FIDELITY LIFE MUTUAL BENEFIT ASSOCIATION, INC.

ANTI-MONEY LAUNDERING OPERATING MANUAL

TABLE OF CONTENTS

I. INTRODUCTION

Fidelity Life Mutual Benefit Association Inc. (FLMBAI) is a non-stock association organized not for profit but solely for the purpose of providing life insurance benefits to its members out of fixed contributions collected from them. FLMBAI was duly recognized and authorized by the Philippine Insurance Commission and registered with the Securities and Exchange Commission. Its home office is located at 9th Floor, King's Court Building 1, 2129 Chino Roces Avenue, Makati City.

FLMBAI in compliance with Circular Letters Nos. 2018-48 and 2018-60 of the Insurance Commission; Republic Act No. 9160, ("The Anti-Money Laundering Act of 2001" or "AMLA, As Amended"); Republic Act No. 10168, ("The Terrorism Financing Prevention and Suppression Act"); their respective Revised lmplementing Rules and Regulations (RIRRs); and the Anti-Money Laundering and Combating the Financing of Terrorism Guidelines ("Guidelines"), hereby formulates this Anti-Money Laundering Operating Manual ("Operating Manual").

II. DEFINITION OF TERMS

For purposes of this Operating Manual, the following terms are hereby defined as follows:

A. Anti-Money Laundering Act (AMLA) refers to Republic Act No. 9160, as amended by Republic Act Nos. 9194, 10167, 10365 and 10927.

B. Anti-Money Laundering Council (AMLC) refers to the financial intelligence unit of the Philippines which is the government agency tasked to implement the AMLA.

C. Financing of Terrorism refers to a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds, or financial service or other related services, by any means, with the inlawful and willful intention that they should be used, in full or in part: (i) carry out or facilitate the commission of any terrorist act; (ii) by a terrorist organizations, association or group; or (iii) by an individual terrorist.

D. Covered transaction refers to:

1. A transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (Php500, 000. 00) or its equivalent in any other currency; or
2. A transaction, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), where the total premiums/fees paid for a policy, plan or

agreement for the entire year exceeds Five Hundred Thousand Pesos (Php500, 000.00) or its equivalent in any other currency.

E. Suspicious Transaction refers to a transaction, regardless of amount, where any of the following circumstances exists:

1. There is no underlying legal or trade obligation, purpose or economic justification;
2. The customer is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the customer;
4. Taking into account all known circumstances, it may be perceived that the customer's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
5. Any circumstance relating to the transaction which is observed to deviate from the profile of the customer and/or the customer's past transactions with the covered person;
6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense that is about to be committed, is being or has been committed; or
7. Any transaction that is similar, analogous or identical to any of the foregoing.

Any unsuccessful attempt to transact with an ICRE, the denial of which is based on any of the foregoing circumstances shall likewise be considered as suspicious transaction.

F. Politically Exposed Person (PEP) refers to an individual who is or has been entrusted with prominent public position in (1) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (2) a foreign State; or (3) an international organization.

The term PEP shall include immediate family members, and close relationships and associates that are reputedly known to have:

1. Joint beneficial ownership of a legal entity or legal arrangement with the main/Principal PEP; or
2. Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP.

G. Immediate Family Member of PEPs refers to spouse or partner; children and their spouses; siblings; and parents and parents-in law.

H. Close Associates of PEPs refer to persons who are widely and publicly known to maintain a particularly close relationship with the PEP and include persons who are

in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

I. Monetary Instrument shall include, but is not limited to the following:

1. Coins or currency of legal tender of the Philippines, or of any other country;
2. Credit instruments, including bank deposits, financial interest, royalties, commissions, and other intangible property;
3. Drafts, checks, and notes;
4. Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument whether written or electronic in character, including those enumerated in Section 3 of the Securities Regulation Code;
5. A participation or interest in any non-stock, non-proflt corporation;
6. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts, or deposit substitute instruments, trading orders, transaction tickets, and confirmations of sale or investments and money market instruments;
7. Contracts or policies of insurance, life or nonlife, contracts of suretyship, pre-need plans, and member certificates issued by mutual benefit association; and
8. Other similar instruments where title thereto passes to another by endorsement, assignment, or delivery.

J. Unlawful Activity refers to any act or omission, or series or combination thereof, involving or having direct relation, to the following:

1. “Kidnapping for Ransom" under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;
2. Sections 4, 5, 6, 8, 9, 10, 11, 12,13, 14,15 and 16 of Republic Act No. 9165, otherwise known as the "Comprehensive Dangerous Drugs Act of 2002”;
3. Section 3 paragraphs b, c, e, g, h and i of Republic Act No. 3019, as amended, otherwise known as the "Anti-Graft and Corrupt Practices Act”;
4. "Plunder' under Republic Act No. 7080, as amended;
5. "Robbery” and "Extortion" under Articles 294, 295, 296, 299, 300, 30l and 302 of the Revised Penal Code, as amended;
6. "Jueteng” and "Masiao" punished as illegal gambling under Presidential Decree No. 1602;
7. "Piracy on the High Seas" under the Revised Penal Code, as amended, and Presidential Decree No. 532:
8. "Qualified Theft” under Article 310 of the Revised Penal Code, as amended;
9. "Swindling” under Article 315 and "Other Forms of Swindling" under Article 316 of the Revised Penal Code, as amended:

10. "Smuggling" under Republic Act No. 455, and Republic Act No. 1937, as amended, otherwise known as the "Tariff and Customs Code of the Philippines";
11. Violations under Republic Act No. 8792, otherwise known as the "Electronic Commerce Act of 2000";
12. "Hijacking" and other violations under Republic Act No. 6235, otherwise known as the "Anti-Hijacking Law", Destructive Arson"; and "Murder", as defined under the Revised Penal Code, as amended
13. "Terrorism" and "Conspiracy to Commit Terrorism" as defined and penalized under Sections 3 and 4 of Republic Act No. 9372;
14. "Financing of Terrorism" under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of Republic Act No. 10168, otherwise known as the "Terrorism Financing Prevention and Suppression Act of 2012";
15. "Bribery" under Articles 210, 211 and 211-A of the Revised Penal Code as amended;
16. "Frauds and Illegal Exactions and Transactions "under Articles 213, 214, 215 and 216 of the Revised Penal Code as amended;
17. "Malversation of Public Funds and Property" under Article 217 and 222 of the Revised Penal Code, as amended;
18. "Forgeries" and Counterfeiting" under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code;
19. Violations of Sections 4 to 6 of Republic Act No. 9208 otherwise known as the "Anti-Trafficking in Persons Act of 2003, as amended;
20. Violations of Sections 78 and 79 of Chapter IV of Presidential Decree No. 705, otherwise known as the "Revised Forestry Code of the Philippines as amended;
21. Violations of Sections 86 to 106 of Chapter VI of Republic Act No. 8550 otherwise known as the "Philippine Fisheries Code of 1998";
22. Violations of Sections 101 to 107 and 110 of Republic Act No. 7942, otherwise known as the "Philippine Mining Act of 1995";
23. Violations of Section 27 (c), (e), (f), (g), and (i) of the Republic Act No. 9147 otherwise known as the "Wildlife Resources Conservation and Protection Act";
24. Violation of Section 7(b) of Republic Act No. 9072, otherwise known as the "National Caves and Cave Resources Management Protection Act;
25. Violation of Republic Act No. 6539, otherwise known as the "Anti-Carnapping Act of 1972 as amended";
26. Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree "Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives;
27. Violation Presidential Decree No.1612, otherwise known the "Anti-Fencing Law";
28. Violation of Section 6 of Republic Act No. 8042, otherwise known as the "Migrant Workers and Overseas Filipinos Act of 1995, as amended;

29. Violation of Republic Act No. 8293, otherwise known as the "Intellectual Property Code of the Philippines" as amended;
30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the "Anti-Photo and Video Voyeurism Act of 2009";
31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the "Anti-Child Pornography Act of 2009";
32. Violation of Sections 5, 6, 7, 8, 9, 10 (c), (d) and (e), 11, 12 and 14 of Republic Act No, 7610 otherwise known as the "Special Protection of Children Against Abuse, Exploitation and Discrimination";
33. Fraudulent practices and other violations under Republic Act No. 8779, otherwise known as the "Securities Regulation Code of 2000";
34. Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

In determining whether or not a felony or offense punishable under the penal laws of other countries is "of similar nature", as to constitute an unlawful activity under the AMLA, the nomenclature of the said felony or offense need not be identical to any of the unlawful activities listed above.

K. Money Laundering - Money laundering is committed by:

1. Any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

    a. Transacts said monetary instrument or property;
    b. Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
    c. Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
    d. Attempts or conspires to commit money laundering offenses referred to in (a), (b), or (c) above;
    e. Aids, abets, assists in, or counsels the commission of the money laundering offenses referred to in (a), (b) or (c) above; and
    f. Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in (a), (b), or (c) above.

2. Any covered person who, knowing that a covered or suspicious transaction is required under the AMLA to be reported to the AMLC, fails to do so.

III. RISK ASSESSMENT AND MANAGEMENT SYSTEM

FLMBAI shall adopt the following guidelines in assessing Anti-Money Laundering/ Counter- Financing of Terrorism (AML/CFT) risks:

1. Establish, implement, monitor and maintain an effective AML/CFT Compliance Program in line with the Guidelines;
2. Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential AML/CFT activities such as but not limited to the following:
   a. Compliance Regime;
   b. Risk Assessment;
   c. Customer Due Diligence;
   d. Training and Awareness;
   e. Employee Screening;
   f. Detection of Suspicious Transactions (STRs); and
   g. Reporting Covered (CTRS) and Suspicious Transactions.
3. Carry-out on a regular basis, independent periodic review of the ML/FT Prevention Program to manage and mitigate the risks identified;
4. Adopt a risk-based approach to know the company's customers based on their profiles;
5. Conduct institutional risk assessment within the company at least once every two (2) years or as may be determined by the AMLC;
6. Ensure submission of the risk assessment information as may be required by the Insurance Commission (IC); and
7. Assist law enforcement in combating illegal money laundering, and minimize the risk of company resources being used for improper purposes.

A. RISK-BASED APPROACH

Due to FLMBAI's nature of business of providing insurance premium to its clients, a risk-based approach shall be used to calculate the inherent risk present in each transaction. Each risk factor is usually assigned a score which reflects the associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas.

While establishing a business relationship with its customers, FLMBAI shall consider the following four (4) risk elements:

1. Product Risk
2. Interface or Delivery Channel Risk
3. Jurisdiction or Geographical Area Risk
4. Customer Risk

1. PRODUCT RISK

FLMBAI shall have a **Money Laundering Detection System (MLD System)** to assess and document the risks of money laundering, terrorist financing and other illicit activities posed by the insurance premium that it offers to its customers.

MLD System has the following features:

a. The system provides for the matching of customer data with sanction lists and PEP lists. It monitors the customer's day-to-day transactions which classifies the specific risk/s of money laundering involved in such transaction like transactions to suspected shell company.
b. After determining the kind of transaction of a particular customer, the system will generate a rating based on the classification of the customer's transaction such as transactions of PEP list with a high rating.
c. It enables the Accounting Department to determine the volume of insurance premium and account types offered by FLMBAI to its customers, thereby determining the account balance of each customer.
d. The system generates data of a particular product (insurance premium) involved in a customer's transaction. Using this data, FLMBAI can be able to determine the risk classification and its corresponding rating and the degree of money laundering risk involved in the insurance premium offered by FLMBAI e.g. low risk versus moderate, versus high versus higher risk, to determine the overall inherent product risk.

   An example table of inherent increased risk scores for different Product/ Transaction is set out in **Appendix A.**

2. INTERFACE OR DELIVERY CHANNEL RISK

FLMBAI shall have a transaction monitoring software known as **"SAS Software"** to address specific risk of Money Laundering, Terrorist Financing and other illicit activities posed by the different types of interface and technological developments through which business relationships are started, conducted and maintained. Money laundering risks can be mitigated by monitoring the activities of the clients. Nonregulated clients or those that are not well known or identified by FLMBAI are much more likely to present a higher inherent risk of money laundering.

The SAS Software features include:

a. Monitoring of customer transactions on a daily basis starting from the application process, by conducting assessment on whether, and to what extent, the method of account origination or account servicing, such as non-face-to-face account opening or the involvement of third parties, including intermediaries.

b. The assessment of the customer's transaction involves account verification which classifies the transaction as face-to-face or non-face-to-face via intermediary, mail or phone.
c. The system has streamlined user interface where FLMBAI can make determinations of ML/CFT faster and much more efficiently and it an navigate between two separate objects. First, it detects transaction records of a particular client by applying a user modeling, then it monitors a new transaction with the same client, comparing it against the corresponding user model and determines if this transaction is unusual.
d. It has the ability to file timely and accurate STRs generated by the system by monitoring new lines of business or new client types or emerging risks.

A table of inherent risk score examples for different delivery channel is set out in **Appendix B.**

3. JURISDICTION RISK

FLMBAI shall have a **Comarch AML Software (C.A.S)** which significantly increases the efficiency of suspicious transaction detection of the customer's transaction within FLMBAI.

The C.A.S has the following features:

a. It has data mining techniques based on historical data which can determine with accuracy the past and present transactions of a particular customer within FLMBAI.
b. It monitors the transaction audit logs of FLMBAI's Cashier Department which can spot data and detect suspicious or covered transaction when the total amount of a particular client/transaction exceeds Php 500, 000.00 within a day.
c. The system calculates the customer's transaction behavior score based on transaction history, then it marks the transaction as suspicious and later on it generates an alert if a significant difference is detected in customers historical transactional pattern and the current behavior.
d. The system has clustering-based approach which is use in grouping transactions/accounts into clusters based on their similarities. This technique helps in building patterns of suspicious sequence of transactions and detecting risk patterns of customer's account.
e. By applying anomaly detection, it has the potential to identify transaction which do not conform to an expected pattern in a dataset and improve the said detection by uncovering new money laundering patterns.
f. It also uses techniques and unlabeled data to detect customer's abusive activities. Once anomaly is detected, it gets categorized and a binary classification is being used to categorize anomalies. Such alert prioritization greatly speeds up the work of AML team.

4. CUSTOMER RISK

FLMBAI shall have a **Customer Identity Management System (CIM System)** which shall monitor the identity of the client using CDD to identify the risk present in each customer.

CIM System has the following features:

a. The system can be used to classify the customer base and to identify customer risks such as customer type, ownership, industry, activity, profession and/or business, thereby determining the risk rating present in each customer.
b. The customer risk rating determines the different treatments customer's identification, verification and additional customer informations. It allows the monitoring and periodic review of customer required under the Guidelines.
c. It also provides for the checking of Sanction Lists and Politically Exposed Persons Lists.
d. It provides detailed procedures in auditing and reporting of STR/CTR whenever there are doubts as to the identity or transaction of the customer concern.
e. Each customer type is assigned a risk score, depending upon the expected amount of ML risk each type carries, the number of customers that fall within each customer type should then be determined. This data can be utilized to determine what percentage of each customer types are rated according to the risk classification, e.g. low risk versus moderate, versus high versus higher risk, in order to determine the overall inherent customer risk.

   A table of inherent risk score examples for different customer risks is set out in **Appendix C.**

To minimize customer risk, the following guidelines shall be followed by the employees and key staffs while performing their duties:

1. Ensure to assess and document the risks of money laundering, terrorist financing and other illicit activities by different type of customers such as Individuals, Legal entities (Companies, Partnership, Trusts, Nominees shareholders & Power of Attorney holders and Politically Exposed Persons);
2. Obtain prior approval from the Management Committee before entertaining business relationship with non-profit organizations or with customer's requiring enhanced customer due diligence measures;
3. Warrants prior approval from the Management Committee before entering into business relationships with Politically Exposed Persons (PEP); and
4. Certifies Enhanced Customer Due Diligence (EDD) and on-going monitoring if an employee suspects that a customer is an individual, a charity, non-profit

organization, legal entity that is associated with, or involved in, terrorist acts or terrorist financing activities.

B. CUSTOMER RISK ASSESSMENT

FLMBAI shall adhere to customer acceptance policies and procedures, specifying a set of criteria of the types of customers that are likely to pose low, normal or high ML/TF risk to its operations.

1. RISK PROFILING

In designing a customer acceptance and risk profiling policy, the following criteria shall be taken into account:

a. The customer risk;
b. The nature of the service/s or product/s to be availed of by the customers;
c. The delivery channels, including cash-based, face-to-face or non-face-to face or cross-border movement of cash
d. The purpose of the transaction;
e. The amount of funds to be transacted by a customer or the size of transactions undertaken;
f. The regularity or duration of the transaction;
g. The fact that a customer came from a high-risk jurisdiction;
h. The existence of suspicious transactions indicators; and
i. Such other factors that may deem reasonable or necessary to consider in assessing the risk of customer to ML/TF.

2. CUSTOMER DUE DILIGENCE (CDD)

FLMBAI shall implement the following CDD Standards:

a. Identify and verify the identity of customers using reliable, independent, source documents, data or information;
b. Verify the identity of any person purporting to act on behalf of the customer and the identity of the beneficial owner;
c. Understand and obtain information and the purpose and intended nature of the business relationship;
d. Conduct ongoing due diligence on the business relationship;
e. Clients shall be made aware of the company's explicit policy that transactions will not be conducted with applicants in the event of failure to complete verification of any relevant subject or to obtain information on the purpose and intended nature of the business relationship and it shall not include the application, perform the transaction or shall terminate the business relationship;

f. Where FLMBAI has already commenced the business relationship and is unable to comply with the verification requirements, it shall terminate the business relationships and consider making suspicious transaction report;
g. Applicants who present only photocopies of identifications and other documents shall be required to produce the original documents for verification purposes; and
h. FLMBAI shall designate an officer or staff authorized to obtain from the customers the necessary informations or documents relative thereto.

CUSTOMER IDENTIFICATION

FLMBAI shall obtain the following minimum information/documents from individual customers/members or when the applicant is acting in a representative capacity:

1. complete name;
2. date and place of birth;
3. name, address and contact information of beneficial owner
4. name of the beneficiary;
5. present address or residence in the Philippines or abroad (non-resident);
6. residence telephone numbers
7. permanent/mailing address;
8. contact number or information;
9. nationality;
10. specimen signature or biometrics of the customer
11. proof of identification;
12. nature of work and name of employer or nature of self-employment/ busines (address and contact number)
13. sources of funds or property;
14. Tax Identification Number, SSS number or GSIS number; and
15. **In case where the applicant is acting in a representative capacity:** the legal capacity of the customer and the identity of the principal owner or beneficiary, including information from numbers 1 to 14; and
16. **If the customer is a legal entity such as a corporation:** the identity of the person authorized, including information from numbers 1 to 9.

FLMBAI shall obtain from the customer prior to the opening of the account: (1) notarized special authorizations, for the representatives; and (2) trust agreement, if acting as a trustee.

For individual clients: The original copy of the identification documents such as Philippine passport or driver's license or any official identity card issued by the Philippine government shall be required.

PROHIBITED ACCOUNTS

FLMBAI shall maintain accounts only in the true and full name of the account holder. It shall not open or keep anonymous accounts, fictitious name accounts, incorrect name accounts and all other similar accounts. FLMBAI shall refuse opening of accounts under any of the following circumstances:

1. Anonymous accounts;
2. Fictitious names accounts;
3. Incorrect name accounts; or
4. Customer fails to provide the requested evidence of identity.

LEGAL ARRANGEMENTS

FLMBAI shall identify and verify the identity of the beneficial owners through the following information:

1. For trusts: the identity of the settlor, the trustee/s, the protector, the beneficiaries and other natural person exercising ultimate effective control over the trust; or
2. The identity of persons in equivalent or similar positions.

NEW TECHNOLOGIES

FLMBAI shall conduct ML/TF risk assessment prior to the introduction of a new product, new business practice or new technology for both new and pre-existing products. The outcome of such product shall be documented and be available to the IC upon request during compliance checking.

RENEWAL OF CLIENT'S IDENTIFICATION

FLMBAI shall provide complete and accurate customer's information and shall regularly update customer identification information at least once every two (2) years whenever there are changes on the customer's information; where there are doubts as to the identity of the client, beneficial owner or the principal that it represents; and whenever necessary pursuant to FLMBAI's established policies.

SIMPLIFIED/REDUCED CUSTOMER DUE DILIGENCE

FLMBAI may opt to apply reduced or simplified CDD in the case of low risk customers which includes:

1. Financial institutions subject to requirements to combat money laundering and the financing of terrorism pursuant to Financial Action Task Force (FATF) Recommendations;

2. Public companies that are subject to regulatory disclosure requirements; and
3. Government institutions and their instrumentalities.

C. RISK MITIGATION

VERIFICATION WITHOUT FACE-TO-FACE CONTACT

1. Whenever possible, FLMBAI shall interview prospective clients personally.
2. FLMBAI shall allow the opening of accounts only through the internet and shall not allow the opening of accounts via postal service or telephone or other such medium which may give rise to verification without face-to-face contact.
3. In accepting business from non-face to face customer, FLMBAI shall use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.
4. FLMBAI shall apply the following number of checks, to verify the identity of prospective clients where there is no face-to-face contact:

    a. Telephone contact with the applicant at an independently verified home or business number;
    b. Subject to the applicant's consent, telephone confirmation of the applicant's employment with the employer's personnel department at a listed business number;
    c. Salary details appearing on recent bank statements, income tax returns or any other document evidencing compensation;
    d. Confirmation of the address through an exchange of correspondence or by any other appropriate method; and
    e. Presentation of other existing insurance policies or contracts issued by other insurance institutions supervised by the Insurance Commission will provide additional comfort.

5. For non-residents who seek to procure insurance in the Philippines, whenever applicable and without face-to-face contact, documents as enumerated above issued by foreign authorities may be submitted, duly authenticated by the Philippine Consulate where such foreign authorities are located.
6. FLMBAI shall require the first payment to be carried out through an account in the customer's name with an insurance company subject to similar CDD standards.
7. No new accounts shall be opened without face-to-face contact unless full compliance with the requirements above is met and the original documents thereof are presented for verification purposes. FLMBAI shall be vigilant in the following transactions: (a) When payment is offered in cash or offered by way share where it is evident that the shares have been held for less than six (6) months; (b) By way of a third-party check without any apparent connection with the prospective client; or (c)

By check where there is variation between the policyholder, the signatory and prospective client.

8. Before establishing a business relationship, FLMBAI shall make a company search and/or other commercial inquiries to ensure that the corporate/other business applicant has not been or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company or its directors, or the business or its partners, FLMBAI shall conduct a research or inquiry with the relevant Supervisory Authority/ Regulatory Agency.

THIRD PARTY RELIANCE- The third party shall be a covered person or a financial institution operating outside the Philippines that is covered by customer identification and face-to-face requirements as defined under the AMLA, as amended.

Where reliance on intermediaries and third parties is permitted, FLMBAI shall take adequate steps to:

1. Perform customer identification and face-to-face contact and other relevant documentation relating to the CDD requirements;
2. Identify the customer and verify the customer's identity using reliable, independent source documents, data or information relating to the CDD requirements and which are made available from the intermediaries/third party upon request without delay;
3. Regulate and supervise the intermediaries and third to ensure that they comply with CDD requirements;
4. Ensure that the customer identification program of the intermediaries and third parties is similar to FLMBAI's customer identification program; and
5. Be ultimately responsible for customer and/or beneficial owner identification and verification.

CORPORATE ACCOUNTS – before establishing a business relationship, FLMBAI shall make a company research or inquiries to ensure that the corporate/business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated.

TRUST, NOMINEE, AGENT AND FIDUCIARY ACCOUNTS

FLMBAI shall establish and record the true and full identity and existence of both: (1) the trustee, nominee, agent, or intermediary; (2) authorized signatories and the nature of their trustees or nominee capacity and duties; and (3) the trustor, principal, or beneficial owner or person on whose behalf the account/business relationship/transaction is being opened or conducted.

In cases where FLMBAI have doubts as to whether the trustee, nominee or agent is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence (EDD) and shall file STR, if warranted, to verify business relationship between the parties.

Where satisfactory evidence of the beneficial owners cannot be obtained, FLMBAI shall not continue its transactions with the client concern and shall record the particular undertaking and shall continue to monitor said account of the client. This action warrants the reporting of STR to the AMLC without further delay. FLMBAI shall also conduct reasonable inquiries whenever the transactions shall pass through accounts opened by a law firm or accountants.

HIGH-RISK CUSTOMERS

FLMBAI relying on third persons, shall conduct EDD procedures under the following circumstances:

1. Where the business relationships and transactions with persons including companies and financial institutions from other countries, do not insufficiently apply FATF Recommendations; or
2. When establishing source of wealth of higher risk customers.

FLMBAI's senior management shall undertake the decisions on business relations with higher risk customers.

SHELL COMPANIES

Shell companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted. FLMBAI shall consider that shell companies may be abused by money launderers and therefore shall be cautious in its dealings with them.

ENHANCED DUE DILIGENCE (EDD)

Higher-risk customers will require the application of EDD to verify customer identity. If the relationship is complex, or if the size of the account is significant, additional identification measures may be advisable, and these should be determined based on the level of overall risk. However, if FLMBAI has any reason to believe that a customer has been refused application by another HMO due to concerns over illicit activities of the customer, it should consider classifying that customer as a higher-risk and apply enhanced due diligence procedures to the customer and the relationship, and not accepting the customer in accordance with its own risk assessments and procedures.

The following information warrants the filling of Suspicious Transaction Report (STR):

1. Raises doubt as to the accuracy of any information or document provided by the customer or the ownership of the entity;
2. The customer is transacting without any purpose, economic justification or underlying legal or trade obligation;
3. The customer might have structured transactions to avoid being the subject of Covered Transaction Report;
4. The customer has been or is currently engaged in any unlawful activity; or
5. Raises suspicions that an intermediary is being used to circumvent anti-money laundering compliance measures.

D. CUSTOMER'S DOCUMENTATION

FLMBAI shall prepare and maintain documentation on its customer relationships and transactions such that:

1. Requirements of the AMLA are fully met; and
2. Any transaction effected directly by FLMBAI or thru a broker or agent can be reconstructed and from which the AMLC will be able to conduct an audit trail for suspected money laundering for such report.

FLMBAI shall comply within a reasonable time to any inquiry or order from the AMLC as to the disclosure of information, including without limitation whether a particular person is the customer or beneficial owner of transactions through FLMBAI.

RECORD KEEPING

FLMBAI shall maintain documentation with retention periods of the following:

1. All customers records and transaction documents shall be retained in their original and certified copies with the name of the employee certifying the same or in such forms as are admissible in court, pursuant to existing laws promulgated by the Supreme Court, the Revised Rules of Court and the E-Commerce Act and its implementing rules and regulations;
   In cases where the original copies of the documents cannot be produced or the certified copies cannot be retained, FLMBAI shall record the reasons for their non-production.
2. All customer relationships, identification and other pertinent data and transaction records shall be maintained in such time, sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution for money laundering, unlawful activity and terrorism financing;
3. FLMBAI shall provide customer's documentation which will enable the AMLC to compile an audit trail should there be a report made pursuant thereto;

4. All CDD information and transaction records shall be available swiftly to the IC, AMLC and other competent authorities in the exercise of their official functions or upon appropriate authority;
5. All customers records and transaction documents shall be maintained and safely stored for five (5) years from the dates of transactions. Should a case have been filed in court involving the account, records must be retained and safely kept beyond the five-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality;
6. All records obtained through CDD, account files and business correspondence, and the results of any analysis undertaken shall be kept for at least five (5) years following the closure of account, termination of the business relationship or after the date of the occasional transaction;
7. All electronic copies of all covered and suspicious transaction reports and the complete file on all transactions brought to the attention of the Compliance Officer and those not reported to the AMLC shall also be kept for at least five (5) years from the dates of submission to the AMLC;
8. All records concerning its internal reporting of covered and suspicious transaction reports and decision making whether to file or not to file said reports with the AMLC, shall be maintained for at least five (5) years following the date of transaction;
9. All customer records and transaction documents including recordings and analysis made to detect unusual or suspicious transactions shall be made available to IC and to AMLC for inspection;
10. FLMBAI shall have automatic back-up system which is maintained for at least five (5) years following the date of transaction; and
11. FLMBAI shall designate an officer to be responsible and accountable for all record keeping requirements of its customers identification and transaction documents readily available without delay to the IC and AMLC during compliance checking or investigation.

Per record of transactions, FLMBAI shall follow the following procedures:

1. To access initial proposal documentation including identity, address or other identifying information, the client financial assessment, client needs analysis, copy of regulatory documentation, details of the payment method, and illustration of benefit in support of verification by FLMBAI;
2. To access all post-sale records associated with the contract through its maturity; and
3. To access details of maturity processing and/or claims settlement, which include completed “discharge documentation”.

FLMBAI ’s documentation shall include the following:

1. Customer/beneficiary’s name and address;
2. Nature and date of transaction;
3. Transaction serial number;

4. Type and amount of currency involved;
5. Type and identifying number of account;
6. Other information regarding the customer or beneficial owner;
7. Date and time of receiving by FLMBAI from customer or other persons purporting to act on their behalf, if any;
8. Instructions details including method of delivery and receipt, if any;
9. Identification cards or passport numbers, telephone numbers and addresses of the customers or persons acting on their behalf, whether locally or abroad;
10. Bank accounts involved, if any; and
11. Date and time of delivery and receipt number, if any.

The provision of any rule, regulation or law to the contrary notwithstanding if the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the disputed retention period until it is confirmed that the case has been closed.

ACCESS TO DATA

FLMBAI shall ensure that there are no secrecy or data protection issues that would restrict prompt access:

(a) to data, or impede the full application of the Guidelines with respect to any outsourced relationship; and
(b) at all time by the IC and AMLC, whether for compliance checking or investigation, to the records of customer identification and transaction documents or impede the full application of this Guidelines.

IV. MONITORING AND MANAGEMENT INFORMATION SYSTEM

FLMBAI shall have MLD System of mandatory reporting of covered transactions and suspicious transactions which includes:

A. Monitoring of Business Relationships and Transactions involving:

1. Trust, nominee and fiduciary accounts;
2. Shell companies which have been allowed to transact after undertaking necessary verifications;
3. Complex, unusual large transactions or unusual patterns of transactions;
4. Persons (juridical or natural) from countries which do not or insufficiently apply the FATF Recommendations;
5. Transactions which are suspected to be made by a person included in the list of suspected terrorists or terrorist organizations that may be furnished by the AMLC

or any other law enforcement agency or pursuant to internal policies and procedures;

6. Transactions made by persons, whether individual or corporate, who had been subjected to further verifications but nonetheless required to be monitored by the covered institution as part of AMLA compliance procedure; and
7. Any other transaction which may deem necessary to be monitored based on surrounding facts or circumstances and FLMBAI's established policies and procedures.

B. Ongoing Monitoring

Ongoing monitoring is conducted in relation to all business relationships and transactions, but the extent of the monitoring should be based on risk as identified in the company's risk assessment and its CDD efforts. Enhanced monitoring should be adopted for higher-risk customers or transactions. FLMBAI should also carry out cross-sectional product/service monitoring in order to identify and mitigate emerging risk patterns.

C. Monitoring Tools and Controls

FLMBAI should have monitoring systems such as CIM system and MLD system in place to detect unusual or suspicious transactions or patterns of activity connected with money laundering. In identifying such activity, FLMBAI should consider the customer's risk profile, customer's category, group of accounts, transaction pattern or product usage developed as a result of the risk assessment; the information collected during its CDD efforts, and other information obtained from law enforcement and other authorities in its jurisdiction. By using CDD information, FLMBAI should be able to identify transactions that do not appear to make economic sense or those that involve large cash, not consistent with the customer's normal and expected transactions.

D. Management Information System

FLMBAI should ensure that they have appropriate Customer Identity Management System (CIM System) commensurate with its size, organizational structure or complexity, based on materiality and risks. It shall provide both business units and risk and compliance officers (including investigating staff) with timely information needed to identify, analyze and effectively monitor customer accounts. The systems used and the information available should support the monitoring of such customer relationships across lines of business and shall include all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer's behavior or business profile and transactions made through a customer account that are unusual.

E. Screening of Customer's Database/s

FLMBAI shall screen its customer database(s) periodically whenever there are changes to sanction lists and to detect PEPs and other higher-risk accounts and shall subject them to enhanced due diligence.

F. Reporting of Suspicious Transactions

The ongoing monitoring and review of accounts and transactions will enable FLMBAI to identify suspicious activity, eliminate false positives and report promptly genuine suspicious transactions. The obligation to make the covered and/or suspicious transaction report to the AMLC is on the employee, officer and/or director of FLMBAI. Such reporting shall be done within ten (10) working days after initial detection of facts that may constitute a basis for filing such reports.

When reporting covered or suspicious transactions to the AMLC, FLMBAI and its officers and employees are prohibited from communicating directly or indirectly, in any manner or by any means, to any person, entity, or to the media, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. Neither may such reporting be published or aired in any manner in form by the mass media, electronic mail o other similar devices. In case of violation thereof, the concerned officer and employees of the FLMBAI and the media shall be held criminally liable.

G. FLMBAI's AML/CFT Operating Manual

The process for identifying, investigating and reporting suspicious transactions are clearly set out in the Operating Manual and communicated to all personnel through regular training. The policies and procedures shall contain a clear description for employees of their obligations and instructions for the analysis, investigation and reporting of such activity.

H. Review of Risk Classification of the Customer and/or the Account

Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity and cooperating with law enforcement agencies, FLMBAI shall warrant that appropriate action is to be taken to adequately mitigate the risk of the company being used for criminal activities.

Where any employee or personnel, director or officer of FLMBAI knows that the client has engaged in any of the unlawful activities under the AMLA, the matter shall be promptly reported to the Compliance Officer who, in turn, shall immediately report the details to the AMLC.

I. Disclosure of Suspicious and/or Covered Transactions

When FLMBAI is required to disclose to an authorized officer knowledge, suspicion or belief that any fund, property or investment is derived from or used in any criminal conduct under the AMLA or any matter on which such knowledge, suspicion or belief is based, such disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by imposed by law, contract or rules of professional conduct.

Furthermore, no administrative, criminal or civil proceedings shall lie against any person for having made a suspicious transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law.

FLMBAI and its directors and employees shall not be liable for any loss, arising out of such disclosure, or any act or omission, in relation to the fund, property or investment in consequence of the disclosure, where such is made in good faith and in the regular performance of their duties under the AMLA.

V. ML/TF PREVENTION PROGRAM

FLMBAI shall adopt the following guidelines in compliance with ML/TF Prevention Program:

A. COMPLIANCE OFFICE

FLMBAI shall have a Compliance Office to be headed by the Compliance Officer. To ensure the independence of the office, it shall have a direct reporting line to the board of directors on all matters related to AML and CFT compliance and their risk management. It shall be principally responsible for the following functions, among other functions that may be delegated by senior management and the board:

1. Ensure compliance by all responsible officers and employees with the Guidelines, the AML and CFT laws and other issuances from the IC and the AMLC and the ML/TF Prevention Program;
2. Ensure that infractions, discovered either by internal audits or by compliance checking conducted by IC or AMLC are immediately corrected;
3. Alert senior management and the board if it believes that FLMBAI is failing to appropriately address AML/CFT issues; and
4. Organize the timing and content of AML/CFT training of officers and employees including regular refresher trainings.

The Compliance Officer who shall head the Compliance Office shall possess the following qualifications:

1. of senior management status, who is in-charge of advising the management and staff on the issuance and enforcement of in-house instructions regarding AMLA, as amended, the Operating Manual, personnel training, and reporting of covered and suspicious transaction and other updates to the compliance measures; and
2. who is well-versed in different types of transactions concerning relevant aspects of the AML, its IRR and international standards.

The Compliance Officer shall perform the following functions/duties:

1. Conduct periodic compliance checking and the evaluation of existing processes and policies including on-going prevention, reporting channels, effectiveness of AML/CFT transaction monitoring system and record retention system through sample testing;
2. Act as liaison officer between FLMBAI and the AMLC in matters relative to compliance with AMLA; and
3. Prepare and submit to the AMLC written reports of the FLMBAI's compliance with AMLA, its Guidelines and its IRR.

   FLMBAI shall also designate another officer to be responsible for all the record keeping requirements under the Guidelines. He shall be responsible for making records of customer identification and transaction documents readily available without delay to the IC and AMLC during compliance checking investigation.

B. BOARD AND SENIOR MANAGEMENT OVERSIGHT

The FLMBAI's Board of Directors is responsible for ensuring compliance with the Guidelines, the AML and CFT laws, their IRRs and other issuances from the IC and AMLC. Senior management shall oversee the day-to-day management of FLMBAI, ensure effective implementation of the AML/CFT policies approved by the board and shall establish a management structure to promote accountability and transparency and upholds checks and balances.

C. RISK MANAGEMENT POLICIES

To combat money laundering and financing of terrorism, FLMBAI shall strictly carry out the following policies:

1. **Updating of information-** FLMBAI shall ensure that the records of its customers remain accurate and up-to-date by conducting regular reviews of existing records and updating the CDD information and shall effectively monitors the accounts for unusual or suspicious activities;

2. **Supplying information to the supervisors –** the employees shall demonstrate to its supervisors and management:
   a. the adequacy of the assessment, management and mitigation of ML/FT risks;
   b. the customer acceptance policy;
   c. the procedures and policies concerning customer identification and verification; and
   d. the ongoing monitoring and reporting of suspicious transactions; and all measures taken in the context of AML/CFT.
3. **"Know Your Customer Principle"-** FLMBAI shall institute effective procedures for obtaining the true identification of its customers. FLMBAI shall not keep anonymous account/s in obviously fictitious names and shall properly identify and record the true identity of its clients applying for health insurance coverage.
4. **Customer Identification and Customer Due Diligence (CDD)** measures depend on the risk attached to a type of customer or transaction. FLMBAI may opt to apply reduced or simplified CDD in the case of low risk customers. The Financial Action Task Force (FATF) Recommendations require additional diligence measures in relation to politically exposed persons (PEPs). For this purpose, FLMBAI must take appropriate risk management measure to determine whether the customer is a PEP.

D. EMPLOYEE TRAINING PROGRAM

FLMBAI shall provide education and training for all its staff and personnel, including directors and officers to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and the financing of terrorism and to be familiar with its system of reporting and investigating suspicious matters which shall include the following:

1. **New Staff -** The training shall be conducted to all new employees, regardless of level of seniority, which includes the general appreciation of the background to money laundering, the need to be able to identify suspicious transaction and report such transactions to the appropriate designated Compliance Officer.
2. **Advisory Staff -** A continuous training shall also be provided to cashiers/dealers representatives or investment representatives/advisory staff or front-line staff on matters regarding identification of suspicious transactions, procedures to be adopted when a transaction is deemed suspicious and the policy dealing with non-regular customers or when large case transactions or complex transaction are involved.

   Members of the staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the strategy in the fight against money laundering. Training are provided on areas that may give rise to suspicious and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that front-line personnel are

made aware of the policies for dealing with non-regular customers particularly where large cash transactions are involved and the need for extra vigilance in cases under suspicious circumstances.

3. **Processing Staff -** Members of the staff who receive completed proposals and checks for payment of the single premium contribution will receive appropriate training in the processing and verification procedures. The identification of the proposer and the matching against the check received in settlement are, for instance, key processes. Such staff are made aware that the offer of suspicious funds accompanying requests to undertake an insurance contract may need to be reported to relevant authorities irrespective of whether or not funds are accepted.
4. **Administrative/Operations Supervisors and Managers-** A higher level of instruction covering all aspects of money laundering procedure are provided to those with the responsibility of managing staff. This will include the acts or omissions punishable under the Act and the penalties therefore, procedures relating to service of production, freeze orders and inquiries, other processes allowed under the Act as well as the requirement for the retention of records.
5. **On-going/ Refresher Training -** FLMBAI shall provide for refresher trainings to review updates to compliance measures as they arise from new legislation, IC and/or AMLC issuances, internal audit findings and discoveries in ML/TF trends and detection techniques. A twelve or six-monthly review of training or alternatively a review of the instructions for recognizing and reporting suspicious money laundering transactions can be considered for the purpose. The employees training regarding AML/CFT shall be conducted annually for three (3) consecutive days within the premises of FLMBAI pursuant to the Guidelines under the AMLA, as amended. The annual record of AML/CFT training program and seminars shall be kept and submitted to the compliance officer and should be made available during IC's compliance checking.

   The scope of training shall include but is not limited to the following:

   1. Provisions of the AMLA and its IRR and its amendments;
   2. The company's AML/ CFT Operating Manual and its amendments;
   3. The company's internal supervision, control and compliance procedures and its amendments;
   4. Updates on PSE/SEC/IC Regulations;
   6. Customer identification process;
   7. Record keeping requirements;
   8. Covered and suspicious transaction reporting; and
   9. Internal processes/chain of command for reporting and cooperation with the IC.

VI. REPORTING OF COVERED AND SUSPICIOUS TRANSACTIONS

FLMBAI shall adopt the following rules in reporting suspicious and covered transactions:

A. FLMBAI shall have a Money Laundering Detection System (MLD System) of mandatory reporting of both covered and suspicious transactions and for ensuring the confidentiality of the reports made to the AMLC.
B. FLMBAI shall report all covered and suspicious transactions to the AMLC within five (5) working days from occurrence thereof, unless the AMLC prescribes a different period not exceeding fifteen (15) days, when the total amount of the premiums/fees for a policy, plan or agreement for the entire year, regardless of the frequency of payment, exceeds Five Hundred Thousand pesos (Php 500, 000.00) within one (1) banking day, notwithstanding the amounts of the amortizations are less than the threshold amount.
C. All covered transactions (CTRs) shall be reported upon payment of the first premium/fee amount, regardless of the frequency of payment and shall be filed only once every year until the policy, plan or agreement matures or rescinded, whichever comes first.
D. When the transaction is any way related to an unlawful activity, or the person transacting is involved in or connected to an unlawful activity or money laundering offense, the ten (10) calendar day shall be reckoned from the date the company knew of, or should have known, the suspicious transaction indicator.
E. In order to facilitate ongoing monitoring of a customer's transaction, FLMBAI shall take note or record instances where a transaction is initially flagged as potentially suspicious, even if does not ultimately report the transactions through an STR.
F. FLMBAI shall guarantee the accuracy and completeness of CTR and STR report, which shall be filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.
G. FLMBAI shall institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there is evidence for him/her to do so and shall monitor indicators of suspicious activities and perform EDD as necessary.
H. FLMBAI shall report to the AMLC transactions, regardless of the amounts involved, where any of the following circumstances exists:

    1. There is no underlying legal or trade obligation, purpose or economic jurisdiction;
    2. The client is not properly identified;
    3. The amount involved is not commensurate with the business or financial capacity of the client;
    4. The client's transaction is structured in order to avoid being the subject or reporting requirements under AMLA, as amended;
    5. Any circumstances relating to the transaction which is observed to deviate from the profile of the clients and/or past transactions with FLMBAI; or
    6. The transaction is in any way related to an unlawful activity or offense under the AMLA, as amended, that is about to be, is being or has been committed.

GUIDELINES IN REPORTING SUSPICIOUS TRANSACTIONS

1. The employee shall immediately report to the Compliance Officer any suspicion or knowledge of ML or TF activity and/or transaction that is identified or detected subject to the policies and procedures embodied in the Manual.
2. The Compliance Officer shall:

    a. investigate STR internally and examine the background and purpose of the activity in question and the findings may be established in writing;
    b. build an internal report outlining the outcome of his investigation including the decision on whether or not to file an STR; and
    c. promptly file an STR with the AMLC should he believes or has reasonable grounds to believe that funds concerning an actual or proposed transaction are the proceeds of any criminal activity or are related to ML/TF.
3. All suspicious transactions (STRs) shall be reported upon occurrence or the date of determination of the suspicious nature of the transaction, which determination shall not exceed ten (10) calendar days. Should a transaction be determined to be both a CTR and STR, it shall be reported ad a suspicious transaction.
4. FLMBAI shall be given a period not exceeding sixty (60) calendar days to gather facts in order to enable the submission of meaningful STR.

INDICATORS OF SUSPICIOUS TRANSACTIONS

FLMBAI shall file a STR before the AMLC where any of the following circumstances occur:

1. A request by the customer to enter into insurance contract/s, pre-need plan/s or HMO agreement/s where the source of the fund is unclear or not consistent with the customer's apparent standing;
2. A sudden request for a significant purchase of a lump sum contract with an existing customer whose current contracts are small and of regular payments only;
3. A proposal which has no discernible purpose and reluctance to divulge a "need" for making investment;
4. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer;
5. Any unusual financial activity of the customer in the context of his usual activities;
6. Any usual transaction in the course of some financial activity;
7. Any unusually-linked transaction;
8. Any unusual or disadvantageous early redemption of an insurance policy;

9. Any unusual employment of an intermediary in the course of some usual transactions or formal activity e.g. payment of claims of high commission to an unusual intermediary; or
10. Any unusual method of payment.

ELECTRONIC MONITORING SYSTEMS FOR AML/CFT

FLMBAI shall have MLD System which has the following automated functionalities:

1. Covered and suspicious transactions - performs statistical analysis, profiling and able to detect unusual patterns of account activity;
2. Watch list monitoring - checks transfer parties and the existing customer database for any listed undesirable individual or corporation;
3. Investigation - checks for given names throughout the history of payment stored in the system;
4. Can generate all the CTRs accurately and completely with all the mandatory field properly filled up;
5. Must provide a complete audit trail;
6. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes, and
7. Has the capability to record all STRs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

CONFIDENTIALITY OF REPORT

FLMBAI and its directors, officers and employees, when reporting covered or suspicious transactions, shall be prohibited from communicating directly or indirectly, in any manner or by any means, to any person or entity or the media, the fact that a covered or suspicious transaction has been or is about to be reported, the contents of the report or any other information in relation thereto.

Any information about such reporting to the AMLC shall not be communicated to the concerned customer nor published or aired, in any manner or form by the mass media or through electronic mail, or other similar devices. In case of violation thereof, the concerned officer and employee and media shall be held criminally liable.

ELECTRONIC SUBMISSION OF REPORTS

The CTR and STR shall be submitted to the AMLC in a secured manner, in electronic form and in accordance with the Guidelines. FLMBAI shall provide complete and accurate information of the report and shall regularly update customer identification information at least once every two (2) years. Only the respective Compliance Officer or duly authorized officers shall electronically sign the STR and CTR. Electronic copies of CTRs

and STRs shall be preserved and safely stored for at least five (5) years from the dates the same were reported to the AMLC.

DEPARTMENTAL PROCEDURE ON REPORTING CTR/STR

CASH MANAGEMENT/ACCOUNTING DEPARTMENT

The department is responsible for the collection of premium and non-premium payments and ensures that the collection is properly turned-over to the FLMBAI's depository bank. The disbursement function of the department is limited to payment of commission to authorized and licensed agents and petty cash expense incurred by all extension offices.

The Cash Management Department shall adopt the following procedures to detect AML/CFT within the company:

1. Extracts daily collection report from all extension offices using the MLD System;
2. Identify transactions involving payments of over Php 500, 000.00 from a single person/transaction within one (1) day;
3. Accomplish the AMLA CTR/STR Reporting Electronic Record Format Template.
4. Convert the template into the AMLA required CSV Format for data encryption; and
5. Log-on to AMLA portal to report the transaction.

VII. INTERNAL CONTROLS AND AUDIT PROCEDURES

Internal audit plays an important role in independently evaluating the risk management and controls and discharges its responsibility to the audit committee of the board of directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures. FLMBAI shall guarantee that the audit scope and methodology are appropriate for the company's risk profile and that the frequency of such audits is also based on risk.

Internal Control & Audit Guidelines to Prevent Money-Laundering:

1. FLMBAI shall establish and implement internal control procedures aimed at preventing and combating money laundering within the company;
2. It shall ensure that its officers and employees are aware such procedures pursuant to the provisions of the law, its implementing rules and regulations as well as all reportorial and compliance control and procedures that shall be established by the Council, the Supervising Authority and the company;
3. The internal policies and procedures dealing with money laundering and in addressing identified risks are clearly set out and reflected in the Operating Manual;

4. The effectiveness of compliance oversight and quality control including parameters of criteria for automatic alerts;
5. Conducting company's training of relevant personnel;
6. Issuing a clear statement of policies in relation to money laundering and adopting the current regulatory requirements which shall be communicated in writing to all management and relevant staff whether in branches and be reviewed in a regular basis;
7. FLMBAI shall institute an audit function or procedure to test the electronic monitoring system to ensure adequate compliance with the program; and
8. It shall have an adequate screening procedure to ensure high standards in hiring employees.

Written Internal Reporting Procedures:

FLMBAI shall inform all its directors, officers, employees, and all key staff to whom they should report any knowledge or suspicion of money laundering activity and shall:

1. Ensure that there is a clear reporting chain under which suspicions of money laundering activity will be passed to the Compliance Officer, in accordance with the reporting procedures;
2. Require the Compliance Officer to consider any report in the light of all relevant information which may be of assistance in the determination as to whether or not suspicious transaction is to be filed. The Compliance Officer shall have access to any information which may be necessary in determining whether or not a suspicious transaction report is to be filed;
3. Promptly disclosed to the AMLC, the information contained in the STR; and
4. Maintain a record of all reports made to the AMLC and all reports relative to covered and suspicious transactions reported to the Compliance Officer but were not reported to the AMLC. Said record shall contain details on the date on which the report is made, the person who made the report and information sufficient to identify relevant papers related to the reports.

APPENDIX A: Example Products and Transactions Risk Ratings

This will serve as a sample to illustrate the risk assessment methodology to be generated by the **Money Laundering Detection System** (**MLD System).** FLMBAI shall fully document the approach for arriving at risk ratings within the risk assessment methodology. The examples provided are neither exhaustive nor binding.

Product Risk	Rating
Basic Life Insurance	Low/Moderate

Transaction Risk	Rating
Unusual/ Suspicious Transactions	Moderate
Suspected Shell Company Transactions	High

APPENDIX B: Example Channel Risk Ratings

This will serve as a sample to illustrate the risk assessment methodology to be generated by the **SAS Software.** FLMBAI shall fully document the approach for arriving at risk ratings within the risk assessment methodology. The examples provided are neither exhaustive nor binding.

Channel Risk	Rating
Account Verification	
- Face-to-face	Low
- Non- face-to-face via intermediary	Moderate
- Non- face-to-face (mail/phone)	High

APPENDIX C: Example Customer Risk Ratings

This will serve as a sample to illustrate the risk assessment methodology to be generated by the **Customer Identity Management System (CIM System).** FLMBAI shall fully document the approach for arriving at risk ratings within the risk assessment methodology. The examples provided are neither exhaustive nor binding.

Customer Risk	Rating
Individuals	Low
Entities (Government/Private)	Moderate
Politically Exposed Person (PEP)	High