and respond appropriately to suspicious transactions. A list of Money Laundering, ''Red Flags'' is provided in Appendix iii. The AML/CFT Compliance Officer shall supervise the monitoring and reporting of suspicious transactions. The Bank would be alert to the various patterns of conduct that have been known to be suggestive of money laundering and maintain a checklist of such transactions which would be disseminated to the relevant staff.

When any staff of the financial institution detects any ''red flag'' or suspicious money laundering activity, he or she should promptly institute a review under the supervision of the Compliance Officer who will then issue a suspicious transaction report (STR) to the appropriate authorities.

16.3 Filing A Suspicious Transaction Report (STR)

Where the Compliance Officer knows, suspects or has reason to believe that:

- A transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity;
- A transaction is designed, whether through structuring or otherwise, to evade the reporting requirements;

- A transaction has no business or apparent lawful purpose or is not the type in which the customer would normally be expected to be engaged in; or
- A transaction involves the use of the institution to facilitate a criminal activity,

the Compliance Officer shall file a suspicious transaction report. See Appendix VI. The Compliance Officer should not base the decision to file a suspicious transaction report solely

on whether the transaction falls above the prescribed threshold but should file such a report in all circumstances where transactions raise reasonable suspicion of criminal, corrupt, or terrorist activities.

The Compliance Officer should report suspicious transactions by completing the prescribed STR form and collect and retain the supporting documentation as required by law and regulations.

16.4 Currency Transaction Report (CTR) and Other Statutory Reports and Returns

The Bank shall at all times, comply with key provisions of the Laws, Rules, Regulations and Guidelines governing our operations. In this regards, CTRs meeting the current minimum reporting threshold of Fifty thousand Ghana Cedis (GHS50,000.00) and above, or its equivalent in other foreign currencies shall be submitted timeously. Suspicious Transactions and other compliance reports shall also be submitted to the respective supervisory body as and when they are due.

16.5 Cash Management

The bank shall put in place prudent cash management systems and policies to check "aggregation" of cash deposits and withdrawals made at different times, days, or branches for linked accounts (belonging to the same customer). This shall be done with the aid of an AML monitoring tool.

16.6 Funds/Wire Transfers

Funds transfer requests from customers shall be strictly subjected to AML and Foreign Exchange Acts to guard against any breach. Domestic funds transfers, using the Automated Clearing House and the Ghana Interbank Settlement Systems, with the amount exceeding Ghs100,000.00, shall not be effected without recourse to the Treasury Department. Funds transfer outside Ghana shall be supported with the required documentation before they are effected.

17.0 Remittance Services

The Bank's AML/CFT Policy is derived from the direction of Bank of Ghana (BoG) and the Financial Intelligence Centre's (FIC) Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Guideline for Banks and Non-Bank Financial Institutions in Ghana, July 2018, as well as the Financial Action Task Force (FATF) Recommendations,

June 2019. It shall at all times be the reference point for all AML/CFT issues hence, applicable to remittance services and branch networks. Where there appears to be grey areas for clarity in a specific product line and for which there is no definite solution in the bank AML/CFT policy, reference may be made to the respective remittance service's AML/CFT control regime and International best practice.

17.1 Detection of Suspicious Transaction

Where a transaction is detected to be suspicious – whether by an internal alert from any of our pay points, or escalated to us by our partners, the bank shall take immediate steps to investigate and where need be, file a suspicious transaction report to the Financial Intelligence Centre and inform our respective partner.

18.0 An Audit Function to Test the System

There shall be an Independent audit function to test the AML system. This periodic audit test will help review the AML/CFT framework with a view to determine its adequacy, effectiveness and completeness.

19.0 Additional Areas of AML/CFT Risk

The bank shall review, identify and record other areas of potential Money Laundering risk not covered by the AML & CFT Guideline and report same half year to Bank of Ghana (BoG) and the Financial Intelligence Centre (FIC).

20.0 AML/ CFT Record Keeping

The Bank shall maintain all necessary records on transactions, both domestic and international; all records obtained through CDD measures, account files and business correspondences and results of any analysis undertaken for at least five (5) years following completion of the transaction. This will enable the Bank to comply swiftly with information requests from Competent authorities in tandem with FATF Recommendation

To accomplish this, document retention policies has been set and procedures would be established for maintaining AML/CFT records. In establishing document retention policy,

the Bank would be guided by both statutory requirements and the needs of the investigating authorities on the one hand and commercial considerations, on the other.

The broad categories of AML/CFT-related records are:

- Customer identification and verification documents.
- Transaction records, including currency transaction reports.
- Suspicious transaction reports, together with supporting documentation.

AML/CFT-related records may be maintained by way of original documents, stored in microfiche, and in computerized or electronic form, subject to the provisions of the law on what is acceptable as evidence.

The Compliance Officer or other designated officer shall be responsible for ensuring that all AML/CFT records are maintained properly and kept for not less than five (5) years before they are sent to the archives.

21.0 Employee Education and Training Programme

21.1 Institutional Policy

Anti-Money Laundering laws in various jurisdictions impose certain obligations on financial institutions and their staff and prescribe criminal sanctions for non-compliance. It is, therefore, imperative that Head/HRD in consultation with the Compliance Officer design comprehensive employee education and training programmes not only to make staff fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks.

21.2 Trainees

The employee training programme would be tailored to meet the perceived needs of the Bank's staff. Nevertheless, a comprehensive training programme would encompass the following staff/areas:

- Compliance Officers.
- New Staff – as part of the orientation programme for those posted to the front office as well as National Service Persons.
- Banking Operations/Branch Office staff, particularly cashiers, account opening, mandate,
  and marketing staff.
- Internal Control/Audit staff

- Managers.

21.3 Content of the Training Programme

The employee training programme shall be developed under the guidance of the AML/CFT Compliance Officer in collaboration with top the Human Resources Department. The basic elements of the employee training programme shall include but not limited to:

- AML regulations and offences
- Know Your Customer/ Customer Due Diligence(KYC/CDD)
- The nature of money laundering
- Money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies.
- Reporting requirements.
- The need to combat Money Laundering
- The effects of Money Laundering
- Risk-based approach to AML/CFT.
- Record keeping and retention policy.

22.0 Monitoring of Employee Conduct

The AML Reporting Officer shall have unfettered access to and monitor all employee accounts for potential signs of money laundering. The latter's own account is to be reviewed by the Chief Internal Auditor or a person of adequate/similar seniority. Employee accounts would be subjected to the same AML/CFT procedures as applicable to other customers' account. Compliance reports including findings are to be rendered to the BOG and FIC at the end of June and December every year.

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

23.0 Tipping Off

The bank, its directors, officers, and employees are prohibited from disclosing the fact that an STR or related information is being reported to the FIC. The identity of the Reporting Officer or any designated officer investigating such transaction shall not be revealed. A risk exists that customers could be unintentionally tipped off when the financial institution is seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigations could

compromise future efforts to investigate. If the bank reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR.

24.0 Protection for Staff who report violations

The bank shall direct its staff in the employees AML Hand book to always co-operate fully with the Regulators and law enforcement agencies. They are also required to make it possible for employees to report any violations of the Institution's AML/CFT compliance programme to the AML/CFT Reporting Officer. Where the infractions involve the Reporting Officer, employees are required to report such to a designated higher authority such as the Chief Internal Auditor.

The bank shall inform its staff in the employees AML Hand book to make such reports confidential and in good faith and that they will be protected from victimization, civil and criminal liabilities for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and regardless of whether illegal activity actually happened.

24.1 Administrative sanctions against staff that violate AML regulations

Any member of Staff that is suspected or found to have contravened any of the AML regulations like tipping-off, aiding and abetting Money Laundering activities, etc, shall be made to appear before the disciplinary committee of the bank. Such a person when found guilty shall be sanctioned according to the rules of the bank, and may not be insulated from further civil and criminal liabilities under the AML Law.

24.2 Penalty for Money Laundering infractions under the AML Act

A person who contravenes Section 1 (Money Laundering) or Section 2 (Aiding and abetting money laundering activities) of the AML Act 2008 (Act 749) as amended, commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not less than twelve months and not more than ten years or to both.

25.0 Willful Blindness

This is the deliberate avoidance of knowledge of the facts" or "purposeful indifference." Courts have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction. The bank shall consider or treat any act of willful blindness on the part of any staff or customer in tandem with how the Courts have interpreted same.

26.0 Concluding note

In the preparation of this Policy and Manual, deliberate efforts have been made to capture and adopt industry best practice. This document shall be reviewed biennially. Nevertheless, should there be a major change in the AML regime whether globally, in the sub region or nationally that calls for adoption, the bank shall co-opt that relevant information into this document.

APPENDICES
Appendix 1:
Categories of Financial Institutions

(i) FATF 40 Recommendations – lists 13 types of activities/operations/transactions. This is useful for regulatory/supervisory purposes because it provides a comprehensive list of financial activities and leaves little room for regulatory arbitrage. The FATF guidelines states that ''Financial Institutions'' means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

- Acceptance of deposits and other repayable funds from the public.
- Lending.
- Financial leasing.
- The transfer of money or value.
- Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
- Financial guarantees and commitments.
- Trading in:
  (a) money market instruments (cheques, bills, CDs, derivatives etc.);
  (b) foreign exchange;
  (c) exchange, interest rate and index instruments;
  (d) transferable securities;
  (e) commodity futures.
- Participation in securities issues and the provision of financial services related to such issues.
- Individual and collective portfolio management.
- Safe-keeping and administration of cash or liquid securities on behalf of other persons.
- Otherwise investing, administering or managing funds or money on behalf of other persons.
- Underwriting and placement of life insurance and other investment relating insurance.

- Money and currency changing.

The FATF Guidelines further provide that:

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

''In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above''.

(ii) From an institutional perspective, 5 broad categories have been identified; by the FATF:

- Banks and other credit institutions;
- Securities;
- Insurance;
- Bureau de Change
- Money Remittance.

This broad categorization is particularly useful for conducting surveys, typologies studies and analytical purpose.

(iii) Subject to the provisions of the relevant national anti-money laundering laws and regulations, financial institutions are encouraged to adopt the FATF definition and type categories of financial institutions.

APPENDIX II:

Categories Of Non-Financial Businesses And Professions (DNFBPs)

(i) **FATF Categories**

- Casinos (which also includes internet casinos).
- Real Estate Agents.
- Dealers in precious metals and dealers in precious stones.
- Lawyers, notaries, other independent legal professionals and accountants.
- Trust and company service providers – all persons or businesses that are not covered elsewhere.

APPENDIX III
Money Laundering And Terrorist Financing ''Red Flag''

1. **Introduction**

Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Financial institutions should, therefore, endeavour to put in place effective and efficient transaction monitoring programmes to facilitate the process. Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering.

This Appendix, which lists various transactions and activities that indicate potential money laundering, may not be exhaustive but it does reflect the ways in which money launderers have been known to operate.

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

2. Suspicious Money Laundering Transactions And ''Red Flags''

(i) Transactions Generally Perceived Or Identified As Potentially

Suspicious Of Money Laundering

- Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.
- Transactions involving shell companies.
- Transactions with correspondents that have been identified as higher risk.
- Large transaction activity involving monetary instruments such as traveller's cheques, Bank drafts, money order, particularly those that are serially numbered.
- Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test an institution's own internal monitoring threshold or controls.

(ii) Typologies Of Money Laundering Using Cash Transactions

- Significant increases in cash deposits of an individual or corporate entity without apparent cause, particularly if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- Unusually large cash deposits made by an individual or a corporate entity whose normal business is transacted by cheques and other non-cash instruments.
- Frequent exchange of cash into other currencies.
- Customers who deposit cash through many deposit slips such that although the amount of each deposit is relatively small, the overall total is quite significant.
- Customers whose deposits contain forged currency notes or instruments.
- Customers who regularly deposit cash to cover applications for Bank drafts.
- Customers making large and frequent cash deposits but with cheques always drawn in favour of persons not usually associated with their type of business.
- Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.
- Branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors.
- Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(iii) **Money Laundering Using Deposit Accounts**

The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business.

- Minimal, vague or fictitious information is provided by a customer which a deposit money bank is not in a position to verify.
- Lack of reference or identification in support of an account opening application by a person who is unable or unwilling to provide the required documentation.
- A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening a bank account.
- Customers maintaining multiple accounts at a bank or different banks for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.
- Customers depositing or withdrawing large amounts of cash with no apparent business source or in a manner inconsistent with the nature and volume of the business.
- Accounts with large volumes of activity but low balances or frequently overdrawn positions.
- Customers making large deposits and maintaining large balances with no apparent rationale.
- Customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances. Typically, these transactions are not consistent with the customers' legitimate business needs.
- Sudden and unexpected increase in account activity or balance arising from deposit of cash and non-cash items. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly.
- Accounts that are used as temporary repositories for funds that are subsequently transferred outside the Bank to foreign accounts. Such accounts often have low activity.
- Customer requests for early redemption of certificates of deposit or other investment soon after the purchase, with the customer being willing to suffer loss of interest or incur penalties for premature realization of investment.

- Customer requests for disbursement of the proceeds of certificates of deposit or other investments by multiple cheques, each below the stipulated reporting threshold.

- Retail businesses which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs.

- Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks.

- Substantial cash deposits by professional customers into client, trust or escrow accounts.

- Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

- Greater use of safe deposit facilities by individuals, particularly the use of sealed packets which are deposited and soon withdrawn.

- Substantial increase in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

- Large number of individuals making payments into the same account without an adequate explanation.

- High velocity of funds that reflects the large volume of money flowing through an account.

- An account opened in the name of a money changer that receives deposits.

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

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

- Over and under-invoicing of goods.
- Multiple invoicing of goods and services.
- False described goods and services and ‘’phantom’’ shipments whereby the exporter does not ship any goods at all after payments had been made, particularly under confirmed Letters of Credit.

- Transfer pricing.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Items shipped are inconsistent with the nature of the customer's normal business and the transaction lacks an obvious economic rationale.
- Customer requests payment of proceeds to an unrelated third party.
- Significantly amended Letters Of Credit without reasonable justification or changes
- to the beneficiary or location of payment.

(v) **Lending Activity**

- Customers who repay problem loans unexpectedly.
- A customer who is reluctant or refuses to state the purpose of a loan or the sources

of repayment or provides a questionable purpose and/or source of repayment.
- Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- Loans lack a legitimate business purpose, provide the bank with significant fees for assuming minimal risk, or tend to obscure the movement of funds (e.g. loans made to a borrower and immediately sold to an entity-related to the borrower).

(v) **Terrorist Financing ''Red Flags''**

- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g. student, unemployed, or self-employed).
- Financial transaction by a non-profit or charitable organization, 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 organization and other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box
- Large number of incoming or outgoing funds transfers takes place through a business account and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high-risk locations.
- The stated occupation of the customer is inconsistent with the type and level of account activity.

- Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which should ordinarily be expected.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
- Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

(vi) **Other Unusual Or Suspicious Activates**

- Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.
- Employee fails to comply with approved operating guidelines, particularly in private banking.

- Employee is reluctant to take a vacation.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area despite the availability of such services at an institution closer to them.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high value assets awaiting conversion to currency, for placement in the banking system.
- Customer uses a personal account for business purposes.
- Official Embassy business is conducted through personal accounts.

- Embassy accounts are funded through substantial currency transactions.
- Embassy accounts directly fund personal expenses of foreign nationals.

APPENDIX IV
Checklist of Politically Exposed Persons (PEPs)

The definition of PEPs by national regulatory authorities and best guidance international bodies such as the FATF, is generally broad and gives room from differing interpretations. For instance, the FATF in the forty recommendations defines PEPs as ''individuals who are or have been entrusted with prominent public functions – for example, Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.'' The Basel Committee on Banking Supervision, in its Customer Due Diligent for Banks paper, defines PEPs in similar terms.

In the light of the varying interpretations, there is need to avoid being too restrictive, thereby undermining AML effectiveness or unduly broad resulting in overburdening designated institutions and targeting the wrong persons. However, given the widespread nature of corruption in the regional socio-political environment and the possibility that even some middle-ranking officials would abuse their public powers for their own illicit enrichment through bribes, embezzlement, etc. it makes sense to adopt a sufficiently definition.

Consequently, the following checklist is provided for the guidance of financial institutions and designated non-financial businesses and professions to enable them conduct effective PEP screening processes:

- Heads of state, government and cabinet ministers.
- Heads of government ministries, departments and agencies.
- Senior Judges/Judicial Officers.
- Senior political party functionaries.
- Members of ruling royal families
- Senior military officers.
- Family members and close associates of PEPs.
- Middlemen, consultants and advisers to PEPs.
- Private companies, trusts and foundations linked to PEPs.
- Members of Parliament.
- Managing Directors and all Board Members on State owned Enterprises and

Departments.

The above checklist is informed by the need not only to target PEPs but also to scrutinize all those who, whether as family members, close associates or advisers and consultants – the people behind the PEPs benefit from being close to such persons and are often used by them as fronts for laundering the proceeds of crime.

APPENDIX V
List of 21 Common Predicate Offences

FATF Designated Categories of Predicate Offences Is As Follows:

- Participation in an organized criminal group and racketeering.
- Terrorism, including terrorist financing.
- Trafficking in human beings and migrant smuggling.
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances.
- Illicit dealing in arms.
- Trafficking in stolen and other goods
- Corruption and bribery.
- Fraud.
- Counterfeiting currency.
- Counterfeiting and piracy of products

- Environmental crime.
- Murder, grievous bodily injury.
- Kidnapping, illegal restraint and hostage-taking.
- Robbery or theft.
- Smuggling
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation
- Tax Evasion

Recommendation

Adopt the FATF categories of designated offences and encourage non-compliant jurisdictions to up-date their laws accordingly.