FIRST METRO ASSET MANAGEMENT INC.

MONEY LAUNDERING AND TERRORIST PREVENTION PROGRAM (MLPP)

Updated as of July 2017

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

I. DECLARATION OF POLICY

FAMI adopts this policy of the State under RA No. 10167 and 10168, otherwise known as AMLA, as amended and the Terrorism Financing Prevention and Suppression Act, also referred to as TF Suppression Act to protect the integrity and confidentiality of its accounts and to ensure that the Philippines in general and this institution shall not be used respectively as a money laundering site and conduit for the proceeds of an unlawful activity as hereto defined. FAMI further supports the State's policy to protect the life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it and reinforce the fight against terrorism by criminalizing the financing of terrorism and related offenses.

II. SCOPE

This Manual shall apply to FAMI and its Mutual Funds, its existing/future branches, including subsidiaries and affiliates supervised and regulated by the SEC under existing regulation. The scope of the money laundering prevention program shall also extend to combating terrorist financing.

Whenever local applicable laws and regulations of a branch, office, subsidiary or affiliate based outside the Philippines prohibit the implementation of these Rules or any of the provisions of the AMLA, as amended, its RIRR; and the supervising authority in that foreign country issued a directive forbidding said branch, office, subsidiary or affiliate, the Covered Person shall formally notify the BSP and the SEC of this situation and furnish a copy of the applicable rules and/or regulations or the supervising authority's directive, as the case may be; and apply appropriate additional measures or mitigating controls to manage the money laundering (ML) and terrorist financing (TF) risks.

III. DEFINITION OF TERMS AND ABBREVIATIONS - Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the AMLA, as amended, Republic Act (RA) No. 10167 and the Terrorism Financing Prevention and Suppression Act of 2012 (RA 10168) and its respective RIRR.

A. Anti-Money Laundering Terminologies

1. AMLA – Anti-Money Laundering Act, or R.A. 9160, as amended
2. RIRR – Revised Implementing Rules and Regulations
3. MLPP or the Manual – Money Laundering and Terrorist Financing Prevention Program
4. AMLC – Anti-Money Laundering Council
5. AML/CFT – Anti-Money Laundering/Combating Financing of Terrorism
6. KYC – Know Your Customer/Client
7. CDD – Customer Due Diligence
8. RDD – Reduced Due Diligence
9. EDD – Enhanced Due Diligence

10. CAF – Client Assessment Form
11. KYCRF – Know Your Customer Reliance Form
12. PEP – Politically Exposed Person
13. BSP – Bangko Sentral ng Pilipinas
14. FATF – Financial Action Task Force
15. SEC – Securities and Exchange Commission
16. AJF – Alert Justification Form
17. CSF – Client Suitability Form

B. **Anti-Money Laundering Council (AMLC)** - refers to the Council created by virtue of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001, as amended" (AMLA, as amended);

C. **Anti-Terrorism Council (ATC**) - refers to the Council created by virtue of Republic Act no. 9372, otherwise known as the "Human Security Act" (HSA) of 2007;

D. **Covered Person**, natural or juridical, refer to:

(1) banks, non-banks, quasi-banks, trust entities, non-stock savings and loan associations, foreign exchange dealers, pawnshops, money changers, remittance and transfer companies, electronic money issuers and other financial institutions which under special laws supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), including their subsidiaries and affiliates. For this purpose, a Subsidiary is an entity more than 50% of its outstanding voting stock is owned by a covered person, while an Affiliate is an entity, the voting stock of which at least 20% but not more than 50% is owned by a covered person.
(2) insurance companies, pre-need companies and all other persons supervised or regulated by the Insurance Commission (IC);
(3) (i) securities dealers, brokers, salesmen, investment houses and other similar persons managing securities or rendering services as investment agent, advisor, or consultant, (ii) mutual funds, close-end investment companies, common trust funds, and other similar persons, and (iii) other entities administering or otherwise dealing in currency, commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or property supervised or regulated by the Securities and Exchange Commission (SEC);
(4) jewelry dealers in precious metals, who, as a business, trade in precious metals, for transactions in excess of One million pesos (P1,000,000.00);
(5) jewelry dealers in precious stones, who, as a business, trade in precious stones, for transactions in excess of One million pesos (P1,000,000.00);
(6) company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; and
(7) persons who provide any of the following services:

(i) managing of client money, securities or other assets;
(ii) management of bank, savings or securities accounts;
(iii) organization of contributions for the creation, operation or management of companies; and
(iv) creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

Notwithstanding the foregoing, the term 'covered persons' shall exclude lawyers and accountants acting as independent legal professionals in relation to information concerning their clients or where disclosure of information would compromise client confidences or the attorney-client relationship: Provided, That these lawyers and accountants are authorized to practice in the Philippines and shall continue to be subject to the provisions of their respective codes of conduct and/or professional responsibility or any of its amendments.

E. **Money Laundering** – is committed by 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 paragraphs (a), (b) or (c) above;
   e. aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (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 paragraphs (a), (b) or (c) above.

   Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required under any of the AMLA provisions, as amended, its RIRR or under this Manual, to be reported to the Anti-Money Laundering Council (AMLC), fails to do so.

   In a broader sense, it is the process of transferring the proceeds of criminal activities into the legitimate mainstream of commerce by concealing their origin. Anyone who conducts a financial transaction with knowledge that the funds are proceeds of an unlawful activity is generally considered to be laundering money.

   Stages of ML

   Generally, the process of money laundering comprises three stages during which there may be numerous transactions that could alert the Company to the money laundering activity:

(a) **Placement** – the physical disposal of cash proceeds derived from illegal activity.

(b) **Layering** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity or to obscure the source of the funds.

(c) **Integration** – the provision of apparent legitimacy to criminally-derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

F. **Financing of terrorism** – 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 unlawful and willful intention that they should be used or with the knowledge that they are to be used in full or in part; 1) to carry out or facilitate the commission of any act of terrorism, 2) by a terrorist organization, association or group; or 3) by an individual terrorist.

G. Dealing, with regard to property or funds" - refers to receiving, acquiring, transacting, representing, concealing, disposing, converting, transferring or moving, using as security or providing financial services.

H. **Designated persons** - refer to:

1. Any person or entity designated as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations Security Council Resolution or by another jurisdiction or supra-national jurisdiction;
2. Any organization, association, or group of persons proscribed pursuant to Section 17 of the HSA of 2007; or
3. Any person, organization, association, or group of persons whose property or funds, based on probable cause are subject to seizure and sequestration under Section 39 of the HSA of 2007.

I. **"Designation" or "Listing"** - refers to the identification of a person, organization, association or group of persons that is subject to targeted financial sanctions pursuant to the applicable United Nations Security Council Resolutions.

J. **Forfeiture** - refers to a court order transferring in favor of the government, after due process, ownership of property or funds representing, involving, or relating to financing of terrorism as defined in Section 4 or an offense under Sections 5, 6, 7, 8, or 9 of the TF Suppression Act.

K. **Freeze** - refers to the blocking or restraining of specific property or funds from being transacted, converted, concealed, moved, or disposed of without affecting the ownership thereof.

L. "**Probable cause**" - refers to a reasonable ground of suspicion supported by circumstances warranting a cautious person to believe that property or funds are in any way related to terrorism financing, acts of terrorism or other violations under the TF Suppression Act.

M. **Terrorist** - refers to any natural person who: (a) commits, or attempts, or conspires to commit terrorist acts by any means, directly or indirectly, unlawfully, and willfully; (b) participates, as a principal, or as an accomplice, in terrorist acts; (c) organizes or directs others to commit terrorist acts; or (d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

N. **Terrorist acts** - refer to the following:
   1. Any act in violation of Section 3 or 4 of the HSA of 2007.
   2. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.
   3. Any act which constitutes an offense that is within the scope of any of the following treaties to which the Republic of the Philippines is a State party:
      a. Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;
      b. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;
      c. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;
      d. International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;
      e. Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980;
      f. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;
      g. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988;
      h. Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988;
      i. International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

O. **Terrorist Organization, Association or Group of Persons** - refers to any entity owned or controlled by any terrorist or group of terrorists that: (1) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (2) participates as an accomplice in terrorist acts; (3) organizes or directs

others to commit terrorist acts; or (4) contributes to the commission of terrorist acts by a group of persons acting with common purpose of furthering the terrorist acts where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

P. **Monetary instrument** refers to:

a. Coins of currency of legal tender of the Philippines, or of any other country;
b. Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property
c. Drafts, checks, and notes;
d. 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.
e. Participation or interest in any non – stock, non – profit corporation
f. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts of deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments;
g. Contracts or policies of insurance, life of non-life, and contracts of surety ship, pre – need plans and member certificates issued by mutual benefit association; and
h. Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

Q. **Transaction** refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a Covered Person.

R. **Covered transaction (CT)** is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of five hundred thousand pesos (P500, 000.00) within one banking day.

S. **Suspicious Transaction (ST)** under Circular 706 and RA 10167 are transactions with Covered Persons, regardless of the amount involved, where any of the following circumstances exist:
1. There is no underlying legal or trade obligation, purpose or economic justification;
2. The client is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the client;
4. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the Act.
5. Any circumstance relating to the transaction which is observed to deviate from

the profile of the client and/or the client'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, is being or has been committed;
7. Any transactions that is similar, identical or analogous to any of the foregoing.
8. Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as suspicious transaction.

Suspicious Transaction defined under RA 10168 – refers to a transaction with a Covered Person, regardless of the amount involved that is, in any way, related to terrorism financing or terrorist acts. It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or groups of persons. In determining whether a transaction is suspicious, Covered Persons should consider the following circumstances:

1. Wire transfers between accounts, without visible legal, economic or business purpose, especially if the wire transfers are effected through countries which are identified or connected with terrorist activities;
2. Sources and/or beneficiaries of wire transfers are citizens of countries which are identified or connected with terrorist activities;
3. Repetitive deposits or withdrawals that cannot be satisfactorily explained or do not make economic or business sense;
4. Value of the transaction is grossly over and above what the client is capable of earning;
5. Client is conducting a transaction that is out of the ordinary for his known business interests;
6. Deposits by individuals who have no known connection or relation with the account holder;
7. Client is receiving remittances from a country where none of his family members is working or residing;
8. Client was reported and/or mentioned in the news to be involved in terrorist activities;
9. Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;
10. Transactions of individuals, companies or Non-Government Organizations (NGOs)/Non-Profit Organizations (NPOs) that are affiliated or related to people suspected of having connection with a terrorist individual, organization, association or group of persons;
11. Transactions of individuals, companies or NGOs/NPOs that are suspected of being used to pay or receive funds from a terrorist individual, organization, association or group of persons;
12. The NGO/NPO does not appear to have expenses normally related to relief or humanitarian efforts;
13. The absence of contributions from donors located within the country of origin of the NGO/NPO;
14. The volume and frequency of transactions of the NGO/NPO are not commensurate with its stated purpose and activity.

T. **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, 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, 301, 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 Nos. 455 and 1937, as amended, of 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; destructive arson and murder, as defined under the Revised Penal Code, as amended, including those perpetrated by terrorists against non-combatant persons and similar targets;
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, and Corruption of Public Officers under Article 212 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 Articles 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, as amended;
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 to 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 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 2002, as amended;
26. Violations 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 of Presidential Decree No. 1612, otherwise known as 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 by Republic Act No. 10022;
29. Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines;
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. Violations of Sections 5, 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. 8799, otherwise known as the Securities Regulation Code of 2000; and
34. Felonies or offenses of a similar nature to 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 said offense or felony need not be identical to any of the unlawful activities listed above.

U. **Proceeds** – refers to an amount derived or realized from any unlawful activity;

V. **Client/Customer** – refers to any person or entity that keeps an account, or otherwise transacts business with a Covered Person and includes the following:
   (1) any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions;
   (2) beneficiary of a trust, an investment fund or a pension fund;
   (3) a company or person whose assets are managed by an asset manager;
   (4) a grantor of a trust and
   (5) any insurance policy holder, whether actual or prospective.

W. **Shell Company**- Legal entities which have no business substance in their own right but through which financial transactions may be conducted.

X. **Shell Bank**- a shell company incorporated as a bank or made to appear to be incorporated as a bank but has no physical presence and no affiliation with a

regulated financial group. It can also be a bank that (1) does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorized to engage; (2) does not employ one or more individuals on a full time basis at this fixed address; (3) does not maintain operating records at this address, and (4) is not subject to inspection by the authority that licensed it to conduct banking activities.

Y. **Beneficial Owner** – refers to natural person(s) who ultimately owns or controls a customer and/or on whose behalf a transaction or activity is being conducted or those who exercise ultimate effective control over a legal person or arrangement. Ultimate effective control refers to a situation in which ownership or control is exercised through actual or a chain of ownership or by means other than direct control.

Z. **Politically Exposed Person or PEP** - an individual who is or has been entrusted with prominent public positions 1) in 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 shall likewise include immediate family members, and close relationships and associates that are reputedly known to have 1.1) joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP or 1.2) sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP.

Immediate family members of PEPs refer to spouse or partner, children and their spouses, and parents and parents – in – law.

Close associates of PEPs are persons 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.

AA. **Correspondent banking** refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank).

BB. **Fund/wire transfer** – refers to any transaction carried out on behalf of an originator (both natural and juridical) through a financial institution (Originating Institution) by electronic means with a view to making an amount of money available to a beneficiary at another financial institution (Beneficiary Institution). The originator person and the beneficiary person may be the same person.

CC. **Cross border transfers** – any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfers that has at least one cross-border element.

DD. **Domestic Transfer** – any wire transfer where the originating and beneficiary institutions are located in the same country. It shall refer to any chain of wire

transfers that takes place entirely within the borders of a single country, even though the system used to effect the fund/wire transfer may be located in another country.

EE. **Originating institution** – refers to the entity utilized by the originator to transfer funds to the beneficiary and can either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (a) but conducts business operations and activities similar to them.

FF. **Beneficiary institution** – refers to the entity that will pay out the money to the beneficiary and can either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (a) but conducts business operations and activities similar to them.

GG. **Intermediary institution** – refers to the entity utilized by the originating and beneficiary institutions where both have no correspondent banking relationship with each other but have established relationship with the intermediary institution. It can be either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (a) but conducts business operations and activities similar to them.

HH. **Monetary instrument or property related to an unlawful activity** refers to (1) All proceeds of an unlawful activity; (2) All monetary, financial or economic means, devices, accounts, documents, papers, items or things used in or having any relation to an unlawful activity;(3) All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds and other similar items for the financing operations, and maintenance of any unlawful activity; and (4) For purposes of freeze order and bank inquiry: related and materially linked accounts.

"*Related accounts*" refer to those accounts, the funds and sources of which originated from and/or are materially linked to the monetary instruments or properties subject of the freeze order or an order of inquiry;

"*Materially – linked accounts* shall include the following:

(1) All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;

(2) All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;

(3) All "In Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

(4) All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry; and
(5) All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing

II. **Payable-through account** – a correspondent account that is used directly by third parties to transact business on their own behalf.

JJ. **Official document –** any of the following identification documents:
(1) For Filipino citizens: Those issued by any of the following official authorities:
a. Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
b Government-Owned or -Controlled Corporations (GOCCs); or
c Covered persons registered with and supervised or regulated by the Bangko Sentral, SEC or lC;
(2) For foreign nationals: Passport or Alien Certificate of Registration
(3) For Filipino Students: School ID signed by the school Principal or Head of the educational institution, and
(4) For Low Risk Clients/Customers: any document or information reduced in writing which the Covered Person deems sufficient to establish the identity of the Client or Customer.

Effects of money laundering:

- It can lead to inexplicable changes in money demand and increased prudential risks for the banking system (economic);
- It can lead to reduced foreign investments if a country's financial system is perceived to be subject to the control of organized crime (security);
- It can destabilize the economies as it infiltrates and corrupts financial, legal and even political institutions (political and economic); and
- It can seriously weaken the moral and ethical standards of society (social).

It is incumbent upon banks and other financial institutions to avoid transactions that will assist criminals in laundering proceeds of their crime. Hence, First Metro Asset Management Inc. (FAMI) and its Mutual Fund companies support the international drive against serious crimes, especially drug trafficking and terrorism. The Company also supports the policy of the State to protect and preserve the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money-laundering site for the proceeds of any unlawful activity.

The Anti-Money Laundering Manual was updated in conformity with the State policy and

consistent with the Revised Implementing Rules of R.A. No. 9160 (as amended) and the Anti-Money Laundering circulars issued by the Securities and Exchange Commission, the AMLC Revised Implementing Rules and Regulations of R.A. No. 9160 and the Bangko Sentral ng Pilipinas (Circular No. 950).

As an integral part of the guidelines on anti-money laundering and as mandated by law and other regulatory bodies like the Securities and Exchange Commission and Anti-Money Laundering Council, the Manual incorporates the following appendices:

Appendix A – Account Opening Folder (Individual)
Appendix B – Account Opening Folder (Corporate)
Appendix C – AMLC Reporting Procedures version 3

IV. BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

A. Know your Customer (KYC)

Satisfactory evidence of the customer's identity shall be obtained. Moreover, effective procedures for verifying the bona fides of new customers shall be implemented. In this regard, the Board of Directors and Senior Management shall ensure that the Company is not used to facilitate money laundering. They shall direct all employees to exercise utmost diligence to ensure that adequate measures are implemented to prevent the Company from being unwittingly involved in such a criminal activity.

B. Compliance with Laws and Regulations

Senior management shall ensure that business is conducted in conformity with the highest ethical standards and those laws, rules and regulations are strictly adhered to. Transactions shall not be allowed where there is good reason to believe that the client is engaged in money laundering activities.

FAMI shall comply fully with these rules and existing laws aimed at combating money laundering and terrorist financing by making sure that officers and employees are aware of their respective responsibilities and carry them out in accordance with superior and principled culture of compliance.

C. Cooperation with Regulatory and Law Enforcement Agencies

The company shall fully cooperate with regulatory and law enforcement agencies within the legal constraints relating to customer confidentiality, particularly on matters relating to the Data Privacy Act. Appropriate measures (e.g., reporting to Anti-Money Laundering Council) shall be taken when there are reasonable grounds for suspecting money laundering.

D. Adoption of Policies and Procedures

Policies consistent with the principles set in the Anti-Money Laundering Law, Implementing Rules and Regulations and Operating Manuals issued by the SEC and AMLC shall be adopted and properly disseminated. Specific control procedures for customer identification, record keeping and retention of transaction documents and reporting of covered and suspicious transactions shall be implemented.

FAMI shall adopt and effectively implement a sound AML and terrorist financing risk management system that identifies, assesses, monitors and controls risks associated with money laundering and terrorist financing.

E. Training on Anti-Money Laundering

All employees shall be provided with adequate training on anti-money laundering law, rules and regulations as well as the policies and procedures established by the Company to ensure awareness and compliance. Training on anti-money-laundering shall be on a regular basis to create awareness in new rules and regulations and to update on the latest trends and techniques applied by money launderers to make them more effective in preventing money laundering activities.

FAMI shall conduct business in conformity with high ethical standards in order to protect its safety and soundness as well as the integrity of the national banking and financial system.

Towards this principle, all employees shall be provided with adequate training on anti-money laundering law, rules and regulations as well as the policies and procedures established by the company to ensure awareness and compliance. Training on AML/CFT shall be on regular basis to create awareness in new rules and regulations and to update on the latest trends and techniques applied by money launderers and terrorist financiers to make them more effective in preventing money laundering/terrorist financing activities.

V. SANCTIONS AND PENALTIES

(a) *Penalties for the Crime of Money Laundering*. The penalty of imprisonment ranging from seven (7) to fourteen (14) years and a fine of not less than Three Million Pesos (Php3,000,000.00) but not more than twice the value of the monetary instrument or property involved in the offense, shall be imposed upon a person convicted under Section 4(a), (b), (c) and (d) of the AMLA, as amended.

The penalty of imprisonment from four (4) to seven (7) years and a fine of not less than One Million Five Hundred Thousand Pesos (Php1,500,000.00) but not more than Three Million Pesos (Php3,000,000.00), shall be imposed upon a person convicted under Section 4(e) and (f) of the AMLA, as amended.

The penalty of imprisonment from six (6) months to four (4) years or a fine of not less than One Hundred Thousand Pesos (Php100,000.00) but not more than Five Hundred

Thousand Pesos (Php500,000.00), or both, shall be imposed on a person convicted under the last paragraph of Section 4 of the AMLA, as amended.

(b) *Penalties for Knowingly Participating in the Commission of Money Laundering* – The penalty of imprisonment ranging from four (4) to seven (7) years and a fine corresponding to not more than two hundred percent (200%) of the value of the monetary instrument or property laundered shall be imposed upon the Company, its Directors, Officers or Personnel who knowingly participated in the commission of the crime of money laundering.

(c) *Penalties for Failure to Keep Records*. The penalty of imprisonment from six (6) months to one (1) year or a fine of not less than One Hundred Thousand Pesos (Php100,000.00) but not more than Five Hundred Thousand Pesos (Php500,000.00), or both, shall be imposed on a person convicted under Section 9(b) of the AMLA.

(d) *Penalties for Malicious Reporting*. Any person who, with malice, or in bad faith, reports or files a completely unwarranted or false information relative to money laundering transaction against any person shall be subject to a penalty of six (6) months to four (4) years imprisonment and a fine of not less than One Hundred Thousand Pesos (Php100, 000.00) but not more than Five Hundred Thousand Pesos (Php500,000.00), at the discretion of the court: Provided, That the offender is not entitled to avail the benefits of the Probation Law.

If the offender is a corporation, association, partnership or any juridical person, the penalty of imprisonment and/or fine shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed by their gross negligence, the commission of the crime and the Court may suspend or revoke its license. If the offender is an alien, he shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties herein prescribed. If the offender is a public official or employee, he shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be. Any public official or employee who is called upon to testify and refuses to do the same or purposely fails to testify shall suffer the same penalties prescribed herein.

(e) *Penalties for Breach of Confidentiality*. The punishment of imprisonment ranging from three (3) to eight (8) years and a fine of not less than Five Hundred Thousand Pesos (Php500,000.00) but not more than One Million Pesos (Php1,000,000.00), shall be imposed on a person convicted for a violation under Section 9(c) of the AMLA.

(g) Imposition of Administrative Sanctions. The imposition of the administrative sanctions shall be without prejudice to the filing of criminal charges against the persons responsible for the violation.

After due notice and hearing, the AMLC shall, at its discretion, impose sanctions, including monetary penalties, warning or reprimand, upon the Company, its Directors, Officers, employees or any other person for the violation of this AMLA, its implementing rules and regulations, or for failure or refusal to comply with AMLC orders, resolutions and other issuances. Such monetary penalties shall be in amounts as may be determined by the AMLC to be appropriate, which shall not be more than Five Hundred Thousand Pesos (P500,000.00) per violation.

The AMLC may promulgate rules on fines and penalties taking into consideration the attendant circumstances, such as the nature and gravity of the violation or irregularity.

(h) The provision of the AMLA shall not be construed or implemented in a manner that will discriminate against certain customer types, such as politically-exposed persons, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny these persons' access to the services provided by the covered persons. Whenever a bank, or quasi-bank, financial institution or whenever any person or entity commits said discriminatory act, the person or persons responsible for such violation shall be subject to sanctions as may be deemed appropriate by their respective regulators.

CHAPTER 2: POLICIES, PROCEDURES AND CONTROLS

A. Customer Acceptance Policies

1. It shall be the policy of the Company to require the **risk-based and tiered policy** for all clients regardless of whether they are small time clients or high net worth individuals;

2. The Company shall also require more extensive due diligence for high risk customers, such as those known in public as controversial personalities, those individuals holding high-profile public position and their associates or companies clearly related with them;

3. In all instances, the Company shall document how a specific customer was profiled (low, normal or high) and what standard of CDD (reduced average or enhanced) was applied;

4. Decisions to enter into business relationships with high risk customers shall be taken exclusively at senior management level;

5. It shall be the policy of the Company not to enter into business relationship with customers who refuse to produce the required identification papers and to discontinue business relationship with customers, who after a series of follow up requests, failed to submit customer identification documents.

6. In designing a customer acceptance policy, the following factors are considered:
    - Background and source of funds;
    - Country of origin and residence or operations;
    - Public/high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory
    - Linked accounts;
    - Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by BSP, AMLC, and Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List
    - Business activities; and
    - Type of services/products/transactions to be entered with the Covered Persons.

B. Classification of Customer and Description

The following are the classification of customers and the corresponding description:

1. Low Risk

a. Individuals who are residents in the area where the office/branch is located
b. Individuals with regular employment
c. Individuals who are employed in the area where the office/branch is located
d. Banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such
e. Publicly listed companies subject to regulatory disclosure requirements
f. Government agencies including government owned and controlled corporations (GOCCs)
g. SEC-registered company
h. Publicly-listed company subject to regulatory disclosure requirements by the SEC/PSE
i. Partnership
j. Association
k. Unincorporated company
l. Company applying for TITF accounts

2. Normal Risk

a. Individual customer or entities not falling under "Low Risk" or "High Risk"
b. Individual or Authorized Signatory (in case of Corporation) who is a Rank and File PEP or PEPs who are no longer in office for the last 5 years or more

3. High Risk

a. Individual/Authorized Signatory (in case of Corporation) who is an **incumbent** Politically Exposed Persons (PEPs):
   i. Local Government Officials: Mayor, Governor, Congressman
   ii. National Government Officials: President, Vice-President and Senators
   iii. Judicial Officials: Justice/Court of Appeals Judge and up
   iv. Uniformed Personnel: Police and Military Officials
   v. Appointive Government Officials: Cabinet Secretary and Undersecretary
   vi. Head of Government Owned or Controlled Corporations
   vii. Leaders of major National Political Parties
   viii. Heads of Foreign States

b. Individuals who present foreign-issued IDs

c. Non-resident Foreigner

d. Overseas Filipino Worker/Immigrant who is not able to provide valid Philippine-issued IDs

e. Client's whose name is found in Watchlist Database as circularized by AMLC, other domestic and international organizations such as, but not limited to, the NBI/FBI/Interpol, OFAC list, UN Sanctions List

f. Cash-intensive businesses, i.e. Foreign Exchange Dealer, Money Changers or Remittance Agents

g. Foundation

h. US Indicia/Citizen

i. Other High Risk Accounts
   i. Dormant and/or Numbered Accounts
   ii. Firm of lawyers or accountants - Account is under the name of Law Firm/Office and Accounting Firm/Office
   iii. Trustee, Nominee, Agent or Intermediary account
   iv. Shell Company/ Shell Bank
   v. Handling of "pooled" funds of entities such as mutual funds, money managers, trusts and foundations, and other professional intermediaries. The Company shall require the customer to disclose the identity/ies of the beneficial owner/s of the funds and those who are in control of the funds invested. Any information gathered shall be verified from trustworthy parties such as banks, reputable law firms'/accounting firms or accessing public or private databases or official sources.
   vi. Wire/Fund Transfers
   vii. High-risk customer - from a country that is recognized as having inadequate internationally accepted anti-money laundering standards under MLPP Chapter III, Section II.E.4

C. Client Assessment Procedures

1. Prior to account opening, all new clients shall be subject to risk assessment for purposes of determining client classification and the due diligence on the account required under the AML rules.

2. The frontliner shall determine classification using the Client Assessment Form for its clients and the corresponding level of due diligence to be performed. In case of Metrobank Group common clients, the Frontliner shall adopt the classification indicated under the CAF accomplished by 3rd party originating unit or branch, which shall be requested in conjunction with the Certification on KYC Reliance.

3. Before entering into a transaction, the Account Officer/Staff shall also check the name of the client against the watchlist database in the TCS Bancs Compliance System. Any addition to the watchlist database (which the AMLC may issue from time to time) shall also be counter-checked against existing list of clients. Checking with service bureaus shall be performed for indication of questionable

activities. The Account Officer/Staff or designated personnel shall print the report generated from the TCS Bancs Compliance system and attach the same with the CAF; affixing his/her signature on the CAF manifesting that the required "Client Verification" process had been completed.

4. After determining the client classification, the Account Officer shall require client to submit information and identification documents according to the level of required customer due diligence.

D. Customer Identification and Customer Due Diligence

1. Customer Identification Policies and Procedures

a. Satisfactory evidence of the true and full identity, representative capacity, domicile, legal capacity, occupation or business purpose/s of the clients, as well as other identifying information on those clients, whether they be occasional or usual, shall be strictly obtained. For this purpose, the necessary official documents as enunciated under Rule 3.M of the RIRR or Part III, JJ of this Manual, relative to the opening of accounts shall be submitted by the clients to support their identity.

b. Face-to-Face contact – No new accounts shall be opened and created without face-to-face contact and personal interview between FAMI duly authorized personnel and the potential customer, except as may be provided by existing rules and regulations of the Securities and Exchange Commission.
The use of Information and Communication Technology (ICT) in the conduct of face-to-face contact and interview is allowed provided that the designated FAMI personnel/agent is in possession of and has verified the identification documents submitted by the prospective client *prior* to the interview and the *entire procedure is documented*.

c. Account opened through a trustee, agent, nominee or intermediary

Where the account is opened through a trustee, agent, nominee on intermediary, FAMI shall establish and record the true and full identity and existence of both the (a) trustee, nominee, agent or intermediary and (b) trustor, principal, beneficial owner, or person on whose behalf the account is being opened. FAMI shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same criteria for assessing the risk profile and determining the standard of due diligence to be applied to both.

In case of several trustors, principals, beneficial owners, or persons on whose behalf the account are being opened where the trustee, nominee, agent or intermediary opens a single account but keeps therein sub-accounts that may be attributable to each trustor, principal, beneficial owner,

or person on whose behalf the account is being opened, FAMI, at the minimum, needs to obtain the true and full name, place and date of birth or date of registration, as the case may be, present address, nature of work or business, and source of funds as if the account was opened by them separately. Where FAMI is required to report a CT or circumstances warrant the filing of an ST, it shall obtain such other information on every trustor, principal, beneficial owner, or person on whose behalf the account is being opened in order that a complete and accurate report may be filed with the AMLC.

In case the Company entertains doubts that the trustee, nominee, agent of intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence or file a Suspicious Transaction Report, if warranted.

d. The Account officer/staff shall require the client or investor to accomplish **one (1) copy of Account Opening Folder** (Individual - Appendix A; Corporate - Appendix B). The client or investor shall complete the form in front of the Account Officer/staff/agent and provide the following minimum information including the specimen signature/s of the authorized signatory/ies and documents/proofs of legal existence:

For Natural Persons/ Individual Clients/Investors:

- Client Name and any other names used (such as maiden name, etc.)
- Date and Place of birth
- Nationality
- Civil Status
- Present Address
- Permanent Address
- Contact Number or information
- Specimen signature or biometrics of the client
- Nature of work, name of Employer or nature of self-employment/business
- T.I.N./SSS/GSIS/Driver's License/Passport No. as may be applicable
- Source/s of Funds

- Name, present address, date and place of birth, nationality, nature of work and source of funds of Beneficial Owner, whenever applicable.

For Corporate Clients/Investors:

- Company/Registered Name
- Nature of Business
- Business Telephone No./Business Fax No.
- Business Address and/or Principal place of business operations
- Business T.I.N.

- SEC Registration No. and Date of Registration/Birth
- Authorized Representative/s with Positions in the company
- Name, present address, date and place of birth, nationality, nature work and source of funds of beneficial owner/s or beneficiary, where applicable, and authorized signatories
- Specimen signatures of authorized signatories

e. **Clients who engage in financial transactions with Covered Persons for the first time shall be** required to present the original and submit a clear copy of at least one (1) valid photo-bearing identification document **issued by an official authority. For this purpose, the term "official authority" shall refer to any of the following**.

The ID to be valid must be issued by:

i. government of the Republic of the Philippines;
ii. its political subdivisions and instrumentalities;
iii. government-owned and/or controlled corporations (GOCCs); and
iv. private entities or institutions **registered with or** supervised or regulated either by the BSP or SEC or IC

Valid IDs include the following:

- Passport
- Driver's License
- PRC ID
- NBI Clearance
- Police Clearance
- Postal ID
- Voter's ID
- Barangay Certification
- Senior Citizen Card
- GSIS e-Card/UMID
- SSS Card
- TIN ID
- OWWA ID
- OFW ID
- Seaman's Book
- IBP ID
- Alien/Immigrant Certificate of Registration
- Government Office and GOCC ID
- DSWD Certification
- Philhealth Insurance Card ng Bayan
- Certification from the National Council for Welfare of Disabled Persons
- Company ID issued by private institutions supervised or regulated by either BSP, SEC or IC
- Student's ID
- SEC Certificate of Registration

- Business Registration Certificate
- Passports issued by foreign governments shall also be considered valid identification documents

Students who are beneficiaries of remittances/fund transfers who are not yet of voting age may be allowed to present the original and submit a clear copy of one (1) valid photo-bearing school ID duly signed by the principal or head of school.

The Company may require additional identification documents to further vouch the identity of the clients.

f. If the client or investor is in business, the following additional legal and other documents shall also be obtained to establish legal existence and structure as well as the authority to open account for corporate clients/investors:

For Natural Persons/Individual Clients/Investors:

- Certificate of Registration issued by the Department of Trade and Industry
- Mayor's Permit

For Corporate Clients/Investors:

- Certificate of Registration issued by the SEC or the BSP for money changers/foreign exchange dealers and remittance and transfer companies
- Articles of Incorporation or Partnership and By-laws
- Secondary license or Certificate of Authority issued by the supervising authority or other government agency
- Board or Partners' Resolution or Secretary's Certificate to Open Account
- Board or Partners' Resolution or Secretary's Certificate of Authorized Signatories containing Specimen Signatures
- Latest General Information Sheet listing the names of Directors/Trustees/Partners, Principal Stockholders owning at least 20% of the outstanding capital stock and its primary Officers such as the President and Treasurer
- Sworn Statement as to Existence or Non-existence of Beneficial Owners
- For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by the Philippine Consulate where said entities are registered.

For Legal Arrangement (e.g. TRUST), the following must be obtained:

- Name of legal arrangement and proof of existence
- Address and country of establishment
- Nature, purpose and objects of the legal arrangement

- The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and other natural person exercising ultimate effective control over the legal arrangement
- Description of the purpose/activities of the legal arrangement
- Expected use of the account and
- Amount, Number, Type, Purpose and Frequency of the transaction expected

g. Authentication of Specimen Signature and Identification Document (ID):

Photocopies of identification and legal documents shall always be authenticated or verified against the original documents to ensure validity and authenticity. However, certified true copies of the said documents shall be accepted in case the original documents are not available.

The Account Officer/Designated Officer or Agent who has face-to-face contact with and/or witnesses the signing of documents by the client, shall authenticate the client's specimen signature on the provided space for this purpose in the Customer Data Sheet. The stamping of "Verified Against Original" on the photocopy of ID's presented shall be done and to be signed and dated by the attending FAMI authorized personnel or agent.

h. Before establishing a business relationship with corporate clients/investors, a company search and/or other commercial inquiries shall be made to ensure that the prospective client has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In case of doubt as to the identity of the company, its directors or the business, a search or inquiry with the Securities and Exchange Commission and/or the BSP shall be made.

i. For companies and businesses registered outside the Philippines, comparable documents duly authenticated by the Philippine Consulate where said companies are located shall be obtained.

j. The Senior Officer or a Designated Officer/Agent shall interview new clients or those clients with non-recurring transactions with the Company.

k. Representatives, acting on behalf of a client or investor, shall be required to present a duly notarized authorization signed by the client or investor. In addition, identification documents (e.g., Employment/Company ID, Driver's License, Passport, SSS/GSIS ID) shall be obtained from the client's or investor's representative to ascertain his true identity.

l. Where the customer or authorized signatory is a non-Philippine resident, similar IDs duly issued by the foreign government where the customer is a resident or a citizen may be presented. For companies and businesses registered outside the Philippines, comparable documents duly authenticated by the Philippine Consulate wherein said companies are located shall be

obtained.

m. For common customers with Metrobank, the Company shall rely on customer due diligence performed by the parent company. For this purpose, the designated Officer of Metrobank shall accomplish the "Certification of KYC Reliance" which provides among others the following;(1) it has conducted the required customer identification procedures on the client/customer, inclusive of the face-to-face contact and custody of the mandated minimum information and documentary requirements and (2) it will provide to FAMI, without delay, the relevant identification documents when so requested by the latter.
The Frontliner shall request for the Certification of KYC reliance from the originating bank or unit on the same date of the transaction and upon its receipt, the same shall be forwarded to the Operations Support Division. On a monthly basis, OSD shall review the completeness of KYC Reliance Certifications and make a follow-up, where necessary from the concerned Metrobank branch or unit.

n. Business transactions shall not be conducted with prospective clients who fail to provide evidence of their identity. This policy shall be properly disseminated to ensure public awareness. However, this will not preclude the Company from reporting suspicious transactions.

o. If during the business relationship, there is reason to doubt the accuracy of the information on the client's identity, the following measures shall be taken to verify the identity of the client or the beneficial owner, whichever is applicable: (a) it shall be classified as high risk account subject to continuous monitoring and (b) disciplinary history and disclosure of past relevant sanctions shall be reviewed.

p. For large clients or investors, a prior bank/non-bank reference shall be requested. A letter inquiring about the client or investor shall be sent to the reference indicated.

q. When circumstances allow, a visual check of the business enterprise shall be performed to verify its actual existence and capability to provide the products or services indicated on the business documents.

r. In case of doubt as to whether the trustee, nominee or agent is being used as dummy in circumvention of existing laws, further inquiries shall immediately be made to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, the Company shall apply the "Know Your Customer" principle in deciding whether or not to proceed with the business.

s. Reasonable inquiries shall be made on accounts opened by a firm of lawyers

or accountants when transactions passing through such accounts give cause for concern.

t. Investment accounts shall be maintained only in the name of the account holder. Hence, the Company shall not open or keep anonymous, fictitious name, incorrect name and similar accounts.

u. U.S. Indicia Accounts – An account has "US Indicia" if any one of the following exists: (1) known to be a U.S. citizen or resident or born in the U.S., (2) has a U.S. residence or mailing address or telephone number, (3) has granted a power of attorney over the account to a person with a U.S. address, (4) tax residents, (5) has a "care of" or "hold mail" address that is the sole address of the account holder, or (6) a corporation or partnership where U.S specified person owns more than 10% of its equity. EDD is required for this account.

v. Numbered Accounts/Fictitious Names. The Company shall maintain customer's account only in the true and full name of the account owner or holder. Anonymous accounts, accounts under fictitious names, numbered accounts and all other similar accounts shall be absolutely prohibited.

w. Foundations, Clubs and Associations – In addition to the identification documents required for Corporate Clients/Investors, the following incorporation papers/documents shall be obtained:

- φ Articles of Incorporation and By- Laws;
- φ Board Resolution or Secretary's Certificate to Open Account/invest;
- φ Board Resolution or Secretary's Certificate of Authorized Signatories Containing Specimen Signatures;
- φ Latest General Information Sheet showing the List of Names of Directors and Principal Stockholders;
- φ Sworn Statement as to Existence or Non-existence of Beneficial Owners;
- φ Description of the real purpose/activities of the client if the same is not expressly indicated in the Articles Incorporation and By-Laws;
- φ SEC registration certificate and/or SEC certification confirming legal existence of account holder.

The Company should verify information derived from the above-mentioned documents by at least one of the following, whichever is applicable:

- Obtaining an independent undertaking from a reputable and known firm of lawyers and accountants;
- Obtaining prior bank references;
- Accessing public and private databases or official sources.

After positively identifying the institution, steps should be taken also to identify and verify at least two (2) signatories and if they are not the key officers of the

entity, the identity of the principal officers should be verified. For this purpose, the principals who should be identified are those persons exercising control or significant influence over the organization's assets. This includes members of a governing body, the President, any of the Board members, the Treasurer and all the signatories.

In all cases, independent verification should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

2. Customer Due Diligence

The Sales and Marketing Group and Operations Department shall comply with the following guidelines for establishing the true and full identity of the customers:

a. Reduced Due Diligence for Low Risk Customer

i. For individual customers, FAMI may open an account under the true and full name of the account owner/s upon presentation of acceptable identification card or official document as defined in this Manual or other reliable, independent source documents, data or information.

ii. For corporate, partnership, and sole proprietorship entities, and other entities such as banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such, publicly listed companies subject to regulatory disclosure requirements, government agencies including GOCCs, FAMI may open an account under the official name of these entities with the minimum information/documents and Board Resolution duly certified by the Corporate Secretary authorizing the signatory to sign on behalf on the entity, obtained at the time of account opening.
Verification of the identity of the customer, beneficial owner or authorized signatory will be done after the establishment of the business relationship.

b. Average Due Diligence for Normal Risk Customers

For New Individual customers – FAMI shall obtain at the time of account opening all the minimum information and confirming this information with the valid identification documents hereof from individual customers before establishing any business relationship.

New Corporate and Juridical Entity – FAMI shall obtain the minimum information and/or documents and authorized signatory/ies of corporate and juridical entities before establishing business relationships.

c. Enhanced Due Diligence for High Risk customers

Whenever enhanced due diligence is applied as required by the customer identification policy, the Sales and Marketing Group shall, in addition to the minimum KYC identification requirements, shall do the following:

1) Obtain additional information other than the minimum information and/or documents required for the conduct of average due diligence;

   (a) In cases of individual customers, i. supporting information on the intended nature of the business relationship/source of funds/source of wealth, ii. Reasons for the intended or performed transactions, iii. list of companies where he is a director, officer or stockholder, iv. list of banks where the individual has maintained or is maintaining an account, and v. other relevant information available through public databases or internet.

   (b) For entities assessed as high risk customers, such as shell companies; i. prior or existing bank references, ii. the name, present address, nationality, date of birth, nature of work, contact number, and source of funds of each of the primary officers (President, Treasurer and authorized signatory/ies), stockholders owning at least 20% of the voting stock, and directors/trustees/partners as well as their respective identification documents; iii. volume of assets, other information available through public databases or internet; iv. supporting information on the intended nature of the business relationship, source of funds or source of wealth; and v. reasons for the intended or performed transactions.

2) Conduct validation procedures on any or all of the information provided

3) Secure senior management approval or the AML Compliance Committee approval to commence business relationship.

4) Conduct enhanced ongoing monitoring of the business relationship

5) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, FAMI shall deny business relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when so warranted.

The Operations Department, on the other hand, in addition to profiling of customers and monitoring of their transactions, shall see to it that the requisites for the conduct of enhanced due diligence has been

complied with and the Sales and Marketing Group has obtained the abovementioned additional information and/or documents from its clients and senior officer's approval.

Enhanced Due Diligence, Minimum Validation Procedures

I. Individual Customers – Validation procedures include but are not limited to the following:

a) Confirming the date of birth from a duly authenticated official document
b) Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters or other documents showing address or through on – site visitation
c) Contacting the customer by phone or email
d) Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means
e) Determining the veracity of the declared source of funds.

II. Corporate or Juridical Entities – Verification procedures shall include, but are not limited to the following:

a) Validating the source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.
b) Inquiring from the supervising authority the status of the entity
c) Verifying the address through on-site visitation of the Company, sending thank you letters, or other documents showing address
d) Contacting the entity by phone or email.

III. Foreign Exchange Dealers/ Money Changers/ Remittance Agents – The Company shall require their customers who are foreign exchange dealers, money changers and remittance agents to *submit a copy of the certificate of registration issued to them by the BSP* as part of their customer identification document. The certificate of registration shall be for each head office, branch, agent, sub-agent, extension office of business outlet of foreign exchange dealers, money changers and remittance agents. Foreign exchange dealers, money changers and remittance and transfer companies presenting greater risk shall be subject to enhanced due diligence. As such, required are a) the submission of AMLC registration, b) reviewing their AML/CFT program and c) securing senior management approval for establishing a business relationship.

IV. High Risk Customer – A customer from a foreign jurisdiction that is recognized as having inadequate internationally accepted AML

standards, or presents greater risk for ML/TF or its associated unlawful activities, shall be subject to ECDD. Information relative to these are available from publicly available information such as the websites of FATF, FATF Style Regional Bodies (FSRB) like the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities like the OFAC of the U.S. Department of the Treasury, or other reliable third parties such as regulators or exchanges, which shall be a component of the Company's customer identification process.

V. Shell Company/ Shell Bank – The Company shall undertake banking relationship with a shell company with extreme caution and always apply EDD on both the entity and its beneficial owner/s.

Because of the dubious nature of shell banks, no shell bank shall be allowed to operate or be established in the Philippines. The Company shall refuse to enter into, or continue, correspondent banking relationship with them. It shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks.

VI. Prohibited accounts – The Company shall maintain accounts only in the true and full name of the account owner. The provisions of existing law to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, numbered checking accounts, and all other similar account shall be absolutely prohibited.

VII. Treatment of dormant accounts. Where a client's account considered dormant for a number of years and suddenly becomes unusually active again transacting large sums of money, it shall be carefully reviewed to ensure that the standard identification procedures are followed.

VIII. Handling of "pooled" funds of entities such as mutual funds, money managers, trusts and foundations, and other professional intermediaries. The Company shall require the customer to disclose the identity/ies of the beneficial owner/s of the funds and those who are in control of the funds invested. Any information gathered shall be verified from trustworthy parties such as banks, reputable law firms'/accounting firms or accessing public or private databases or official sources.

CHAPTER 3: ON-GOING MONITORING OF ACCOUNTS AND TRANSACTIONS

On-going monitoring of accounts and transactions is an essential aspect of effective KYC procedures. The front line staff members of the Company including senior management who are directly in contact with high-net worth customers shall have an understanding of

the normal and reasonable account activity of the clients. The process of on-going monitoring of accounts includes the following:

1. Customer information and identification documents should be *kept up to date once every three (3) years* in conformity with the RIRR. A risk-and-materiality based on-going monitoring of customer's accounts and transactions is to be part of customer due diligence.

2. Timely information like reports on critical customer data not obtained/disclosed despite diligent follow up, or such reports on customers with unusual activities that may lead to suspicious transactions shall be provided to the Sales and Marketing Group Head copy furnished the Compliance Officer/Coordinator who will analyze and effectively monitor high risk customer accounts.

3. Members of senior management who are in direct contact with high net worth/important customers shall endeavor to know the personal circumstances of these customers and be alert to sources of third party information. Unusual activities of these types of customers that may put the Company at risk shall be reported to the AMLC Committee.

Enhanced Due Diligence – Sales and Marketing Group and Operations Support Division shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. To this extent, the Company shall apply enhanced due diligence on its customer if it acquires information in the course of its customer account or transaction monitoring that:

1. Raises doubt as to the accuracy of any information or document provided or the ownership of the entity.
2. Justifies reclassification of the customer from low or normal risk to high-risk pursuant to its own criteria; or
3. Any of the circumstance for the filing of a suspicious transaction exists such as but not limited to the following:
   a. Transacting without any underlying legal or trade obligation, purpose or economic justification;
   b. Transacting an amount that is not commensurate with the business of financial capacity of the customer or deviates from his profile;
   c. Structuring of transactions in order to avoid being the subject of covered transaction reporting; or
   d. Knowing that a customer was or is engaged or engaging in any unlawful activity as herein defined.

4. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the Company shall immediately close the account and refrain from further conducting business relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

CHAPTER 4: MAINTENANCE OF RECORDS AND RETENTION

A. Record Keeping

1. All customer identification records and transaction documents of FAMI shall be maintained and safely stored for five (5) years from the date of the transaction.

2. Client relationships and transactions shall be properly documented. In this regard, adequate records on customer identification shall be maintained to ensure that:

   a. Any transaction can be reconstructed and an audit trail is established when there is suspected money laundering; and

   b. Any inquiry or order from the regulatory agency or appropriate authority can be satisfied within a reasonable time such as disclosure of information (e.g., whether a particular person is the client or beneficial owner)

3. In the instance that a case has been filed in Court involving the account, records must be retained and safely kept beyond the five (5) year until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

4. For closed accounts, all records of customer identification and transaction documents shall be maintained and safely stored for at least five (5) years.

B. Safekeeping of Records and Documents – FAMI shall designate at least two (2) Officers who will be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA, as amended, its RIRR and this Manual. They shall have the obligation to make these documents and records readily available without delay during SEC/AMLC regular or special examinations.

1. The Operations Support Division Head shall be responsible and accountable for safekeeping of records and documents pertaining to account opening, signature cards and transaction trails.

2. Records of Covered and Suspicious Transaction reporting shall be maintained and safekept by the Compliance and Administrative Division. A register of all reports made to the AMLC, as well as reports made by the directors, officers or employees relative to suspicious transactions, whether or not such were reported to the Council, shall be maintained. Said register shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant papers. In addition, the Compliance Division shall ensure that the reports and other records on all transactions brought to the attention of the AML/CFT Committee including transactions that are not reported to the AMLC are complete and properly kept.

D. Form of Records – Records shall be retained as originals or copies in such forms as are admissible in court pursuant to existing laws, such as the e-commerce act and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court. Further, electronic copies of all covered and suspicious transaction reports shall be kept for at least five (5) years from the date of submission to the AMLC.

CHAPTER 5: COVERED AND SUSPICIOUS TRANSACTIONS

A. Covered Transactions as defined under Section 3, paragraph (b) of R. A. No. 9160 (as amended) and Section 1 of R.A. No. 9194, is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (Php 500,000.00) within one (1) banking day.

B. Suspicious Transactions as defined under Section 3, paragraph (b-1) of R. A. No. 9160 (as amended) and Section 2 of R.A. No. 9194, are transactions with Covered Persons, regardless of the amounts involved, where any of the following circumstances exist:

a. There is no underlying legal or trade obligation, purpose or economic justification;

b. The client is not properly identified;

c. The amount involved is not commensurate with the business or financial capacity of the client;

d. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the Act.

e. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the Covered Person;

f. The transaction is in any way related to an unlawful activity or offense under this Act that is about to be, is being or has been committed; or

g. Any transactions that is similar or analogous to any of the foregoing.

C. The Company officers and staff shall at all times be alert of any customers falling under the above circumstances.

D. Initial inquiries and, when necessary, further investigations on the source of funds shall be immediately performed if any suspicious transaction is identified.

E. If the Operations Officer/Staff identifies a substantial increase in cash deposits or placements from an individual or local business entity, he/she shall satisfy himself/herself that the client has a legitimate explanation for the unusual activity.

F. Investigation of Suspicious Transactions

Any indication of suspicious activity shall be investigated to prevent money laundering and other illegal transactions of similar nature:

1. Any transaction that is outside the usual activity of a known client or involving large sums of money in cash or financial instruments received from or payable to non-clients is potentially suspicious and shall be carefully examined.

2. The degree of investigation shall depend on what the Company knows about the client and the nature of the proposed transaction:

    a. The Company shall satisfy itself that the transaction is legitimate.

    b. A general explanation for an isolated transaction from highly regarded clients whose normal activity is known shall be obtained.

    c. A more detailed explanation for large transaction from clients shall be obtained. If the explanation is unsatisfactory, more information shall be obtained before a transaction is authorized or declined.

    d. The transaction shall be referred to higher authority or the AMLC Committee for disposition when in doubt.

3. If the Company's concerns are not resolved during discussion with the client, discreet inquiries shall be performed without his/her knowledge. Uncorroborated explanation from the client shall not be relied on if the transaction is unusual or the potential for abuse is great. If necessary, independent verification for at least a material part of the explanation shall be obtained. The Company shall be alert that something may be wrong if minimal information provided by the client could not be verified independently.

4. The Company shall be vigilant for any unusual, strange and/or peculiar transactions. It shall always follow sound banking practices.

    The Operations Officer/staff shall be particularly vigilant about unusual placement activity if its client is a foreign exchange, securities, commodity or precious metals dealer or is engaged in any other business, which is particularly susceptible to money laundering:

    a. These customers shall be closely monitored.

    b. The Company shall ensure that its file contains an explanation of unusual transactions.

c. Large/unusual transactions shall be reviewed with the Division or Group Head for advice, counsel and direction.

5. Follow-up calls or letter to the client's residence and/or place of business shall be made, thanking him/her for opening an account. Disconnected phone service warrants further investigation.

6. The concerned Officer/Staff who identified a suspicious transaction shall refer the suspected account to the Division Head for further verification.

G. Unusual and Suspicious Transactions Monitoring

1. Monitoring System for Money Laundering – FAMI shall ensure that it has the means of flagging and monitoring the transactions below:

   a. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;

   b. Watch list monitoring – checks the existing customer database for any listed undesirable individual or corporation;

   c. Investigation – checks for given names throughout the history of payment stored in the system;

   d. Can generate all the CTRs of the Covered Person accurately and completely with all the mandatory field properly filled up;

   e. Must provide a complete audit trail;

   f. Capable of aggregating activities of a customer with multiple accounts on consolidated basis for monitoring and reporting purposes; and

   g. Has the capability to record all STs 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.

H. Reporting of Covered and Suspicious Transactions

1. All covered transaction (CTR) and suspicious transaction (STR) shall be reported to the AMLC within five (5) working days from occurrence thereof, unless the AMLC prescribes a different period not exceeding fifteen (15) working days.

2. For a suspicious transaction, occurrence refers to the date of determination of the suspicious nature of the transaction, which determination shall be made not exceeding ten (10) calendar days from the date of the transaction. However, when

the transaction is in a way related to or the person transacting is involved or connected to an unlawful activity or money laundering offense, the 10-day period shall be reckoned from the date there was knowledge of the suspicious transaction indicator.

3. In case the transaction to be reported is both a covered and suspicious transaction, the same shall be reported as a suspicious transaction only.

4. CTR and STR shall be filed in the forms prescribed by the AMLC and shall be submitted in a secured manner in electronic form in conformity with the AMLC Reporting Procedure version 3 issued in March 2014.

5. No administrative, criminal or civil proceedings shall prosper against any person for having made a CTR or STR in the regular performance of duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other law of the Philippines.

6. Deferred Reporting of Certain Covered Transactions – Pursuant to AMLC Resolution No.58 dated 25 March 2005 as amended by AMLC Resolution No. 24 dated 18 March 2009, the following are considered as "non-cash, no/low risk covered transactions" the reporting of which to the AMLC are deferred:

    a. Transactions between banks and the BSP;
    b. Transactions between banks operating in the Philippines;
    c. Internal operating expenses of banks;
    d. Transactions involving transfer of funds from one deposit account to another deposit account of the same person within the same bank;
    e. Roll-overs of placements of time deposit; and
    f. Loan/Interest principal payment debited against borrower's deposit account maintained with the lending bank.

    AMLC, in its letter dated 06 April 2011, clarified that:

    - If the settlement between FAMI and its client (also a Metrobank client) is made through fund transfers or "debiting and crediting" of their respective accounts within the same bank (in which case there is no physical movement of funds but only a book-entry transfer of funds), FAMI need not file a CTR thereon in as much as the said transactions are akin to a transaction in check reporting of which pertains to the concerned bank.

    - Inasmuch as roll-over/re-investment of money market placements partakes the nature of "roll-overs of placements of time deposits" – one of the BSP identified non-cash, no/low risk covered transactions enumerated under AMLC Resolution No. 58, series of 2005, the reporting of such transaction is likewise deemed deferred.

J. Suspicious Transaction Reporting Procedures

Upon identification of unusual or suspicious transaction, the following procedures shall be followed:

1. The concerned CRM or business unit front liner or Operations personnel who identified a suspicious transaction shall refer the suspected account to the Division Head or Group Head for further verification.

2. The Division Head or Group Head shall evaluate the report and he/she is of the opinion that there is/are reasonable basis for the suspicion, shall prepare his/her evaluation report and shall be forwarded to the Compliance Officer/Coordinator.

3. Upon receipt of the reports, the Compliance Officer/Coordinator shall convene a meeting of the AML Compliance Committee to evaluate the reports and determine if the suspicion is based on reasonable grounds.

4. If the Committee decides that there is reasonable basis for considering a suspicious transaction or other illegal activity, a Suspicious Transaction Report (STR) must be sent to AMLC using the prescribed form duly signed by the Compliance Officer together with other supporting documents. The STR shall be submitted to the AMLC within ten (10) calendar days from the date that the transaction was determined to be suspicious.

5. In the event that urgent disclosure is required, particularly when the account concerned is part of an ongoing investigation, the Compliance Officer/Coordinator shall notify in writing the AMLC Committee.

6. The Company and its directors, officers and employees shall not warn the clients when information relating to them is being reported or will be reported to the AMLC or that a 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 shall not be published or aired, in any manner or form, by the mass media or through electronic mail or other similar devices. In case of violation, the concerned Officer or employee shall be held criminally liable.

7. A director, officer or employee of the Company who knows that a client has engaged in any of the predicate crimes under R.A. No. 9160 (as amended) shall promptly report the matter to the Compliance Officer. In this regard, the Compliance Officer shall immediately report the details to the AML Compliance Committee and the AMLC.

8. If there are reasonable grounds to suspect that the client has engaged in an unlawful activity, the AML Compliance Committee, on receiving such a report, shall promptly evaluate whether the suspicion if valid. The case shall be immediately reported to the AMLC unless the committee considers that such reasonable grounds do not exist. However, unreported suspicion shall be properly recorded.

9. A register of all reports made to the AMLC, as well as reports made by the directors, officers or employees relative to suspicious transactions, whether or not such were reported to the Council, shall be maintained. Said register shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant papers. In addition, the AMLC Committee shall ensure that the reports and other records on all transactions brought to their attention, including transactions that are not reported to the AMLC are complete and properly kept.

K. Training

1. The Company shall provide education and training for all personnel, including officers and directors, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and be familiar with the system of reporting and investigating suspicious transactions.

2. The lecture/briefing on anti-money laundering shall generally be conducted by competent personnel of the Company or FMIC. However, if necessary, the training functions can be assigned to outside party/ies provided due diligence is exercised to ensure that the person/s appointed is/are able to perform effectively.

3. The FMIC Compliance Division shall formulate an annual AML training program aimed to provide efficient, adequate and continuous education program for all FAMI personnel, including officers and directors, to ensure that they fully comply and are fully aware of their obligations and responsibilities in combating money laundering particularly in relation to customer identification process, record keeping requirements and CT/ST reporting and ample understanding of the internal reporting processes including the chain of command for the reporting and investigation of suspicious and money laundering activities.

4. The timing and scope of training shall be based on the level of awareness and instruction needed for each group of employees:

   a. ***For New Hires*** - a general appreciation of the background of money laundering and identification and reporting of suspicious transactions to the appropriate authority. This training shall be provided to all new employees regardless of seniority, which shall be conducted by FAMI HRD within 30 days from effective date of hiring. This shall be conducted thru the use of AML Computer-Based Training (CBT) e-learning program followed by a written examination. An employee is considered to have passed the AML examination when he/she meets a passing rate of 75%. Those who fail the exam shall undertake to repeat the exam until he/she passes.

   b. A refresher training shall be conducted, at least once a year, to remind key personnel of their responsibilities and to make them aware of any changes in the law, rules and regulations relating to money laundering as well as the internal policies and procedures.

The lecture/briefing on anti-money laundering and countering financing of terrorism shall be conducted by the Compliance Management Department officer/s. CMD may also invite external resource speaker/s to conduct workshop on AML/CFT. However, if necessary, the training functions can be assigned to outside party/ies provided due diligence is exercised to ensure that the person/s appointed is/are able to perform effectively.

5. The Compliance Officer/Coordinator shall regularly circulate compliance bulletins covering amendments in the anti-money laundering law and changes in the pertinent rules and regulations. Developments in the anti-money laundering campaign of the government shall also be advised to all concerned.

6. Training Programme Records

FAMI's annual AML training program and records of all AML seminars and trainings conducted by FMIC and / or attended by its personnel (internal or external), including copies of AML seminar / training materials, shall be appropriately kept by the Compliance and Administrative Division.

CHAPTER 6: AML/CFT RISK MANAGEMENT

FAMI shall develop sound risk management policies and practices to ensure that risks associated with money-laundering such as counterparty, reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of these regulations, to the end that FAMI shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate of finance terrorism.

Four (4) areas of sound risk management practices:

A. Active Board and Senior Management oversight

1. Board and Senior Management Oversight

It shall be the ultimate responsibility of the Board of Directors to fully comply with the provisions of these rules, the AMLA, as amended and its RIRR. It shall ensure that oversight on the institution's compliance management is adequate.

Senior Management shall oversee the day to day management of the covered person, ensure effective implementation of the AMLCFT policies approved by the Board and alignment of activities with the strategic objectives, risk profile and corporate values set by the BOD. Further, Senior Management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

2. Committee on Money Laundering

The Company shall set up a Committee on Money Laundering composed of the members of the Senior Management and the Compliance Officer. It shall be the designated unit responsible for advising management and staff on the issuance and implementation of policies, procedures and controls to promote adherence to R.A. No. 9160 (as amended), IRR and operating manuals and regulations issued by SEC and BSP. The internal guidelines shall include personnel training, reporting of covered and suspicious transactions, and generally, all matters relating to the prevention of money laundering.

3. Compliance Office and Designation of Compliance Officer

Management of the implementation of FAMI's Money Laundering and Terrorist Financing Prevention Program (MLPP) shall be a primary task of the Compliance and Administrative Division and the designated Compliance Officer/Coordinator. To ensure independence of the division, it shall have a direct reporting line to the Board of Directors through the AMLC Committee on all matters related to AML and Terrorist Financing compliance and their risk management.

The designated Compliance Officer, as duly approved by the Board of Directors to oversee and coordinate the implementation of the Compliance System, shall also oversee and coordinate the implementation of the Anti-Money Laundering Manual.

The following are the primary duties and responsibilities of the Compliance Officer in relation to anti-money laundering:

1. Responds sufficiently well to inquiries pertaining to the covered person and the conduct of its business;

2. Establishes and maintains a manual of compliance procedures in relation to the business of the Company;

3. Ensures compliance by the officers and employees with the provisions of the anti-money laundering law as amended, implementing rules and regulations and this Manual; conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system through sample testing and review of audit or examination reports. Further, to report to the AMLCC any compliance findings;

4. Ensures that infractions, discovered either by internally initiated audits, or by special or regular examinations conducted by applicable regulators are immediately corrected;

5. Apprises all responsible Officers and employees of all resolutions, circulars and other issuances by the AMLC in relation to matters aimed at preventing MF and TF and organizes the timing of AML training of Officers and employees including refresher trainings;

6. Alerts senior management, the BOD or FAMI AMLC Committee if it believes that the covered person is failing to appropriately address AML/CFT issues;

7 Acts as the liaison between the Company and the AMLC in matters relating to compliance with the provisions of the anti-money laundering law, rules and regulations; and

8 Prepares and submits to the AMLC written reports on the Company's compliance with the provisions of anti-money laundering law, rules and regulations, in such form and submitted at such time as the Council may determine.

B. Acceptable policies and procedures embodied in a Money Laundering and Terrorist Financing Prevention Program (MLPP)

FAMI shall adopt a comprehensive and risk-based MLPP geared toward the promotion of high ethical and professional standards and the prevention of the Company being used, intentionally or unintentionally, for money laundering and terrorism financing. The MLPP shall be consistent with the AMLA, as amended, and the provisions set out in AMLC's 2016 RIRR of R.A. No. 9160.

It shall be in writing, approved by the Board of Directors, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same.

C. Appropriate Monitoring and Management Information System

FAMI shall adopt an AML and terrorist financing monitoring system that is appropriate for their risk-profile and business complexity and in accordance with existing rules and regulations on AMLA under AMLC and SEC. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the Board of Directors and Senior Management on anti-money laundering and terrorist financing compliance at least once every year or annually**.**

Manual monitoring – FAMI need not have an electronic system but must ensure that it has the means of complying with the AML regulations, its internal policies and Compliance System Manual (Monitoring and Reporting Tools).

D. Periodic Audit

The Internal Audit group of Metrobank shall perform a periodic review of the implementation of the policies and procedures indicated on the Anti-Money Laundering Manual to determine compliance with existing laws and regulations, evaluate adequacy and measure effectiveness. Any adverse findings shall be advised to the Compliance Officer or Compliance Coordinator and the AMLCC for appropriate action.