FIRST METRO ASSET MANAGEMENT, INC.

Metrobank Group

MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM (MTPP)

As of April 2021

TABLE OF CONTENTS

CHAPTER ONE – INTRODUCTION

I. Declaration of Policy

FAMI and mutual funds adopt 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 and mutual funds further support 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. Title

These Guidelines shall be referred to as the "FAMI and Mutual Funds Anti-Money Laundering Manual".

III. 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 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.

CHAPTER TWO – DEFINITION OF TERMS

Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the AMLA (Republic Act (RA) No 9160), as amended 9194, 10167, 10365 and the Terrorism Financing Prevention and Suppression Act of 2012 (RA 10168), their respective RIRRs and BSP Circular No. 706 and 950.

A. Anti-Money Laundering Terminologies

a. AMLA – Anti-Money Laundering Act, or R.A. 9160, as amended
b. RIRR – Revised Implementing Rules and Regulations
c. MLPP or the Manual – Money Laundering and Terrorist Financing Prevention Program
d. AMLC – Anti-Money Laundering Council
e. AML/CFT – Anti-Money Laundering/Combating Financing of Terrorism
f. KYC – Know Your Customer
g. CDD – Customer Due Diligence
h. RDD – Reduced Due Diligence
i. EDD – Enhanced Due Diligence
j. CAF – Client Assessment Form
k. CP – Covered Person
l. FATF – Financial Action Task Force
m. AJF – Alert Justification Form
n. CSF – Client Suitability Form
o. PEP – Politically Exposes Person
p. BSP – Bangko Sentral ng Pilipinas
q. SEC – Securities and Exchange Commission
r. IC – Insurance Commission

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. Supervising Authority refers to the BSP, the SEC and the IC. Where the BSP, SEC or IC supervision applies only to the registration of the covered person, the BSP, the SEC or the IC, within the limits of the AMLA, as amended, shall have the authority to require and ask assistance from the government agency having regulatory power and/or licensing authority over said covered person for the implementation and enforcement of the AMLA, as amended, and these Rules.

E. 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.

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.

F. Designated Persons refers 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.

G. 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.

H. Securities Broker is a person engaged in the business of buying and selling securities for the account of others.

I. Securities Dealer means any person who buys and sells securities for his/her own account in the ordinary course of business.

J. Securities Salesman is a natural person hired to buy and sell securities on a salary or commission basis properly endorsed to the Commission by the employing Broker Dealer.

K. Associated Person of a Broker or Dealer is any person employed full time by the Broker Dealer whose responsibilities include internal control supervision of other employees, agents, salesmen, officers, directors, clerks and stockholders of such Broker Dealer for compliance with the SRC and rules and regulations adopted thereunder.

L. Investment Company Adviser / Fund Manager shall refer to an Investment Company Adviser licensee who regularly advises or recommends investment

decisions with regard to the securities or other portfolio of the Investment Company pursuant to an advisory contract with the Investment Company.

M. Mutual Fund Distributor shall refer to a juridical person duly licensed or authorized by the Commission to distribute shares or units of an Investment Company as either principal distributor or sub-distributor.

N. Investment Company is any issuer which is or holds itself out as being engaged primarily, or proposed to engage primarily, in the business of investing, reinvesting or trading in securities.

O. Open-End Investment Company is an Investment company which is offering for sale or has outstanding any redeemable security of which it is the issuer. Also referred to as Mutual Fund.

P. Closed-End Investment Company refers to an Investment company which offers for sale a fixed number of non-redeemable securities which are offered in an initial public offering and thereafter traded in an organized market as determined by the Commission.

Q. Investment Advisor / Agent / Consultant shall refer to any person:

1. who for an advisory fee is engaged in the business of advising others, either directly or through circulars, reports, publication or writings, as to the value of any security and as to the advisability of trading in any security; or
2. who for compensation and as part of a regular business, issues or promulgates, analyzes reports concerning the capital market, except:
   a. any bank or trust company;
   b. any journalist, reporter, columnist. Editor, lawyers, accountant or teacher;
   c. the publisher of any bona fide newspaper, news, business or financial publication of general and regular circulation, including their employees;
   d. any contract market; or
   e. such other person not within the intent of this definition, provided that furnishing of such service by the foregoing persons is solely incidental to the conduct of their business or profession.
3. who undertakes the management of portfolio securities of investment companies, including the arrangement of purchases, sales or exchange of securities.

R. **Financing Companies** are corporations which are primarily organized for the purpose of extending credit facilities to consumers and to industrial, commercial or agricultural enterprises, by direct lending or by discounting or factoring commercial papers or accounts receivable or by buying and selling contracts, leases, chattel mortgages, or other evidences of indebtedness, or by financial leasing of movable as well as immovable property. The same does not include banks, investment houses, savings and loan associations, insurance companies, cooperatives, and other financial institutions organized or operating under other special laws.

S. **Lending Company** shall refer to a corporation engaged in granting loans from its own capital funds or from funds sourced from not more that nineteen (19) persons. It shall not be deemed to include banking institutions, investment houses, savings and loan associations, financing companies, pawnshops, insurance companies, cooperatives and other credit institutions already regulated by law. The term shall be synonymous with lending investors.

T. An **affiliate** means an entity:

1. at least twenty percent (20%) but not more that fifty percent (50%) of the voting stock of which is owned directly or indirectly by a covered institution; or

2. over which a covered institution has the ability in fact to exert a significant influence.

Significant influence refers to the ability to participate in the managerial, operating or financial decisions of an entity with the reasonable possibility, but not certainty, of determining the content of those decisions, This may be shown, for example, by:

a. a contract between the entities, or a provision contained in the lower tier entity's articles of incorporation or other constitutional documents;

b. the ability, in any manner, of the upper tier entity to appoint a member of the board of directors or any equivalent body of the lower tier entity;

c. any situation in which one or more members of the board of directors of the lower tier entity, or any equivalent body of that entity, are accustomed or under an obligation, whether formal or informal, to act in accordance with the instructions or wishes of the upper tier entity in conducting its affairs; or

d. the existence of material and regular transactions between the entities.

U. A **subsidiary** means an entity that is controlled, directly or indirectly, by a covered institution, which may be evidenced by:

a. more than 50% of the outstanding voting stock of which being owned directly or indirectly by such covered institution;

b. such covered institution having the ability in fact to elect a majority of the members of the board of directors or any equivalent body; or

c. such covered institution having the ability in fact to exert a dominant influence over the financial, operational or managerial affairs of the entity. This may be shown, for example by:

1. a contract between the entities, or a provision contained in the entity's articles of association or other constitutional documents;

2. a majority of the members of the board of directors of the entity, or any equivalent body of the entity, being accustomed or under an obligation, whether formal or informal, to act in accordance with the covered institution's directions, instructions or wishes in conducting its affairs.

Any legal entity that beneficially owns, either directly or through one or more controlled companies, more than thirty (30) per centum of the voting securities of another company shall be presumed to control such company. Any such presumption may be rebutted by evidence, but shall continue until a determination to the contrary is made by the Commission.

V. Beneficial Owner refers to any natural person who:

a. Ultimately owns or controls the customer and / or on whose behalf a transaction or activity is being conducted; or
b. Has ultimate effective control over customer that is a legal person or arrangement.

Legal arrangements shall refer to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiducie, treuhand and fideicomiso

Ultimate effective control refers to any situation in which ownership/ control is exercised through actual or a chain of ownership or by means other than direct control. This may be achieved through, but not limited to, any of the following situations:

a. direct or indirect ownership of at least 25% of any category of voting shares or capital of a legal person, arrangement, understanding, relationship or otherwise has or shares voting power, which includes the power to vote, or to direct the voting of such security; and/or investment returns or power, which includes the power to dispose of, or to direct, the disposition of such security; Provided, that a person shall be deemed to have an indirect beneficial ownership interest in any security which is:

    i. held by members of his/her immediate family sharing the same household;

    ii. held by a partnership in which he/she is a general partner;

    iii. held by a corporation of which he/she is the controlling shareholder; or

    iv. subject to any contract, arrangement or understanding which gives him/her voting power or investment power with respect to such securities; Provided, however, that a person shall not be deemed to be a beneficial owner of securities held by him/her for the benefit of third parties or in customer or fiduciary accounts in the ordinary course of business, so long as such shares were acquired by such person without the purpose or effect of changing or influencing control of the issuer.

b. the ability to elect a majority of the board of directors, or any similar body, of a legal person or arrangement; or

c. any situation in which:

    i. a person has the ability in fact to exert a dominant influence over the management or policies of a legal person or arrangement; or

    ii. a majority of the members of the board of directors of a such legal person or arrangement, or any equivalent body, are accustomed or under an obligation, whether formal or informal, to act in accordance with a given person's directions, instructions or wishes in conducting the affairs of the legal person or arrangement.

In exceptional cases where no natural person is identifiable who ultimately owns or exerts control over the legal entity, covered institutions, having exhausted all other means of identification, and provided there are no grounds for suspicion, may consider the senior managing official/s to be the beneficial owner/s.

All securities o the same class beneficially owned by a person, regardless of the form such beneficial ownership takes, shall be aggregated in calculating the number of shares beneficially owned by such person.

A person shall be deemed to be the beneficial owner of a security if that person has the right to acquire beneficial ownership within thirty (30) days, including, but not limited to, any right to acquire, through the exercise of any option, warrant or right; through the conversion of any security; pursuant to the power to revoke a trust, discretionary account or similar arrangement; or pursuant to automatic termination of a trust, discretionary account or similar arrangement.

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

X. 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.

Y. 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.

Z. 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.

AA. 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.

BB. 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.

CC. 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.

DD. 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

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

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

1. Kidnapping for ransom under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;

2. Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15 and 16 of Republic Act No 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;

3. Section 3 paragraphs b, c, e, g, h and i of Republic Act no. 3019, as amended, otherwise known as the "Anti-Graft and Corrupt Practices Act";

4. Plunder under Republic Act No. 7080, as amended;

5. Robbery and Extortion under Articles 294, 295, 296, 299, 300, 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 RA 455, and Republic Act No. 1937, as amended, otherwise known as the "Tariff and Customs Code of the Philippines";

11. Violations under Republic Act no. 8792, otherwise known as the Electronic Commerce Act of 2000;

12. Hijacking and other violations under Republic Act 6235, otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the Revised Penal Code, as amended;

13. Terrorism and Conspiracy to Commit Terrorism as defined and penalized under Sections 3 and 4 of Republic Act No. 9372;

14. Financing of Terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of Republic Act No. 10168, otherwise known as the "Terrorism Financing Prevention and Suppression Act of 2012";

15. Bribery under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, 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;;

29. Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;

30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;

31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;

32. 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 nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

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

GG. Proceeds refers to an amount derived or realized from any unlawful activity.

HH. 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 any insurance policy holder, whether actual or prospective

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

JJ. 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.

KK. Politically Exposed Person, or PEP refers to an individual who is or has been entrusted with a prominent public position/function in:

a. the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources;
b. a foreign state; or
c. an international organization.

It shall be presumed that a person who has been entrusted with a prominent public position/function as referenced above shall continue to be considered a PEP, even if he or she no longer holds such a position, unless it is clearly shown otherwise.

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

1. joint beneficial ownership of a legal entity or legal arrangement with the main/ principal PEP; or

2. sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/ principal PEP.

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

Close associates of PEPs refer to persons who 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. Close associates may include:

1. beneficial owners of a legal entity or legal arrangement that is known to exist for the benefit of the main/ principal PEP;

2. business partners or associates, especially those that share beneficial ownership of legal entities or legal arrangements with the PEP;

3. persons who are otherwise connected to the PEP (e.g. through joint membership of a company board);

4. prominent members of the same political party, civil organization, labor or employee union as the PEP;

5. persons (sexual and/or romantic) partners outside the family unit (e.g. girlfriends, boyfriends, mistresses, etc.).

LL. Covered Institution - The term "covered institutions" shall refer to persons regulated by the Commission under the SRC, the Investment Houses Las, the Investment Company Act, the Financing Company Act of 1998, the Lending Company Regulations Act of 2007, other laws and regulations implemented by the Commission, and the AMLA, as amended. The covered institutions are as follows:

a. Banks, non-banks, quasi-banks, trust entities, foreign exchange dealers, non-stock savings and loan associations, pawnshops, foreign exchange dealers, money changers, remittance and transfer companies, electronic money issuers and other financial institutions/similar entities and all other persons and their subsidiaries and affiliates supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), wherever they may be located;

i. A subsidiary means an entity more than fifty percent (50%) of the outstanding voting stock of which is owned by a bank, quasi_bank, trust entity or any other institution supervised or regulated by the BSP.

ii. An affiliate means an entity at least twenty percent (20%) but not exceeding fifty percent (50%) of the voting stock of which is owned by a bank, quasi_bank, trust entity, or any other institution supervised and/or regulated by the BSP.

b. Insurance companies, pre-need companies, insurance agents, insurance brokers, professional reinsurers, reinsurance brokers, holding companies, holding company systems, mutual benefit associations and all other persons and their subsidiaries and affiliates supervised or regulated by the Insurance Commission (IC);

c. Financing Companies and Lending Companies, both with more than 40% foreign participation in its voting stock or with paid-up capital of Php10 Million or more;

d. Persons supervised or regulated by SEC such as (a) securities dealers, brokers, salesmen, associated person of a broker or dealer, investment houses and other similar entities managing securities or rendering services as investment agent, advisor, or consultant, (b) mutual funds,

closed-end investment companies, common trust funds, mutual fund distributors and other similar persons, and (c) 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);

i. A securities broker includes a person engaged in the business of buying and selling securities for the account of others.

ii. A securities dealer includes any person who buys and sells securities for his/her account in the ordinary course of business.

iii. An investment house includes an enterprise which engages or purports to engage, whether regularly or on an isolated basis, in the underwriting of securities of another person or enterprise, including securities of the Government and its instrumentalities.

iv. A mutual fund or an open-end investment company includes an investment company which is offering for sale or has outstanding, any redeemable security of which it is the issuer.

v. A closed-end investment company includes an investment company other than open ended investment company.

vi. A common trust fund includes a fund maintained by an entity authorized to perform trust functions under a written and formally established plan, exclusively for the collective investment and reinvestment of certain money representing participation in the plan received by it in its capacity as trustee, for the purpose of administration, holding or management of such funds and/or properties for the use, benefit or advantage of the trustor or of others known as beneficiaries.

vii. Investment Advisor/Agent/Consultant shall refer to any person:
   (a) who for an advisory fee is engaged in the business of advising others, either directly or through circulars, reports, publications or writings, as to the value of any security and as to the advisability of trading in any security;
   (b) who for compensation and as part of a regular business, issues or promulgates, analyzes reports concerning the capital market, except:
      - any bank or trust company;
      - any journalist, reporter, columnist, editor, lawyer, accountant, teacher;
      - the publisher of any bona fide newspaper, news, business or financial publication of general and regular circulation, including their employees;

- any contract market;
- such other person not within the intent of this definition, provided that the furnishing of such service by the foregoing persons is solely incidental to the conduct of their business or profession.

(c) who undertakes the management of portfolio securities of investment companies, including the arrangement of purchases, sales or exchanges of securities.

d. The following Designated Non-Financial Businesses and Professions (DNFBPs) such as:

i. Jewelry dealers in precious metals/stones, who, as a business, trade in precious metals/stones;

i. Dealer refers to an individual or entity who buys and/or sells precious metals, precious stones, and/or jewelry in the course of its business activities. The purchases or sales of precious metals, precious stones, and/or jewelry, as referred to herein, exclude those carried out for, connected with, or for the purpose of extracting precious metals or precious stones from a mine, or cutting or polishing precious stones.

ii. Jewelry refers to finished goods deriving fifty percent (50%) or more of their value from jewels, precious metals or precious stones constituting, forming part of, or attached to said finished goods.

iii. Jewel refers to organic substances that have a market-recognized gem level of quality, beauty and rarity, such as pearl, amber and coral.

iv. Precious metals shall mean gold, silver, platinum, palladium, rhodium, ruthenium, iridium and osmium. These include alloys of precious metals, solders and plating chemicals such as rhodium and palladium plating solutions and potassium gold cyanide and potassium silver cyanide and silver cyanide in salt solution.

v. Precious stones shall mean diamond, ruby, emerald, sapphire, opal, amethyst, beryl, topaz, and garnet that are used in jewelry making, including those formerly classified as semiprecious stones. ii. Company service providers which, as a business, provide any of the following services to third parties:

(a) acting as a formation agent of juridical persons;

(b) 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;
(c) 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
(d) acting as (or arranging for another person to act as) a nominee shareholder for another person; and iii. Persons, including lawyers and accountants, who provide any of the following services:
    (a) managing of customer money, securities or other assets;
    (b) management of bank, savings or securities accounts;
    (c) organization of contributions for the creation, operation or management of companies; and
    (d) creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

Notwithstanding the foregoing, lawyers and accountants who are: (1) authorized to practice their profession in the Philippines; and (2) engaged as independent legal or accounting professionals, in relation to information concerning their clients, or where disclosure of information would compromise client confidences or the attorney-client relationship, are not covered persons. "Independent legal or accounting professional" are lawyers and accountants working in a private firm or as a sole practitioner who by way of business provides purely legal, notarial or accounting services to their clients.

MM. 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.

NN. 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.

OO. 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.

PP. 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.

QQ. Terrorist acts - refer to the following:

- Any act in violation of Section 3 or 4 of the HSA of 2007.
- 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.
- 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.

RR. 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.

SS. Monetary instrument refers to:

- Coins of currency of legal tender of the Philippines, or of any other country;
- Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property
- Drafts, checks, and notes;
- 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.
- Participation or interest in any non – stock, non – profit corporation
- 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;
- 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
- Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

TT. 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.

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:

- 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;
- Sources and/or beneficiaries of wire transfers are citizens of countries which are identified or connected with terrorist activities;
- Repetitive deposits or withdrawals that cannot be satisfactorily explained or do not make economic or business sense;
- Value of the transaction is grossly over and above what the client is capable of earning;
- Client is conducting a transaction that is out of the ordinary for his known business interests;
- Deposits by individuals who have no known connection or relation with the account holder;
- Client is receiving remittances from a country where none of his family members is working or residing;
- Client was reported and/or mentioned in the news to be involved in terrorist activities;
- Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;
- 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;
- 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;
- The NGO/NPO does not appear to have expenses normally related to relief or humanitarian efforts;
- The absence of contributions from donors located within the country of origin of the NGO/NPO;
- The volume and frequency of transactions of the NGO/NPO are not commensurate with its stated purpose and activity.

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 – Customer Data Sheet (Individual)
Appendix B – Customer Data Sheet (Corporate)
Appendix C – Client Assessment Form

CHAPTER THREE – DESCRIPTION OF MONEY LAUNDERING

Money Laundering – Money laundering is the processing of the proceeds of a crime to disguise their origin. It is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the AMLA, so that they appear to have originated from a legitimate source.

Money laundering is committed by:

A. Any person who, knowing that any monetary instrument 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 Money-Laundering - The process of money laundering generally comprises three (3) stages during which there may be numerous transactions that, could alert a covered institution to the money laundering activity;

Placement – the physical disposal of cash proceeds derived from illegal activity.

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.

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.

Because of the nature of the business relationships entered into and among clients and the Company, which are no longer predominantly cash-based, they are less conductive to the initial placement of criminally-derived funds other than financial industries such as banking. Most payments are made by way of checks from another financial institution; hence, it can be assumed that the first stage of money laundering has already been achieved. Nevertheless, the purchases by cash are not unknown and the risk of the business being used at the placement stage cannot be ignored. The business of the Company is most likely to be used at the second stage of money laundering i.e. the layering process, as it provides a potential avenue which may allow a dramatic alteration of the form of funds, from cash on hand to securities such as stock certificates, investment contracts, and evidences of indebtedness, bearer, and other negotiable instruments. Investment transactions incorporate an added attraction to the money launderer in that the alternative asset is normally highly liquid. The ability to

liquidate investment portfolios containing both lawful and illicit proceeds, whilst concealing the criminal source of the latter, combined with the huge variety of investments available, and the ease of transfer between them, offers the sophisticated criminal launderer an ideal route to effective integration into the legitimate economy. Due diligence must, therefore, be exercised to prevent the use of the Company as instrument for money laundering.

CHAPTER FOUR - BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

Money Laundering and Terrorist Financing Prevention Program (MLPP). The Company shall adopt a comprehensive and risk-based MLPP geared toward the promotion of high ethical and professional standards and the prevention of the Company from 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 these rules and designed according to the company' corporate structure and risk profile. 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. Where the Company has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, it shall adopt an institution-wide MLPP that shall be implemented on a consolidated basis.

The MLPP shall also be readily available in user-friendly form, whether in hard or soft-copy. The Company must put up a procedure to ensure an audit trail evidencing dissemination process for new and amended policies and procedures. The program shall embody the following at a minimum:

1. Detailed procedures of the covered institution's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, and these Rules, to wit:

    a. Customer identification process including acceptance policies and on-going monitoring process;
    b. Record keeping and retention;
    c. Covered transaction reporting; and
    d. Suspicious transaction reporting including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregated amounts breach the threshold. The ST reporting shall include a reporting chain under which a suspicious transaction will be processed and the

designation of a Board level or approved Committee who will ultimately decide whether or not the covered institution should file a report to the AMLC. If the resources of the covered institution do not permit the designation of a Committee, it may designate the compliance officer to perform this function instead provided that the Board of Directors is informed of his decision.

2. An effective and continuous anti-money laundering and countering of terrorist financing training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under these rules, the AMLA, as amended, its RIRR and their internal policies and procedures as embodied in the MLPP. The training program shall also include refresher trainings to remind these individuals of their obligations and responsibilities as well as update them of any changes in AML laws, rules and internal policies and procedures.

3. An adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed to assume sensitive banking functions;

4. An internal audit system

5. an independent audit program with written scope of audit that will ensure the completeness and accuracy of the information and identification documents obtained from clients, the covered and suspicious transaction reports submitted to the AMLC, and the records retained in compliance with these rules as well as adequacy and effectiveness of the training program on the prevention of money laundering and terrorism financing;

6. A mechanism that ensures all deficiencies noted during the audit and/or SEC regular or special examination are immediately corrected and acted upon;

7. Cooperation with the AMLC; and

8. Designation of an AML compliance officer, who shall at least be at senior officer level, as the lead implement or of the program within an adequately staffed Compliance Office. The AML compliance officer may also be the liaison between the Company, and the AMLC in matters relating to the Company's AML compliance. Where resources of the Company do not permit the hiring of an AML compliance officer, the Compliance Officer shall also assume responsibility of the former.

9. A mechanism where information required for customer due diligence and ML/TF risk management are accessible by the parent covered institution and information are freely shared among branches, subsidiaries, affiliates and offices located within and/or outside the Philippines. Exchange of information among branches, subsidiaries, affiliates, and offices located within and/or outside the Philippines shall

not be deemed a violation of Rule 9, Item C of the IRR as long as it is done within the group. The MLPP may require a potential and/or existing customer to sign a waver on the disclosure of information within the group; Provided, however, that covered persons should take measures to ensure that its officers and employees are aware of their respective responsibilities in maintaining the confidentiality of financial investigations, and that no officer or employee communicates to any person any information in relation to any request for details and documents by the AMLC in the course of its investigation.

10. Policies and controls procedures and monitoring mechanism for prevention of mitigation of ML/TF risks.

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 and mutual funds 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 and mutual funds 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 and mutual funds 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.

Updating of MLPP - The Manual shall be regularly updated **at least once every two (2) years** to incorporate changes in AML/CFT policies and procedures, latest trends in Money Laundering and Terrorist Financing typologies, and latest pertinent SEC issuances. Any revision or update in the Company Anti-Money Laundering Manual shall be likewise be approved by Board of Directors.

Checking of Covered Person's MLPP - Covered person shall make their MLPPs readily available for inspection during the onsite examination.

CHAPTER FIVE - CUSTOMER IDENTIFICATION

The Company shall obtain satisfactory evidence of the true and full identity, representative capacity, domicile, legal capacity, occupation or business purposes of clients, as well as other identifying information on those clients, whether they be occasional or usual, through the use of documents such as, but not limited to:

1. identity documents, such as passports, birth certificates, driver's licenses, employment identification cards, and other similar identity documents, which are verifiable from the institutions issuing the same;

   The identifying documents should provide evidence of true and complete name or names used, residential address, date of birth, nationality, office address and contact details. They should include at least one (1) identifying document bearing the photograph and signature of the client. The identifying document which are considered most reliable are official identity cards and passports. While identification documents that are easily obtained in any name e.g. medical cards, credit cards and student identification cards, may be used, they should not be accepted as the sole means of identification.

   Clients engaging in transactions with the Company shall present at least one (1) original official identity card with photo and signature. The clients shall submit the photocopy of identity card at the commencement of the relationship. For this purpose, the term "official identity card" shall refer to those issued by any of the following: the National Government of the Republic of the Philippines, its political subdivisions or instrumentalities, or government owned and controlled corporations, private entities or institutions supervised or regulated either by the BSP or SEC or IC.

   Passports issued by foreign governments shall be considered as prima facie identification documents of persons engaging in transactions with the Company.

2. Incorporation and partnership papers, for corporate and partnership accounts. These documents should be certified as true copies by the entity's Corporate Secretary;

3. Special authorizations for representatives, which must be verified, or signature authenticated and duly notarized;

4. Other pertinent and reasonable documents as may be deemed necessary under the prevailing circumstances.

In conducting customer due diligence, a risk-based approach shall be undertaken depending on the type of customer, business relationship, or nature of the product, transaction or activity.

Clients should be made aware of the Company's explicit policy that business transactions will not be conducted with applicants who fail to provide evidence of their identity, but

without derogating from the Company's obligations to report suspicious transactions. Where initial checks fail to identify the applicant, or give rise to suspicions that the information provided is false, additional verification measures should be undertaken to determine whether to proceed with the business. Details of the additional checks are to be recorded in writing.

The Company shall take further measures to verify the identity of the customer or the beneficial owner, as applicable, if during the business relationship, it has reason to doubt:

1. The accuracy of the information relating to the client's identify;
2. That the client is the beneficial owner; or
3. The client's declaration of beneficial ownership.

Unusual Transactions – The Company shall pay special attention to all unusually large transactions or unusual pattern of transactions.

Acquisition by Covered Institution of the Business of Another Covered Institution - When the Company acquires the business of another financial sector company or covered institution, either in whole or as product portfolio, it is **not** necessary for the identity of all existing customers to be re-identified, provided that:

1. All customer account records are acquired with the business; and
2. Due diligence inquiries do not raise any doubt as to whether the anti-money laundering procedures previously adopted by the acquired business have satisfied Philippine requirements.

Conduct of Face-to-Face Contact. No new accounts shall be opened and created without face-to-face contact. The Company shall conduct face-to-face contact at the commencement of the relationship, or a reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business and the risks involved; Provided, that money laundering risks are effectively managed.

Face-to-face contact through the use of Information and Communication Technology shall be allowed provided the Company is in possession of and has verified the identification documents of the client prior to the interview and that the entire procedure is documented.

Third Party Reliance. The Company may rely on a third party to perform customer identification including face-to-face contact, or customer due diligence requirement as long as the intermediary or third party relied upon are considered as covered institution

as defined under 2018 AML/CFT guidelines, or any other guidelines or rules issued by the BSP or IC, or as defined and identified by foreign jurisdiction in so far as covered institutions in their respective jurisdiction is concerned.

The following criteria shall be considered in performing a third party reliance:

1. Third Party is a covered institution specifically defined by these Rules and as generally defined by AMLA, as amended, and its RIRR – The Company may rely on the identification process conducted by this third party provided that the Company shall obtain from the third party a written certification containing the following:

    a. The Third Party has conducted the requisite customer identification requirements in accordance with these Rules and its own MLPP including the face-to-face contact requirement to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and

    b. The relying Company shall have the ability to obtain identification documents from the Third Party upon request without delay.

2. Third Party is a financial institution operating outside the Philippines but conducts business similar to the covered institutions– All the contents required in the certification shall apply with the additional requirement that the laws of the country where the third party is operating has equal or more stringent customer identification process requirement and that it has not been cited in violation thereof. It shall, in addition to performing normal due diligence measures, do the following:

    a. Gather sufficient information about the third party and the group to which it belongs to understand fully the nature of its business and to determine from publicly available information the reputation of the institution and the quality of supervision, whether it has been subject to money laundering or terrorist financing investigation or regulatory action;

    b. Document the respective responsibilities of each institution; and

    c. Obtain approval from senior management at inception of relationship before relying on the third party.

3. The customer identification program of the third party intermediary is similar to or is equivalent to the customer identification program of the Company.

4. Ultimate responsibility for customer and/or beneficial owner identification and verification remains with the Company relying on the intermediaries or third parties.

In cases of high risk customers, the covered person relying on the third person shall also conduct enhanced due diligence procedures.

Outsourcing the Conduct of Customer Identification. – The Company may outsource the conduct of customer identification, including face-to-face contact, to a counter-party, intermediary or agent. The outsource, counter-party or intermediary shall be regarded as agent of the covered person – that is, the processes and documentation are those of the covered person itself. The ultimate responsibility for identifying the customer and keeping the identification documents remains with the Company. The Company outsourcing the conduct of customer identification including face-to-face contact, shall ensure that the employee or representative of the counter-party, intermediary or agent undergo equivalent training program as that of the Company's own employees undertaking similar activity.

Fictitious/Prohibited Accounts - The Company shall maintain accounts only in the name of the account holders. They shall not open or keep anonymous accounts, fictitious name accounts, incorrect name accounts, numbered accounts and other similar accounts. Any attempt of the prospective client to open an account under such name shall be politely declined by the front liner by explaining the restriction of RA 9160.

Personal Customers
The Company shall obtain from all individual clients the following information:

1 complete name and names used;
2 present address;
3 permanent address;
4 mailing address;
5 date and place of birth;
6 nationality;
7 contact details such as phone number, email address and mobile phone number (avoid pre-paid cellular phone numbers);
8 nature of work, name of employer or nature of self-employment or business;
9 Tax Identification Number, Social Security System number or Government Service and Insurance System number;
10 specimen signature;
11 sources of funds, whenever necessary;

- GSIS e-Card
- SSS Card
- Senior Citizen Card
- OWWA ID
- OFW ID
- Seaman's Book
- Alien Certification of Registration/ Immigrant Certificate of Registration
- Government Office and GOCC ID (e.g. AFP, HDMF IDs)
- Certification from NCWDP
- DSWD Certification
- IBP ID
- School ID (if student)
- Company ID issued by private entities or institutions registered with or supervised or regulated either by the BSP, SEC or IC

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

Risk Assessment/Risk Profiling of Customers

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

Reduced Due Diligence – If the risk of money laundering or financing of terrorism is lower based on the Company's assessment, and if information on the identity of the customer and the beneficial owner is publicly available, or adequate checks and controls exist elsewhere in national systems, it could be reasonable for covered institutions to apply simplified or reduced customer due diligence measures when identifying and verifying the identity of the customer, the beneficial owner and other parties to the business relationship. Examples of customers where simplified or reduced customer due diligence measures could apply are:

1 Financial institutions where they are subject to requirements to combat money laundering and financing of terrorism consistent with the Financial Action Task Force (FATF) Recommendations and are supervised for compliance with those controls.
2 Public companies that are subject to regulatory disclosures requirements.
3 Government institutions and its instrumentalities

Whenever reduced due diligence is applied in accordance with the Company's customer acceptance policy, the following rules shall apply:

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.

Reduced due diligence shall not be applied if there is suspicion of ML/TF.

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
The Company shall examine, as far as reasonably as possible, the background and purpose of all complex, unusual large transactions and/ or unusual patterns of transactions which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Where the risks of ML/TF are higher, the Company is required to conduct EDD measures consistent with the risks identified. Whenever EDD is applied to customers as required by these Rules or by the Company's customer acceptance policy, or where the risk of ML/TF is higher, the Company shall,

in addition to profiling of customers and monitoring of their transactions, do the following:

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:

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

   In cases of individual customers,

   a. supporting information on the intended nature of the business relationship/source of funds/source of wealth;
   b. reasons for the intended or performed transactions;
   c. list of companies where he is a director, officer or stockholder;
   d. list of banks where the individual has maintained or is maintaining an account, and
   e. other relevant information available through public databases or internet.

   For entities assessed as high-risk customers, such as shell companies;

   a. prior or existing bank references;
   b. 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;
   c. volume of assets, other information available through public databases or internet or supporting information on the intended nature of the business relationship, source of funds or source of wealth; and
   d. reasons for the intended or performed transactions.

ii. Conduct validation procedures on any or all of the information provided

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

iv. Conduct enhanced ongoing monitoring of the business relationship

v. 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 Fund Operations, 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.

Minimum Validation Procedures Enhanced Due Diligence

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.

Failure to Conduct/Complete EDD and Tipping off.

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.

If the company forms a suspicion that transactions relate to ML/TF, it should take into account the risk of tipping off when performing the CDD process. If the company reasonable believes that performing the CDD process will tip off the customer or potential customer, it may choose not to pursue that process and should file an STR. The company should ensure that all employees are aware of, and sensitive to, these issues when conducting the CDD.

High Risk Costumers

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.

Politically Exposed Person

The Company shall endeavor to establish and record the true and full identity of PEPs, as well as their immediate family members and entities related to them. The Company shall also establish a policy on what standard of due diligence will apply to them taking into consideration their position and the risks attendant thereto.

Single Proprietorships, Corporations, Stocks or Non-Stock and Partnerships.

The Company shall determine and identify the legal existence and structure of the client and in the event of doubt as to identity of the corporation or its directors, the Company shall verify from the appropriate agency (city/municipal government, SEC, DTI, BFAD, etc.) proof of incorporation, legal structure, including information concerning the customer's name, address, directors, principal officers and provisions regulating the power behind the entity. Corporate applicants must be checked with the Negative File Information System, if necessary.

The Company shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities as well as the stockholders/partners/owners, directors, officers and authorized signatory of these entities. It shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in the process of being, dissolved, struck-off, wound-up, terminated, or otherwise placed under receivership or liquidation.

Documentary Requirements

The following relevant documents shall be obtained in respect of corporate/other business applicants which are regulated in the Philippines:

For Single Proprietorships

The Company shall require the clients to present the original and submit certified true copies of the following:

1. Certificate of Registration(COR) issued by the Department of Trade and Industry (DTI); or
2. Application papers with the Department of Trade and Industry

For Partnerships

1. Certificate of Registration issued by the Securities and Exchange Commission
2. Articles of Partnership / Certificate of Partnership
3. Secretary's Certificate of Partners' Resolution authorizing the signatories and opening of account

For Corporation

1. Certificate of Registration issued by the Securities and Exchange Commission
2. Articles of Incorporation
3. By-Laws
4. Latest General Information Sheet which lists the names of directors
5. Secretary's Certificate of Board Resolution authorizing the signatories and opening of account
6. Signed application forms or account opening authority containing specimen signatures or biometrics of the authorized signatory.
7. Principal business address
8. Source of funds and nature of business
9. Contact numbers of the entity and authorized signatory/ies.

For Legal Arrangement (e.g. TRUST)

1. Name of legal arrangement and proof of existence
2. Address and country of establishment
3. Nature, purpose and objects of the legal arrangement
4. 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
5. Description of the purpose/activities of the legal arrangement
6. Expected use of the account and
7. Amount, Number, Type, Purpose and Frequency of the transaction expected

The originals or certified true copies of all of the foregoing documents shall be required to be submitted and compared with the photocopies to confirm the authenticity of the documents.

The Company shall obtain from all single/corporate clients the following information:

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

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.

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.

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.

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 shall be made.

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

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

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.

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.

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 Fund Operations. On a monthly basis, Fund Operations shall review the completeness of KYC Reliance Certifications and make a follow-up, where necessary from the concerned Metrobank branch or unit.

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.

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.

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.

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.

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.

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.

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.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.

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.

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.

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.

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.

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.

Trust, Nominee and Fiduciary Accounts

The Company shall establish whether the applicant for business relationship is acting on behalf of another person as a trustee, nominee or agent. The Company should obtain competent evidence of the identity of such agents and authorized signatories, and the nature of their trustee or nominee capacity and duties.

Where the Company entertains doubts as to whether the trustee, nominee or agent is being used as a dummy in circumvention of existing laws, it shall immediately make further inquiries to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, the Company shall consider whether to proceed with the business, bearing in mind the "Know-Your-Customer" principle. If the Company decides to proceed, it shall record any misgiving and give extra attention to monitoring the account question.

Where the account is opened by a firm of lawyers or accountants, the Company should not be precluded from making reasonable inquiries about transactions passing through the subject accounts that give cause for concern or from reporting those transactions if any suspicion is aroused. If a money laundering Suspicious Transaction Report is made to the Council in respect of such clients' accounts, the Council will seek information directly from the lawyers or accountants as to the identity of its client and the nature of the relevant transaction, in accordance with the powers granted to it under the Act and other pertinent laws

Transactions Undertaken on Behalf of Account Holders or Non-Account Holders

Where transactions are undertaken on behalf of account holders, the Company shall take particular care to ensure that the person giving instructions is authorized to do so by the account holder.

Transactions undertaken for non-account holders demand special care and vigilance. Where the transaction involves significant amounts, the customer should be asked to produce positive evidence of identity including nationality, especially in case where the client is not a Filipino, the purposes of transaction and the source(s) of the funds.

Shell Company/ Shell Bank / Bearer share entities

The company shall undertake banking relationship with a shell company with extreme caution and always apply enhanced due diligence on both the entity and its beneficial owner/s.

Because of the dubious nature of shell banks, FAMI shall refuse to deal, 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.

Bearer share entities refer to those juridical entities where the ownership is accorded to those who possess the bearer share certificate. FAMI shall conduct enhanced due diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account. These entities shall be subject to ongoing monitoring at all times and the list of stockholders and/or beneficial owners shall be updated within thirty (30) days after every transfer of ownership and the appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

Wire/Fund Transfers

Because of the risk associated with dealing with wire/fund transfers, where a covered person may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, it shall establish policies and procedures designed to prevent it from being utilized for that purpose which shall include, but not limited to, the following:

a. The beneficiary institution shall not accept instructions to pay-out wire/fund transfers to non-customer beneficiary, unless it has conducted

the necessary customer due diligence to establish the true and full identity and existence of said beneficiary. Should the originator and beneficiary be the same person, the beneficiary institution may rely on the customer due diligence conducted by the originating institution subject to the rules on Third Party reliance to be promulgated by the Supervising Authorities, treating the originating institution as Third Party as herein defined;

b. The originating institution shall not accept instructions to wire/fund transfer from a non_customer originator, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said originator;

c. In cross border wire/fund transfers, if the originator is a high risk customer as herein described, the beneficiary institution shall conduct enhanced due diligence under Rule 9.a.9.a on the beneficiary and the originator. 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 beneficiary institution shall refuse to effect the wire/fund transfers or the pay_out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant;

d. Whenever possible, manually initiated fund transfer (MIFT) instructions should not be the primary delivery method. Every effort shall be made to provide customer with an electronic banking solution. However, where MIFT is utilized, the Supervising Authorities shall issue pertinent rules on validation procedures;
    i. Prior to the bank accepting from a customer a manually initiated funds transfer request the customer must execute and sign an agreement which preferably is part of the account opening documentation, wherein are outlined the manual instruction procedures with related security procedures including customer agreement to accept responsibility for fraudulent or erroneous instructions provided the bank has complied with the stated security procedures.
    ii. It is mandatory that written MIFT instructions are signature verified. In addition, one (1) of the following primary security procedures must be applied: a recorded callback to the customer to confirm the transaction instructions, or test word arrangement/ verification. The callback or test word requirement may be substituted by any of the following

validity checks: use of a controlled PIN or other pre-established code; sequential numbering control of messages; pre-established verifiable forms; same as prior transmissions; standing/predefined instructions; or value for value transactions.

iii. It is mandatory that MIFT instructions are signature verified and the device be located in a secured environment with limited and controlled staff access which permits visual monitoring. lf monitoring is not possible, the device must be secured or programmed to receive messages into a password protected memory. MIFT transactions below a certain threshold (approved by the President/Country Manager (for branches of foreign banks) or Business Risk Manager may be processed with the mandatory procedure described above and an enhanced security procedure such as (a) a recorded callback to the customer to confirm the transaction instructions and/or (b) test word arrangement/verification, and/or (c) utilization of secured forms that incorporate verifiable security procedures such as watermarks or codes, and/or (d) transmission encryption. iv. Telephone callback numbers and contacts must be securely controlled. The confirmation callback is to be recorded and made to the signatory/ies of the customer's individual account/s. For commercial and company accounts the callback will be made to the signatory/ies of the account or, if so authorized, another person designated by the customer in the MIFT agreement. The party called is to be documented on the instructions. The callback must be made by someone other than (a) the person receiving the original instructions and (b) effecting the signature verification.

e. Cross border and domestic wire/fund transfers and related message not exceeding a threshold amount to be determined by the Supervising Authorities or its equivalent in foreign currency shall include accurate and meaningful originator and beneficiary information. The following information shall remain with the transfer or related message through the payment chain:
   - the name of the originator;
   - the name of the beneficiary; and
   - an account number of the originator and beneficiary, or in its absence, a unique transaction reference number.

f. For cross border and domestic wire/fund transfers and related message amounting to P50,000 or its equivalent in foreign currency, the following information accompanying all qualifying wire transfers should always contain:

- the name of the originator;
- the originator account number where such an account is used to process the transaction;
- the originator's address, or national identity number, or customer identification number, or date and place of birth;
- the name of the beneficiary; and
- the beneficiary account number where such an account is used to process the transaction.

For domestic wire transfers, the originating institution should ensure that the required information accompanies the wire transfers, unless this information can be made available to the beneficiary institution and relevant authorities by other effective means. In the latter case, the ordering institution shall include only the account number or a unique identifier within the message or payment form which will allow the transaction to be traced back to the originator or beneficiary. Originating institutions are required to provide the information within three (3) working days from receiving the request either from the beneficiary institution or from relevant authorities or agencies.

Should any wire/fund transfer amounting to the threshold amount to be determined by the Supervising Authorities or more or its equivalent in foreign currency be unaccompanied by the required originator and beneficiary information, the beneficiary institution shall exert all efforts to establish the true and full identity and existence of the originator by requiring additional information from the originating institution or intermediary institution. It shall likewise apply enhanced due diligence under Rule 9.a.9.a to establish the true and full identity and existence of the beneficiary. 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 beneficiary institution shall refuse to effect the wire/fund transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

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. The Company shall keep current and accurate all material information with respect to customers by regularly conducting verification and update of customer information.

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 Fund Operations 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 SIX – RECORD KEEPING

The Company shall prepare maintain documentation on its customer relationships and transactions, including customer identification and verification, such that:

1. Requirements of the AMLA, as amended, are fully met;
2. Any transaction effected via the Company can be reconstructed and from which the AMLC, and/ or the courts will be able to compile an audit trail for suspected money laundering, when such a report is made to it;
3. The Company can satisfy within a reasonable time any inquiry or order from the AMLC as to disclosure of information, including without limitation, whether a particular person is the customer or beneficial owner of transactions conducted through the covered institutions.

Periods of Retention

The following document retention periods shall be followed:

1. All records of all transactions of the Company, especially customer identification records, shall be maintained and safely stored in an easily accessible place for five (5) years from the dates of transactions.

2. With respect to closed accounts, the records on customer identification, account files and business correspondences, shall be preserved and safely stored for at least five (5) years from the dates when they were closed.

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

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

- 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)

4. SRC Rule 52.1.1 Books and Records Keeping Rule and Records Retention Rule of the 2015 Implementing Rules and Registration of the SRC continue to be in full force and effect.

Records Relating to Pending Case

If the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.

Forms of Records

Transaction documents (domestic or international records) may be retained as originals or copies, on microfilm, or in electronic form, provided that such forms are admissible in court, pursuant to the Revised Rules of Court and the E-Commerce Act and its Implementing Guidelines.

Digitization of Customer Records

The Company shall comply with the Guidelines on Digitization of Customer Records as promulgated by the AMLC in accordance with the terms thereof, as may be applicable.

Persons Responsible for Safekeeping of Records

The company 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 these Rules. They shall have the obligation to make these documents and records readily available without delay during AMLC/SEC regular or special examinations.

1. The Funds Operations 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.

CHAPTER SEVEN – REPORTING OF COVERED ANS SUSPICIOUS TRANSACTIONS

Covered Transaction Report (CTR) - The company shall file a Covered Transaction Report (CTR) with the AMLC involving any transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (Php500,000.00) per single transaction within one (1) banking day/trading day.

Suspicious Transaction Report (STR) The Company shall file a Suspicious Transaction Reports (STR) with the AMLC for transactions, regardless of the amounts transactions, 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 AMLA;

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 Company.

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

7. Any transaction that is similar or analogous to any of the foregoing.

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

Transaction Reporting – The company shall report to the AMLC all covered transactions and suspicious transactions within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

For suspicious transactions, "occurrence" refers to the date of determination of the suspicious nature of the transaction, which determination should be made not exceeding ten (10) calendar days from the date of transaction. However, if the transaction is in any way related to, or the person transacting is involved in or connected to, an unlawful activity or money laundering offense, the 10-day period for determination shall reckoned from the date the company knew or should have known the suspicious transaction indicator.

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.

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.

Suspicious Transaction Reporting Procedures

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

1. The business unit front liner or Operations personnel who identified a suspicious transaction shall refer the suspected account to the Department , Division 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.

Transaction that are both Covered and Suspicious – Should a transaction be determined to be both a covered and a suspicious transaction, the company shall report the same as a suspicious transaction.

Attempted Suspicious Transactions. – The Company shall file STR for suspicious attempted transactions. An attempted transaction is one that a client intended to conduct and made overt acts to do so. Such overt acts include entering into negotiations or discussions to conduct the transaction and involves definite measures to be undertaken by the SEC covered institution or the client. In order for an attempted transaction to be reported as an attempted suspicious transaction, there must be reasonable grounds to suspect that said attempted transaction is related to money laundering or terrorist financing or when any of the circumstances enumerated in Section 7.3 hereof exists.

Reporting of Customer's Unlawful Activities

(a) Where any employee or personnel, director or officer of the Company knows that the client has engaged in any of the predicate crimes under the Act, the matter must be promptly reported to the Reporting Officer.

(b) If there are reasonable grounds to the suspect that the customer has engaged in an unlawful activity, the Reporting Officer/Compliance Officer/Anti-Money Laundering Compliance Committee , on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the AMLC through the Chairman of the Board unless the Reporting Officer / Compliance Officer / Committee considers, and records an opinion, that such reasonable grounds do not exist.

The Company shall maintain a complete file on all transactions that have been brought to the attention of the Reporting Officer (s) including transactions that are not reported to the Council.

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.

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.

Confidentiality of CTR and STR

The company, its directors, officers and employees shall not warn customers when information relating to them is being reported to the Council or communicate, directly or indirectly, such information to any other person other than the Council. Any violation of this confidentiality provision shall render them liable for criminal, civil and administrative sanctions under the AMLA.

When reporting CTs and STs to the AMLC, the company, directors, officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction report was made, the contents thereof, 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.

Safe Harbor Provision

No administrative, criminal or civil proceedings shall lie against any person for having made a CTR or an STR in the regular performance of his duties in good faith, whether or not such

reporting results in any criminal prosecution under the AMLA, as amended, its RIRR or any other Philippine law. The company, its directors and employees shall likewise not be liable for any loss arising out of such disclosure, or any act or omission, in relation to the fund, property or investment in consequence of the disclosure, where such is made in good faith and in the regular performance of their duties under the Act.

CHAPTER EIGHT – COMPLIANCE

The Compliance Officer – The company shall appoint a senior officer as the Compliance Officer who will be in charge of the implementation of its Operating Manual and the application of the internal programs and procedure, including customer identification policies and procedures, proper maintenance of records, reporting of covered and suspicious transaction to the AMLC, and training of employees.

A Compliance Officer shall be:

1. A senior officer with relevant qualification and experience to enable him to respond sufficiently well to inquiries relating to the relevant person and the conduct of its business;
2. Responsible for establishing and maintaining a manual of compliance procedures in relation to the business of the company;
3. Responsible for ensuring compliance by the staff of the company with the provisions of the AMLA, as amended, its Implementing Rules and Regulations, and the company's manual of compliance Procedures established under Internal Controls and Procedures.
4. Responsible for disseminating to its board, officers and all employees memorandum circulars, resolutions, instructions, and policies issued by the AMLC and by the Commission in all matters relating to the prevention of money laundering;
5. The liaison the company and the AMLC in matters relating to compliance with the provisions of the AMLA and its Implementing Rules and Regulations;
6. Responsible for the preparation and submission to the AMLC written reports on the company's compliance with the provisions of the AMLA and its Implementing Rules and Regulations, in such form as the AMLC may determine, and within such period as the Commission may allow in accordance with the AMLA, as amended;
7. Responsible for organizing training sessions for the staff on issues related to AML/CFT compliance, including providing guidance to the staff on how to avoid "tipping off" if any ST is filed or if any transaction or set of circumstances is flagged internally as potentially suspicious;

8. Responsible for analyzing transactions to determine whether any are subject to reporting according to the indicators of suspicious transactions mentioned in the AMLA, relevant SEC regulations and this manual, and undertaking closer investigation of transactions when necessary;
9. Responsible for reviewing all internal reports of potentially suspicious transactions for their completeness and accuracy;
10. Responsible for preparing STRs and ensuring their timely filing with the AMLC;
11. Responsible for keeping records of internally and externally reported suspicious transactions;
12. Responsible for remaining informed of the national and international developments on money laundering and terrorist financing and making suggestions to the board of directors and management for upgrading the institution's policies and procedures in light of these developments and;
13. Responsible for periodically reporting information on the institution's efforts to combat money laundering and terrorist financing to the board, and recommending changes in the institution's policies or procedures when deemed necessary.

Adviser Regarding AML matters – The company shall appoint one or more senior officers, or an appropriate unit, to advise its management and staff on the issuance and enforcement of in-house instructions to promote adherence to the AMLA, as amended, the RIRR, its MLPP, including personnel training, reporting of covered and suspicious transactions, and generally, all matters relating to the prevention of money laundering.

Responsibility of Covered Institution and its Board - The ultimate responsibility for proper supervision, reporting and compliance under AMLA, as amended, its RIRR shall rest with the company and its board of directors.

CHAPTER NINE – INTERNAL CONTROL AND PROCEDURES

The Company shall establish and implement internal control procedures aimed at preventing and impeding money laundering. Such procedures shall, among others things, ensure that the Company and its employees are aware of the provision of the law, its implementing rules and regulations, as well as all reportorial and compliance control and procedures appurtenant thereto.

Coverage of Internal Controls Policies and Procedures - Policies and procedures should cover, among others;

1. Account opening and customer identification, indcluding requirements for proper identification;
2. Maintenance record;
3. Compliance with the requirement of the AMLA, as amended, is Revised Implementing Rules and Regulations, and all Circulars issued by the Commission and the AMLC;
4. Cooperation with the Commission and other relevant Authorities.

Written Internal Reporting Procedures – Company shall establish written internal reporting procedures which shall:

(a) Enable all its directors, officers, employees, all key staff to know to whom they should report any knowledge or suspicion of money laundering activity;

(b) Ensure that there is a clear reporting chain under which suspicions of money laundering activity will be passed to the Compliance Officer, in accordance with the reporting procedures of the company;

(c) Require the Compliance Officer to consider any report in the light of all relevant information available for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering;

(d) Ensure that the Compliance Officer has reasonable access to any other information which may be of assistance in the determination as to whether or not a suspicious transaction report is to be filed;

(e) Require that, upon determination of the suspicious nature of the report, the information contained therein is disclosed promptly to the AMLC;

(f) Require the maintenance of a register of all reports made to the Council, as well as all reports made by its own staff relative to suspicious transactions, whether or not such were reported to the Council. 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.

CHAPTER TEN - INTERNAL AUDIT

Internal Audit Function and Reporting Line - The Internal Audit function associated with money laundering and terrorist financing should be conducted by qualified personnel who are independent of the office being audited. It must have the support of the Board of

Directors and Senior Management and have a direct reporting line to the Board or a Board level Audit Committee.

Frequency and Scope of Internal Audit - The Internal Audit shall, in addition to those specified by these rules, be responsible for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, CT and ST reporting and record keeping and retention, as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

Electronic AML/CFT Monitoring System - The internal audit shall include determination of the efficiency of the system's functionalities.

Reporting of Internal Audit Findings - The result of the internal audit shall be timely communicated to the Board of Directors and shall be open for scrutiny by SEC examiners in the course of the regular or special examination without prejudice to the conduct of its own evaluation whenever necessary. Results of the audit shall likewise be promptly communicated to the Compliance Office for its appropriate corrective action. The Compliance Office shall regularly submit reports to the Board to inform them of management's action to address deficiencies noted in the 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.

CHAPTER ELEVEN – TRAINING

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.

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.

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.

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 Compliance 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.

Training Program and Records of Trainings Conducted - The company's annual AML training program and records of all AML seminars and trainings conducted by the Company and/or attended by its personnel (internal or external), including copies of AML seminar/training materials, shall be appropriately kept by the compliance office/unit/department, and should be made available during periodic or special SEC/AMLC examination.

Cascading of Updates and New Requirements – The company shall ensure that all relevant personnel are informed in a timely manner of any new provisions, updates or changes in laws, as well as new, amended or updated Commission rules, regulations, guidelines and

circulars relating to money laundering and/or terrorist financing, and the internal procedures based on any of the foregoing. Training of any such new provisions, amendments, updates or changes shall be provided as necessary.

CHAPTER - TWELVE 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. 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.

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).

CHAPTER - THIRTEEN Notice Of Freeze Order (NFO)

1. Under the Implementing Rules and Regulations of Republic Act 9160:

1.1 NFO refers to an order issued by the Court of Appeals directing the Company to put on hold a stated balance/ amount of money against subject investment account. This is aimed to determine if the proceeds of investment account

subject of the freeze order is related to/ derived from an unlawful activity such as money laundering

1.2 Upon receipt of NFO, Company is required to perform certain actions with the period specified in NFO.

2. Receipt of NFO

2.1 Official receipt of NFO shall be centralized at the Compliance Unit.

i. All Freeze Orders (FO) shall be received and handled by Compliance Unit. Any other unit who is being served NFO or any other order from Court of Appeals related to the NFO shall immediately refer the bearer to the Compliance Unit Head, or in her/his absence, to Compliance Officer who shall **stamp the date and time the NFO was received**.

ii. Any personnel who is being served NFO or any order from Court of Appeals related to the NFO during or after office hours shall refer the bearer to the Head of Compliance Unit or in her/his absence, to Compliance Officer.

iii. All personnel are prohibited from calling and/ or informing the customer/ accountholder subject of the FO. Any need for clarification on the FO shall be directed to, and addressed by, Compliance Unit.

3. Freeze Order Advisory

Within one (1) hour from the receipt of the FO, Compliance Unit shall issue via email a Freeze Order Advisory (Exhibit A) to all concerned units as follows:

ii. Corporate Service and Finance
iii. Technology Department
iv. Fund Operations
v. Partnership Distribution
vi. Direct Sales
vii. Special Markets and Training
viii. Legal
ix. President
x. Members of AMLC Committee

In the email advisory, Compliance Unit shall instruct ITD to immediately generate a summary report of accounts with outstanding balances that are listed in the FO. The

summary report shall specify pertinent and relevant information on all frozen accounts, including related accounts or materially-linked accounts. TMD shall forward the generated report to Fund Operations who shall verify and certify the completeness of the content of the report.

Fund Operations shall submit the report to Compliance Unit, within three (3) hours from receipt of the Freeze Order Advisory from Compliance Unit.

4. Implementation of Freeze Order

Following issuance of the FO Advisory by Compliance Unit:

1. Account Name in the FO is Listed under FAMI-Frozen Account:

   Within three (3) hours from receipt of the advisory from Compliance Unit, the **Sales Support shall**:

   a. Determine whether the person subject to FO is the same person as its customer by checking the account name, account number and address indicated in the FO Advisory are the same as the account details of its customer appearing in the system or other manual database or KYC documents.
   For cases when the address of the person specified in the FO is different from the details in the database, confirm that the customer is the same person subject of the FO by coordinating with Compliance Unit for clarification with Anti-Money Laundering Council (AMLC).

   b. If the person subject of the FO has no outstanding investments with FAMI, inform Compliance unit of the same via email immediately.

   c. If details are exactly the same, immediately freeze the account specified in the FO.

   d. Identify and freeze other accounts that are under the name of the person specified in the FO even if the account numbers are not specified therein. Identification of accounts shall include closed accounts.

   e. Immediately upon freezing accounts, accomplish the Instruction Slip (IS) to transfer the account under FAMI-Frozen Account, and forward to Fund Operations for handling and execution.

   f. Prepare IS and tag customer subject of the FO as “High Risk” and update the Customer Assessment Form (CAF).

g. Immediately provide the following information to Compliance Unit via email:

1. Account Number(s)
2. Account Name(s)
3. Status of Account as of FO (e.g. still for verification, repetitive, and others)
4. Date of account closure (for Closed Account)
5. Balance of Account as of FO
6. Date and time of freezing the account(s)
7. Name and Position of Officer who tagged the account(s)
8. For related/ materially linked account, basis for determining account is related/materially linked account i.e. Description of transactions/ movements of the account before the freeze; Origins/ destinations of transactions/ movements of the accounts.

Submit to Compliance Unit original copies of KYC and transaction documents.

Send a notice and a copy of FO to the customer subject of the FO via courier within one (1) banking day after execution of the FO.

Send scanned copies of the notice and proof of dispatch to Compliance Unit via email.

Copy of the letter and the evidence of receipt by client (i.e. transmittal slip/ acknowledgement receipt) or sending to the client via registered mail shall be filed in the client's respective KYC folder.

Additional transactions made to frozen accounts shall not be allowed.

Compliance Unit shall:

Prepare the "Written Return" on the FO and submit via email to Legal for review and confirmation, **cc**: All Listed Units

Upon receipt of confirmation from Legal, print the "Written Return" and **personally** submit to the Court of Appeals and AMLC within the prescribed Turn-Around Time (TAT):

Account for Freezing	TAT
Account number is specified in the FO	Within 24 hours from receipt of the FO

Account number is not specified in the FO but the name of the account holder is specified in the FO	Within 48 hours from receipt of the FO

Monitoring of Accounts Under FO

Freeze status of the accounts shall:

Be effected within the period specified in NFO unless extended by the Court of Appeals.

Not be lifted even after the lapse of the specified period without official confirmation from Compliance Unit.

Compliance Unit shall write AMLC two weeks before the expiry of the FO to obtain confirmation and status of the expiring FO.

Custody of Documents of Accounts Subject of FO

Fund Operations shall be the custodian of original KYC and transaction documents in case of the accounts are covered by Freeze Order, Inquiry Order, Preservation Order or any Money Laundering related court cases. These shall be safe kept in the Stock Room maintained by the Administration.

Fund Operations shall prepare transmittal slip and turnover original copies of KYC and transaction documents of accounts subject of the FO to Administration (5) days from receipt of NFO advice. Fund Operations shall keep the transmittal slip and maintain copies of the documents for reference and file.

Lifting of Freeze Order

The lifting of the NFO shall originate from the Court that issued the FO. The FO shall be lifted only upon receipt of official confirmation from the AMLC.

Compliance Unit shall do the following:

- write the AMLC two (2) weeks before the expiry of the NFO to obtain status of the NFO
- upon receipt of the confirmation from the AMLC, shall forward via email the confirmation to Legal to validate the authenticity of such notice of lifting
- after validation of authenticity of the notice of lifting of the NFO, shall provide a copy of notice via email to recipients listed above

Accounts lifted after the FO shall be immediately closed unless otherwise justified and approved by Head of Online Sales/ Institutional Sales Department/ President.

Sales Support upon receipt of the email, shall prepare an IS to close or unfreeze the accounts and submit to Fund Operations for the handling and execution.

Account not closed shall be tagged as High Risk by Fund Operations subject to proper monitoring and due diligence.

Sales Support shall send a letter to the clients regarding the lifting of the NFO together with a copy of the notice of lifting. Copy of the letter and evidence of receipt by the client, i.e. transmittal slip or sending to the client via registered mail shall be filed in the client's respective documentation folders.

Compliance Unit shall submit a report to the AMLC Committee and Board of Directors of accounts not closed but was subject of a NFO which was subsequently lifted.

CHAPTER FOURTEEN – SANCTIONS AND PENALTIES

Any violation of the requirements set forth in this manual shall be considered as a violation of the Rules, Regulations or Orders promulgated by the Commission, and shall be penalized in accordance with Section 54.1.(a) in relation to Section 54.1(a)(i), (ii) and (v) of the Securities and Regulations Code without prejudice to the penalties that may be imposed by the AMLC RIRR. Accordingly, the Commission may imposed any or all of the following sanctions as may be appropriate in the light of the facts and circumstances:

a. Suspension or revocation or any registration for the offering of securities;
b. A fine of no less than Ten Thousand Pesos (Php 10,000) nor more than One Million Pesos (Php 1,000,000) plus not more than Two Thousand Pesos (Php 2,000) for each day of continuing violation;
c. Other penalties within the power of the Commission to impose.

Criminal Actions and Criminal Liability – The imposition of the foregoing administrative sanction shall be without prejudice to the filing of criminal charges against the individuals responsible for the violation, in accordance with Section 54.2 in relation to Section 73 of the Securities Regulations Code.

Manner of Imposition of Penalties – The penalties shall be imposed in a manner that is effective, proportionate and dissuasive.

(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.