Securities and Exchange Commission
PHILIPPINES

SEC Memorandum Circular No. 16
Series of 2018

TO : **ALL SEC COVERED INSTITUTIONS**

SUBJECT : **2018 GUIDELINES ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM FOR SEC COVERED INSTITUTIONS *("2018 AML/CFT GUIDELINES")***

****

The Securities and Exchange Commission ("SEC", "Commission"), in conformity with the provisions of Republic Act No. 9160 (Anti-Money Laundering Act of 2001), as amended, its Revised Implementing Rules and Regulations (RIRR), Republic Act No. 10168 (Terrorism Financing Prevention and Suppression Act of 2012), its Implementing Rules and Regulations, and taking into consideration international best practices in the implementation and enforcement of the Anti-Money Laundering (AML) and the Combating the Financing of Terrorism (CFT) regimes, hereby issues this *"2018 Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for SEC Covered Institutions"* ("2018 AML/CFT Guidelines").

SECTION 1. All covered institutions as defined in this 2018 AML/CFT Guidelines are required to amend their respective Money Laundering and Terrorist Financing Prevention Program (MLPP) to conform to the attached 2018 AML/CFT Guidelines.

SECTION 2. All covered institutions shall, within six (6) months from the effectivity of these Guidelines, submit their revised MLPP to the Commission through the Operating Departments having supervision over such covered institutions copy furnished the Anti-Money Laundering Division (AMLD) of the Enforcement and Investor Protection Department (EIPD). The revised or updated MLPP shall be approved by the board of directors, or the country/ regional head or its equivalent for local branches of foreign covered institutions and shall embody the principles and policies enunciated in these Guidelines.

Covered institutions which have not submitted their respective programs shall prepare the same in accordance with the 2018 AML/CFT Guidelines and submit said MLPP within the period specified above.

SECTION 3. The attached 2018 AML/CFT Guidelines shall serve as guide to covered institutions in revising and reformulating their own MLPP, taking into consideration their respective corporate structure. Accordingly, all covered institutions are directed to revise their MLPP and to provide therein specific procedures and policies that would achieve the ends prescribed in the 2018 AML/CFT Guidelines.

Published:
Manila Bulletin, November 8, 2018
Manila Standard, November 8, 2018

SECTION 4. A covered institution which fails to submit a revised MLPP within the prescribed period shall be subject to a penalty of Five Hundred Pesos (P500.00) per day of delay until the revised MLPP has been submitted to the Commission.

SECTION 5. This Memorandum Circular shall take effect fifteen (15) days after its publication in two (2) national newspapers of general circulation and its posting in the Commission's website.

Pasay City, Philippines, 7 November 2018.

FOR THE COMMISSION:

EMILIO B. AQUINO
Chairperson

2018 GUIDELINES ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM FOR SEC COVERED INSTITUTIONS

The Securities and Exchange Commission ("SEC", "Commission") hereby issues this *"Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for SEC Covered Institutions"* pursuant to the authority granted to it under the Anti-Money Laundering Act of 2001 (AMLA) (Republic Act (RA) No. 9160), as amended and its regulatory and supervisory powers under the Securities Regulation Code ("SRC") (RA 8799), the Corporation Code of the Philippines (Batas Pambansa (BP) Blg. 68), Presidential Decree 902-A, as amended, the Investment Houses Law (Presidential Decree (PD) No. 129), the Investment Company Act (RA 2629), the Financing Company Act of 1998 (RA 8556), the Lending Company Regulation Act of 2007 (RA 9474) and other pertinent laws, rules and regulations administered and enforced by the Commission taking into consideration international best practices in the implementation and enforcement of the Anti-Money Laundering (AML) and the Combating the Financing of Terrorism (CFT) regimes.

CHAPTER 1
TITLE AND SCOPE

Section 1.1. Title. – These Guidelines shall be referred to as the *"SEC Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for SEC Covered Institutions"* or the *"2018 AML/CFT Guidelines"*.

Section 1.2. Covered Institutions – The term "covered institutions" shall refer to persons regulated by the Commission under the SRC, the Investment Houses Law, the Investment Company Act, the Financing Company Act of 1998, the Lending Company Regulation Act of 2007, other laws and regulations implemented by the Commission, and the AMLA, as amended. The covered institutions are as follows:

1.2.1 Securities Brokers, Dealers and Salesmen, Associated Person of a Broker or Dealer, Investment Houses and other similar entities managing securities or rendering similar services;

1.2.2 Investment Company Advisers/Fund Managers, Mutual Fund Distributors, Mutual Fund Companies, Closed-End Investment Companies;

1.2.3 Investment Advisor/Agent/Consultant;

1.2.4 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;

1.2.5 Other entities administering or otherwise dealing in currency, commodities or financial derivatives based thereon, cash substitutes and other similar monetary instruments or property, supervised or regulated by the Commission.

Section 1.3. Scope. – These Guidelines shall apply to the foregoing covered institutions, including their subsidiaries and affiliates that are also covered institutions, wherever they may be located.

Section 1.4. Covered Institutions Subject to Regulatory Power of Other Government Agency. – The Commission, as the Supervising Authority of the covered institutions as enumerated under Section 3(a)(3) of the AMLA, as amended, and where its supervision applies only to the incorporation of the covered institution, shall have the authority to require and ask assistance from the government agency having regulatory power and/or licensing authority over said covered institution for the implementation and enforcement of the AMLA, as amended, and its Revised Implementing Rules and Regulations (RIRR).

CHAPTER 2
DEFINITION OF TERMS

Section 2.1. 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, as amended.

2.1.1 **"Securities broker"** is a person engaged in the business of buying and selling securities for the account of others.

2.1.2 **"Securities dealer"** means any person who buys and sells securities for his/her own account in the ordinary course of business.

2.1.3 **"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.

2.1.4 **"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.

2.1.5. **"Investment House"** means any enterprise which primarily engages, 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.

2.1.6 **"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.

2.1.7 **"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.

2.1.8 **"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.

2.1.9 **"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.

2.1.10 **"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.

2.1.11 **"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, lawyer, 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 the 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.

2.1.12 **"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.

2.1.13 **"Lending Company"** shall refer to a corporation engaged in granting loans from its own capital funds or from funds sourced from not more than 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.

2.1.14 An "**affiliate**" means an entity:

(1) at least twenty percent (20%) but not more than 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:

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

(2) 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;

(3) 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

(4) the existence of material and regular transactions between the entities.

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

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

(2) 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

(3) 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:

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

(b) 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.

2.1.16 **"Beneficial Owner"** refers to any natural person who:

(1) Ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or

(2) 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 of 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.

2.1.17 **"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 Republic Act No. 455, and Republic Act No. 1937, as amended, otherwise known as the "Tariff and Customs Code of the Philippines";

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

12. "Hijacking" and other violations under Republic Act No. 6235, otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the Revised Penal Code, as amended;

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

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

15. "Bribery" under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, 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 IV 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. Violations 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. Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree "Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives";

27. Violation 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";

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 not be identical to any of the unlawful activities listed above.

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

1. the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources;

2. a foreign state; or

3. an international organization.

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 parents-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.).

CHAPTER 3
DESCRIPTION OF MONEY-LAUNDERING

Section 3.1. Definition of 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 or property represents, involves, or relates to the proceeds of any unlawful activity:

1. transacts said monetary instrument or property;
2. converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
3. conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
4. attempts or conspires to commit money laundering offenses referred to in (1), (2), or (3) above;
5. aids, abets, assists in, or counsels the commission of the money laundering offenses referred to in (1), (2), or (3) above; and
6. performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in (1), (2), or (3) above.

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

Section 3.2. 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:

3.2.1 *Placement* - the physical disposal of cash proceeds, derived from illegal activity.

3.2.2 *Layering* - separating the 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.

3.2.3 *Integration* - provides appearance of legitimacy to criminally- derived wealth. If the layering process has succeeded, the 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 covered institutions, which are no longer predominantly cash-based, they are less conducive 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 businesses of these covered institutions are most likely to be used at the second stage of money laundering, i.e., the layering process, as they provide 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, 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 these covered institutions as instruments for money laundering.

CHAPTER 4
BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

Section 4.1. Money Laundering and Terrorist Financing Prevention Program. All covered institutions shall adopt a comprehensive and risk-based Money Laundering and Terrorist Financing Prevention Program (MLPP) geared toward the promotion of high ethical and professional standards and the prevention of the covered institutions from being used, intentionally or unintentionally, for money laundering and terrorism financing.

The MLPP shall be consistent with the AMLA, as amended, its RIRR and the provisions set forth in these Guidelines and designed according to the covered institution's corporate structure and risk profile. It shall be in writing, approved by the board of directors or by the country/regional head or its equivalent for local branches of foreign covered institutions, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same.

Where a covered institution has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated system to ensure the coordination and implementation of the MLPP on a group-wide basis, taking into account local business considerations and the requirements of the host jurisdiction.

The covered institution at the head of the group shall be responsible for effective implementation of the MLPP at the level of the group. The covered institution at the head of the group refers to the covered institution that is not a subsidiary of any other covered institution in the group (i.e., the ultimate parent company/covered institution in the group).

For purposes of these Guidelines, a group of covered institutions shall refer to a covered institution, its subsidiaries and affiliates that are covered institutions.

The MLPP shall also be readily available in user-friendly form, whether in hard or soft copy. The covered institution must put up a procedure to ensure an audit trail evidencing the 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, other applicable guidelines issued by the AMLC and these Guidelines, to wit:

   (a) Customer identification process including acceptance policies and on-going monitoring processes;

   (b) Record keeping and retention;

   (c) Covered transaction reporting; and

   (d) Suspicious Transaction (ST) 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 ST 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 approves this decision in writing.

(2) An effective and continuous AML/CFT training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under these Guidelines, 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/CFT 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 or adverse circumstances in their backgrounds that would entail a risk of involvement in money laundering or terrorist financing are employed to assume sensitive functions within the covered institution;

(4) An internal audit system in accordance with Chapter 10 of this Guidelines;

(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 transactions reports submitted to the AMLC, and the records retained in compliance with these Guidelines 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 or other applicable regulator's examination are immediately corrected and acted upon;

(7) Cooperation with the AMLC;

(8) Designation of an AML Compliance Officer, who shall at least have a rank of senior vice president or an equivalent position with adequate stature and authority in the corporation as the lead implementor of the program within an adequately staffed compliance office. The AML compliance officer should not be a member of the Board of Directors and should annually attend AML trainings. The AML Compliance Officer may also be the liaison between the covered institution, the SEC and the AMLC in matters relating to the covered institution's AML/CFT compliance. Where resources of the covered institution do not permit the hiring of an AML Compliance Officer, the board of directors may provide that the Compliance Officer shall also assume the 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 RIRR as long this is done within the group. The MLPP may require a potential and/or existing customer to sign a waiver 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 control procedures and monitoring mechanism for prevention or mitigation of ML/TF risks.

Section 4.2. Submission of the Revised and Updated MLPP with Approval by the Board of Directors or Country Head. – Within six (6) months from the effectivity of these Guidelines, all covered institutions shall submit their MLPP to the Commission through the Operating Department having supervision over such covered institutions copy furnished the Anti-Money Laundering Division (AMLD) of the Enforcement and Investor Protection Department (EIPD). The revised or updated MLPP shall be approved by the board of directors, or the country/ regional head or its equivalent for local branches of foreign covered institutions and shall embody the principles and policies enunciated in these Guidelines.

Section 4.3. Updating of MLPP. – The MLPP shall be regularly updated at least once every two (2) years to incorporate changes in AML/CFT policies and procedures, latest trends in ML and TF typologies, and latest pertinent SEC issuances. Any revision or update in the MLPP shall likewise be approved by board of directors or the country/ regional head or its equivalent for local branches of foreign covered institutions.

Section 4.4. Checking of Covered Person's MLPP. – Covered persons shall make their MLPPs readily available for inspection during onsite examination.

CHAPTER 5
CUSTOMER IDENTIFICATION

A. General Requirements

Section 5.A.1. Written Client Identification and Acceptance Policies and Procedures. – Covered institutions must develop clear written client identification and graduated acceptance policies and procedures including a set of criteria for customers that are likely to pose low, normal or high risk to their operations. Such policies and procedures must be designed to ensure that the financially or socially disadvantaged are not denied access to financial services, while at the same time prevent suspicious individuals or entities from opening an account or establishing a relationship.

The policies and procedures must include procedures for providing customers with adequate notice that the covered institution is requesting information to verify their identities. If appropriate, the covered institution may use the following sample language to provide notice to its customers:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight money laundering activities, the Anti-Money Laundering Act, as amended, requires all covered institutions to obtain, verify and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth, business, TIN, SSS or GSIS Nos. and other information that will allow us to identify you. We may also ask to see your driver's license, passport or other competent evidence of identity bearing your photograph and signature.

Section 5.A.2. Continuing Due Diligence. – "Know your customer" measures of the covered institution should include conducting continuing due diligence on the business relationship to ensure that the transactions being conducted are consistent with the covered institution's knowledge of the customer and/or beneficial owner, their business profile, including, where necessary, the source of its funds.

Section 5.A.3. Customer Information and Identification Documents. – Covered institutions shall obtain and record competent 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, and other similar identity documents, which are verifiable from the institution issuing the same.

The identifying documents should provide evidence of 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 documents 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 covered institutions shall present one (1) original official identity card with photo and signature. 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.

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

(2) Incorporation and partnership papers, for corporate and partnership accounts. These documents should be certified as true copies from the issuing government agency.

(3) Special authorizations for representatives, which must be duly notarized.

Section 5.A.4. Additional or Further Verification Measures. – Clients should be made aware of the covered institutions' explicit policy that business transactions will not be conducted with applicants who fail to provide competent evidence of their identity, but without derogating from the covered institutions' obligation to report suspicious transactions. Where initial verification fails to identify the applicant, or gives rise to suspicion/s that the information provided is false, additional verification measures should be undertaken to determine whether to proceed with the business and/or make a suspicious transaction report if circumstances under Section 3(b-1) of the AMLA, as amended, would apply. Details of the additional verification are to be recorded in writing and be made available for inspection by the Commission or appropriate authorities.

The covered institution 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 customer's identity;
(2) That the customer is the beneficial owner; or
(3) The customer's declaration of beneficial ownership.

Section 5.A.5. Updating Client Information. – Covered institutions shall ensure that they know their customers well, and accordingly, shall keep current and accurate all material information with respect to their customers by regularly conducting verification and an update thereof.

Section 5.A.6. Unusual Transactions. – A covered institution should pay special attention to all unusually large transactions or unusual patterns of transactions. This requirement applies both to the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities.

Section 5.A.7. Acquisition by Covered Institution of the Business of Another Covered Institution. – When a covered institution acquires the business of another covered institution, either in whole or as a 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.

Section 5.A.8. If the True identity of Customer cannot be established. – The covered institution's policies and procedures must include procedures for responding to circumstances in which the covered institution cannot form a reasonable belief that it knows the true identity of a customer or when the covered institution is unable to comply with Section 5.A.3 hereof. These procedures should include, among others, the following:

(1) When the covered institution should not open the account or commence business relations or perform the transaction;

(2) The terms under which a customer may conduct transactions while the covered institution attempts to verify the customer's identity;

(3) When the covered institution should close an account or terminate business relationship after attempts to verify customer's identity fail; and

(4) Should consider filing a Suspicious Transaction Report with the AMLC.

Section 5.A.9. Conduct of Face-to-Face Contact. – Covered persons shall conduct face-to-face contact at the commencement of the relationship, or as 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.

The use of Information and Communication Technology in the conduct of face-to-face contact may be allowed, provided that the covered person is in possession of and has verified the identification documents submitted by the prospective client prior to the interview and that the entire procedure is documented.

Section 5.A.10. Presentation of Original Identification Documents. – Covered institutions shall request individual clients who present only photocopies of identification card and other documents to produce the original documents thereof for verification purposes.

Section 5.A.11. Use of New or Developing Technologies. – Covered institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Section 5.A.12. Third Party Reliance. – The covered institution's policies and procedures may include procedure specifying reliance on an intermediary or third party for its know your customer or customer due diligence requirements as long as the intermediary or third party relied upon are considered as covered institution as defined under these Guidelines or any other guidelines or rules issued by the Bangko Sentral ng Pilipinas (BSP) or the Insurance Commission (IC), or as defined and identified by foreign jurisdictions in so far as covered institutions in their respective jurisdictions are concerned.

It is understood that the Commission reserves the right to disapprove arrangements of covered institutions with intermediaries or third parties when it has been proven to have been abused by covered institutions.

Where such reliance is permitted, the following criteria should be met:

(1) The covered institution, relying on the intermediary or third party, should immediately take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the intermediaries and third parties upon request without delay. The covered institution should be satisfied with the quality of the due diligence undertaken by the intermediaries and third parties.

(2) The covered institution should satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with customer due diligence requirements.

(3) The customer identification program of the third party intermediary is similar to or is equivalent to the customer identification program of the covered institution.

(4) Ultimate responsibility for customer and/or beneficial owner identification and verification remains with the covered institution relying on 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.

Section 5.A.13. Outsourcing the Conduct of Customer Identification. – Covered persons 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 covered person.

The covered person outsourcing the conduct of customer identification, including face-to-face contact, shall ensure that the employees or representatives of the counter-party, intermediary or agent undergo equivalent training program as that of the covered person's own employees undertaking similar activity.

Section 5.A.14. Prohibited Accounts. – Covered institutions shall maintain customer accounts only in the name of the account holder. They shall not open or keep anonymous accounts, fictitious name accounts, incorrect name accounts, and similar accounts.

B. Personal Customers

Section 5.B.1. Covered institutions 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 (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 number or Government Service and Insurance System number;
(10) specimen signature;
(11) sources of funds, whenever necessary;
(12) names of beneficial owner or beneficiaries, if applicable;
(13) complete name, address and contact information of beneficial owner, if applicable.

C. Risk-Assessment/Risk-Profiling of Customers

Section 5.C.1. A covered institution shall formulate a risk-based and tiered customer acceptance, identification and retention policy that involves reduced customer due diligence (CDD) for potentially low risk clients and enhanced CDD for higher risk accounts.

Covered institutions shall specify the criteria and description of the types of customers that are likely to pose low, normal or high ML/TF risk to their operations, as well as the standards in applying reduced, average and enhanced due diligence, including a set of conditions for the denial of account opening or services.

Enhanced due diligence shall be applied to customers that are assessed by the covered institution or under these Guidelines as high risk for ML/TF.

For customers assessed to be of low risk such as small account balances and transactions, a covered institution may apply reduced due diligence. Some entities may likewise be considered as low risk clients, e.g., banking institutions, trust entities and Qualified Buyers (QBs) authorized by the BSP to operate as such and publicly listed companies subject to regulatory disclosure requirements.

In designing a customer acceptance and risk profiling policy, the following criteria relating to the product or service, the customer, and geographical location, at a minimum, shall be taken into account:

(1) The nature of the service or product to be availed of by the customers and the purpose of the account or transaction;

(2) Source of funds/nature of business activities;

(3) Public or high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;

(4) Country of origin and residence of operations or the fact that a customer came from a high risk jurisdiction;

(5) The existence of ST indicators;

(6) Watch list of individuals and entities engaged in illegal activities or terrorist-related activities as circularized by the BSP, SEC, AMLC, and other international entities or organizations, such as the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List; and

(7) Such other factors, e.g., the amount of the funds involved or the size of the transaction undertaken by a customer or the size of transactions, and regularity or duration of the transaction, as the covered institution may deem reasonable or necessary to consider in assessing the risk of a customer to ML/TF.

In assessing the risk profile of customers which are juridical entities, the covered institution should also consider the financial profile and other relevant information of the active authorized signatories.

The covered institution shall document the risk profiling results as well as how a specific customer was profiled and what standard of CDD (reduced, average or enhanced) was applied. Further, it shall regularly update its risk-assessment/risk-profiling of its clients.

Section 5.C.2. Reduced Due Diligence. – In general, the full range of customer due diligence measures should be applied. However, if the risk of money laundering or the financing of terrorism is lower based on the covered institution'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 the 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 disclosure requirements.
(3) Government institutions and its instrumentalities.

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

Section 5.C.3. Enhanced Due Diligence (EDD). – Covered persons shall examine, as far as reasonably 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, covered persons are required to conduct enhanced CDD measures consistent with the risks identified.

Whenever EDD is applied as required by these Guidelines, or by the covered institution's customer acceptance policy, or where the risk of ML/TF are higher, the covered institution shall do all of the following, in addition to profiling of customers and monitoring of their transactions:

(1) Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of normal due diligence.

(a) In case of individual customers-

(i) supporting information on the intended nature of the business relationship/source of funds/source of wealth (such as financial profile, ITR, etc.);

(ii) reasons for intended or performed transactions;

(iii) list of companies where he/she is a stockholder, beneficial owner, director, officer, or authorized signatory;

(iv) other relevant information available through public databases or internet; and

(v) a list of banks where the individual has maintained or is maintaining an account.

(b) In case of entities –

(i) prior or existing bank references;

(ii) the name, present address, nationality, date of birth, nature of work, contact number and source of funds of each of the primary officers (e.g., President, Treasurer);

(iii) volume of assets, other information available through public databases or internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial Statements, etc.); and

(iv) reasons for intended or performed transactions.

(2) Conduct validation procedures on any or all of the information provided;
(3) Secure senior management approval to commence or continue business relationship/transacting with the customer;
(4) Conduct enhanced ongoing monitoring of the business relationship, by, among others, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

(5) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and
(6) Perform such other measures as the covered institution may deem reasonable or necessary.

Section 5.C.4. Minimum Validation Procedures for EDD. – The procedures performed must enable the covered institution to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

Validation procedures for individual customers shall include, but are not limited to, the following:

(1) Confirming the date of birth from a duly authenticated official document;
(2) 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;
(3) Contacting the customer by phone or e-mail;
(4) 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; or
(5) Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include, but are not limited to, the following:

(1) Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
(2) In the case of an entity that is subject to supervision by a financial regulatory/supervisory body, inquiring from the supervising authority the status of the entity;
(3) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
(4) Contacting the entity by phone or e-mail.

Section 5.C.5. 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 result of the validation process is unsatisfactory, the covered institution shall decline to establish the relationship with the customer, or to execute the requested transaction, without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

Where the covered person fails to satisfactorily complete EDD and reasonably believes that conducting EDD will tip off the customer, it shall file an STR and closely monitor the account and review the business relationship.

If the covered institution 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 institution reasonably believes that performing the CDD process will tip off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting the CDD.

D. High Risk Customers

Section 5.D.1. Covered institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which:

(1) Are subject to financial sanctions, embargoes or similar measures by the United Nations or other public international organizations;

(2) Have been identified by credible sources as:

(a) having deficient AML/CFT regimes;
(b) having significant amounts of corruption or other criminal activity, including in particular illegal drug production, distribution or trafficking, money laundering, or human trafficking;
(c) providing financing or supporting terrorism or terrorist activities, or having terrorist organizations operating within their territory;
(d) being tax havens;
(e) experiencing significant civil unrest.

Credible sources include the FATF, FATF Style Regional Bodies (FSRB) such as the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities such as the Office of Foreign Assets Control of the U.S. Department of the Treasury, or other reliable third parties such as regulatory authorities, international standard setting bodies such as the IOSCO, the Basel Committee, the IAIS, or securities or commodities exchanges.

The background and purpose of these transactions should, as far as possible, be examined, and the findings established in writing. Whenever this examination reveals that these transactions have no apparent economic or visible lawful purpose, the covered institution should decline to proceed with the transaction or to establish the business relationship, or terminate the existing relationship, and should consider filing an STR with the AMLC.

Section 5.D.2. Covered institutions should ensure that the principles applicable to covered institutions are also applied to branches, offices, affiliates and subsidiaries located abroad, especially in countries which do not or insufficiently apply the anti-money laundering measures implemented in the Philippines, to the extent that local applicable laws and regulations permit.

Whenever a covered institution's branch, office, subsidiary or affiliate based outside the Philippines is prohibited from implementing these Guidelines or any of the provisions of the AMLA, as amended, or its RIRR, by reason of local laws, regulations or a supervisory directive, the covered institution shall:

(1) formally notify the Commission of this situation;
(2) furnish a copy of the applicable laws and/or regulations or the supervising authority's directive, as the case may be;
(3) advise the Commission of what measures or mitigating controls it intends to adopt to manage the money laundering (ML) and terrorist financing (TF) risks in such branches, offices, subsidiaries, or affiliates to the extent feasible;
(4) keep the Commission apprised of its efforts in this area, including any updates to the measures or controls referred to in point 3 above;
(5) at the direction of the Commission, close any branch or office, or divest itself of its interest in any subsidiary or affiliate, as the case may be, if the Commission determines that the covered institution cannot effectively manage the ML and/or TF risks arising from its relationship with such branch, office, subsidiary, or affiliate.

Section 5.D.3. Customers from countries referred to in Section 5.D.1 above are considered higher risk customers. In addition to the requirements under Sections 5.A.2 and 5.A.3 hereof, covered institutions are required to establish the source of wealth of higher risk customers. Decisions on business relations with higher risk customers must be taken by its senior management.

E. Politically Exposed Persons

Section 5.E.1. Covered institutions shall establish and record the true and full identity of PEPs, as well as their immediate family members and entities related to them.

In case of domestic PEPs or persons who have been entrusted with a prominent function by an international organization, or their immediate family members or close associates, in addition to performing the applicable due diligence measures, covered persons shall:

(a) Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
(b) In cases when there is a higher risk business relationship, adopt measures under Section 5.C.3 and Section 5.C.4 hereof on Enhanced Due Diligence relative to individual customers.

In relation to foreign PEPs or their immediate family members or close associates, in addition to performing the applicable customer due diligence measures, covered persons shall:

(a) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
(b) Adopt measures under Section 5.C.3 and Section 5.C.4 hereof on Enhanced Due Diligence relative to individual customers.

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

Section 5.F.1. Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In case of doubt as to the veracity of the corporation or identity of its directors and/or officers, or of the business or its partners, a search or inquiry with the Commission or the relevant Supervising Authority/Regulatory Agency shall be made.

Section 5.F.2. The following relevant documents shall be obtained in respect of corporate/other business applicants that are regulated in the Philippines:

(1) Copies of the Certificate of Registration issued by the Department of Trade and Industry, for single proprietors, or by the SEC, for corporations and partnerships, including the Articles of Incorporation or Certificate of Partnership, as appropriate; copies of the By-Laws of the corporation; the latest General Information Sheet, which lists the names of directors/trustees/partners and principal stockholders; and secondary licenses, if any; and other documents such as but not limited to clearance/certification from the Commission that the company is active and compliant with the reportorial requirements.

The original or certified true copies of any or all the foregoing documents, where required, should be produced for comparison and verification.

(2) Corporate/Partners' Secretary Certificate citing the pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity;

(3) Where necessary and reasonable, covered institutions may also require additional information about the nature of the business of clients, copies of identification documents of shareholders, directors, officers and all authorized signatories; and

(4) In the case of a corporate/business applicant that is owned or controlled indirectly or through a chain of entities, a detailed organizational chart or organogram clearly showing the respective ownership and/or control structure, including identification of all beneficial owners.

The type of measures that would normally be needed to satisfactorily perform identification of beneficial owners would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the management of the legal person or arrangement. Where the customer or owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

Section 5.F.3 For companies, businesses or partnerships registered outside the Philippines, comparable documents are to be obtained, duly authenticated by a senior officer of the covered person assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

Section 5.F.4. If significant changes to the company structure or ownership occur subsequently, or suspicions arise as a result of a change in the payment profile as reflected in a company account, further checks are to be made on the identities of the new owners.

Section 5.F.5. It is not necessary for a covered institution to routinely verify the details of the intermediate companies in the ownership structure of a company. However, the covered institution must always use its best efforts to determine who actually controls the customer. Complex ownership structures (e.g. structures involving multiple layers, cross-ownership, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk. In these cases, further steps may be necessary to ensure that the institution is satisfied on reasonable grounds as to the identity of the beneficial owners.

The need to verify the intermediate corporate layers of the ownership structure of a company will therefore necessarily depend upon the covered institution's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the covered institution to consider if it has taken adequate measures to identify the beneficial owners.

It is a good business practice for a covered institution to have each legal entity account holder complete and sign a "beneficial owner declaration form" for each account, and to obtain an organizational chart clearly showing the companies in the group, the relationship of the companies to each other, the ownership of each company, and the ultimate beneficial owner(s) of the customer.

G. Shell Companies

Section 5.G.1. Shell companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted. Covered institutions should note that shell companies may be abused by money launderers and therefore be cautious in their dealings with them.

Section 5.G.2. In addition to the requirement under Section 5.F.2, covered institutions should also obtain a Board of Directors' Certification as to the purposes of the owners/stockholders in acquiring the shell company. There must likewise be satisfactory evidence of the identities of the beneficial owners, bearing in mind the "Know-Your-Customer" principle.

H. Trust, Nominee and Fiduciary Accounts

Section 5.H.1. Covered institutions shall establish whether the applicant for business relationship is acting on behalf of another person as a trustee, nominee or agent. Covered institutions should obtain competent evidence of the identity of such agents and authorized signatories, and the nature of their trustee or nominee capacity and duties.

Section 5.H.2. Where the covered institution 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, covered institutions shall consider whether to proceed with the business, bearing in mind the "Know-Your- Customer" principle. If the covered institutions decide to proceed, they are to record any misgivings and give extra attention to monitoring the account in question.

Section 5.H.3. Where the account is opened by a firm of lawyers or accountants, the covered institutions should make 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 AMLC in respect of such client's 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 AMLA, as amended, and other pertinent laws.

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

Section 5.I.1. Transactions Undertaken on Behalf of Account Holders or Non-Account Holders. – Where transactions are undertaken on behalf of account holders of a covered institution, particular care shall be taken 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 competent evidence of identity including nationality, especially in cases where the client is not a Filipino, the purposes of the transaction, and the sources of the funds.

J. Bearer Shares

Section 5.J.1. Bearer shares are equity securities that are wholly owned by whoever holds the physical stock certificate. The issuing company does not register the owner of the stock or track transfers of ownership. Transferring the ownership of the stock involves only delivering the physical document. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded. Due to the higher ML/TF risks associated with bearer shares, the FATF standards require countries that allow companies to issue bearer shares to take appropriate measures to ensure that they are not misused for money laundering.

Philippine legislation prohibits domestic companies from issuing bearer shares. However, some foreign jurisdictions do permit companies to issue such shares, and there is a possibility that Philippine securities firms may encounter such firms as customers. Thus, institutions dealing with companies that issue such shares need to be particularly diligent, as it is often difficult to identify the beneficial owner(s). Covered institutions should adopt procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified whenever there is a change of holder or beneficial owner.

A covered institution dealing with bearer share entities 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.

Specifically, covered institutions should obtain declarations prior to account opening, and annually thereafter, from each beneficial owner holding at least five percent (5%). Covered institutions should also require the customer to notify it immediately of any changes in the ownership of the shares.

K. Wire Transfers

Section 5.K.1. Because of the risk associated with dealing with fund/ wire transfers, where a covered institution 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:

(1) A beneficiary institution shall not accept instructions to pay-out 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 provided the rules on third party reliance under section 5.A.12 are met, treating the originating institution as third party as therein defined;

(2) An originating institution shall not accept instructions to fund/wire 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;

(3) In cross border transfers, if the originator is a high risk customer as herein described, the beneficiary institution shall conduct enhanced due diligence 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 fund/wire transfer or the pay-out of funds without

prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant;

(4) Whenever possible, manually initiated funds transfer (MIFT) instructions should not be the primary delivery method. Every effort shall be made to provide client with an electronic solution. Where MIFT is utilized, the following validation procedures shall apply:

a) Prior to the covered institution 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 covered institution has complied with the stated security procedures.

b) It is mandatory that written MIFT instructions are signature verified. In addition, one of the following primary security procedures must be applied:

(i) a recorded callback to the customer to confirm the transaction instructions, or

(ii) test word arrangement/verification, provided that this procedure 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/ pre-defined instructions; or value for value transactions.

c) 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. If monitoring is not possible, the device must be secured or programmed to receive messages into a password protected memory.

d) MIFT transactions below a certain threshold [approved by the [branch manager/country manager] (for branches of foreign covered institutions) or Business Risk Manager in accordance with policies and procedures approved by the covered institution's board of directors] may be processed with the mandatory procedure described above and an enhanced security procedure such as any or all of the following:

e) 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 the person receiving the original instructions and effecting the signature verification.

(5) Cross border and domestic fund/wire transfers and related message not exceeding P50,000.00 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:

(a) Name of the originator;
(b) Name of the beneficiary; and
(c) Account number of the originator and beneficiary, or in its absence, a unique reference number.

(6) For cross border and domestic fund/ wire transfers and related message amounting to P50,000.00 or more, or its equivalent in foreign currency, the following information shall be obtained and accompany the wire transfer:

(a) Name of the originator;

(b) Originator account number where such an account is used to process the transaction or a unique transaction reference number which permits traceability of the transaction;

(c) Originator's address, or national identity number, or customer identification number, or date and place of birth;

(d) Name of the beneficiary; and

(e) Beneficiary account number where such an account is used to process the transaction, or unique transaction reference number which permits traceability of 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.

(7) Should any wire/fund transfer amounting to P50,000.00 or more or its equivalent be unaccompanied by the required originator 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 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 fund/wire transfer or the pay-out of funds without prejudice to the reporting of an ST to the AMLC when circumstances warrant.

CHAPTER 6
RECORD KEEPING

Section 6.1. General Requirements for Record Keeping. – The covered institutions' policies and procedures as described in Chapter 5 hereof, must include procedures for making and maintaining a record of all 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 covered institution 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 report is made to it;

(3) The covered institution 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.

Section 6.2. Periods of Retention. – The following document retention periods shall be followed:

(1) All records of all transactions of covered institutions, 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 correspondence, shall be preserved and safely stored for at least five (5) years from the dates when they were closed.

(3) SRC Rule 52.1.1 (Books and Records Keeping Rule) and Rule 52.1.2 (Records Retention Rule) of the 2015 Implementing Rules and Regulations of the SRC continue to be in full force and effect.

Section 6.3. Records Relating to Pending Case. – Notwithstanding Section 6.2 hereof, 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.

Section 6.4. Forms of Records. – Transaction documents may be retained as originals or copies, on microfilm, provided that such forms are admissible in court, pursuant to the Revised Rules of Court and the E-commerce Act and its Implementing Rules and Regulations.

Section 6.5. Digitization of Customer Records. – Covered institutions 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.

Section 6.6. Persons Responsible for Safekeeping of Records. – The covered institution shall designate at least two (2) persons responsible in the safekeeping of all records and report to the Commission any change in the person/s responsible.

CHAPTER 7
REPORTING OF COVERED AND SUSPICIOUS TRANSACTIONS

Section 7.1. Reporting System. – Each covered institution shall institute a system for the mandatory reporting of covered transactions and suspicious transactions. The system shall be described in detail in the operating manual of the covered institutions.

Section 7.2. Registration with AMLC. – All covered persons shall register with the AMLC's electronic reporting system.

Section 7.3. Covered Transaction Report (CTR). – Covered institutions 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) within one (1) banking day;

Section 7.4. Suspicious Transaction Report (STR). – Covered institutions shall file Suspicious Transaction Reports ("STR") with the AMLC for transactions, regardless of the amount of the transaction, where any of the following circumstances exists:

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 file of the client and/or the client's past transactions with the covered institution;
6. The transaction is in any way related to an unlawful activity or offense under the 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.

In this regard, the covered institution should exercise due diligence by implementing adequate systems for identifying and detecting suspicious transactions.

Suspicious transactions are likely to involve a number of factors which together raise a suspicion in the mind of the covered institution that the transaction may be connected with any unlawful activity.

Section 7.5. Transaction Reporting. – Covered institutions 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 be reckoned from the date the covered institution knew or should have known the suspicious transaction indicator.

Section 7.6. Transactions that are both Covered and Suspicious. – Should a transaction be determined to be both a covered and a suspicious transaction, the covered institution shall report the same as a suspicious transaction.

Section 7.7. Attempted Suspicious Transactions. – Covered persons shall likewise 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 7.4 hereof exists.

Section 7.8. Reporting of Customer's Unlawful Activities. – Where any employee or personnel, director or officer of the covered institution knows that the client has engaged in any of the unlawful activities under the AMLA, the matter must be promptly reported to its Compliance Officer who, in turn, must immediately report the details to the AMLC.

If there is reasonable ground to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, 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, unless he considers, and records an opinion, that such reasonable grounds do not exist.

Section 7.9. Register of Suspicious and Covered Transactions. – Each covered institution shall maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the AMLC.

Each covered institution shall likewise maintain a register of all covered transactions which are not reported to the AMLC pursuant to AMLC Resolution No. 292, Series of 2003.

The registers shall contain details of the date on which the report is made, the person who made the report to its Compliance Officer, and information sufficient to identify the relevant papers related to said reports.

Section 7.10. Confidentiality of CTR and STR. – Covered institutions, their directors, officers and employees, shall not warn their customers that information relating to them has been reported or is in the process of being reported to the AMLC, or communicate, directly or indirectly, such information to any person other than the AMLC. 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, covered institutions, their 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.

In case of violation thereof, the concerned officer and employee of the covered institution shall be criminally liable in accordance with the provision of the AMLA, as amended.

Covered institutions, their directors, officers and employees, shall not notify their customers that information relating to them has been flagged internally with a view toward making a determination as to whether to file a ST, or communicate, directly or indirectly, such information to any person other than the AMLC.

Section 7.11. Safe Harbor Provision. – No administrative, criminal or civil proceedings shall lie against any person for having made a suspicious or covered transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law. Covered institutions, 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 8
COMPLIANCE

Section 8.1. The Compliance Officer. – Each covered institution 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 procedures, including customer identification policies and procedures, proper maintenance of records, reporting of covered and suspicious transactions to the AMLC, and training of employees.

Unless otherwise provided in its Operating Manual, the registered Associated Person of covered institution covered by the SRC shall also be the Compliance Officer as contemplated herein. A Compliance Officer shall be:

1. A senior officer with relevant qualifications 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 covered institution;
3. Responsible for ensuring compliance by the staff of the covered institution with the provisions of the AMLA, as amended, its Implementing Rules and Regulations, and the covered institution's manual of compliance Procedures established under Section 9.2 (b);
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 between covered institution 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 covered institutions' 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 Guideline, 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.

The Compliance Officer should not simply be a passive recipient of ad hoc reports of suspicious transactions, but should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfill these functions, covered institutions must ensure that the Compliance Officer receives full co-operation from all staff and full access to all relevant documentation.

Section 8.2. Adviser Regarding AML matters. – Each covered institution 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.

Section 8.3. Responsibility of the Covered Institution and its Board. – Notwithstanding the duties of the Compliance Officer, the ultimate responsibility for proper supervision, reporting and compliance under the AMLA, as amended, its RIRR shall rest with the covered institution and its board of directors.

CHAPTER 9
INTERNAL CONTROL AND PROCEDURES

Section 9.1. General Requirements. – Covered institutions are required to establish and implement internal control and procedures aimed at preventing and impeding money laundering. Such procedures shall, among other things, ensure that such covered institutions and their employees are aware of the provisions of the AMLA, its implementing rules and regulations, as well as all reportorial and compliance control and procedures that shall be established by the AMLC, the Supervising Authority and each covered institution.

Covered institutions shall see to it that their respective policies and procedures for dealing with money laundering, reflecting the requirements under the AMLA and its implementing rules and regulations, are clearly set out and reflected in their Operating Manual.

Section 9.2. Coverage of Internal Control Policies and Procedures. – Policies and procedures should cover, among others:

9.2.1 Communications of firm policies relating to money laundering, including timely disclosure of information and internal audits to ensure compliance with policies, procedures and controls relating to money laundering;

9.2.2 Account opening and customer identification, including requirements for proper identification;

9.2.3 Maintenance of records;

9.2.4 Compliance with the requirement of the AMLA, as amended, its Revised Implementing Rules and Regulations, and all Circulars issued by the Commission and the AMLC;

9.2.5 Cooperation with the Commission and other relevant Authorities.

Section 9.3. Written Internal Reporting Procedures. – Covered institutions shall establish written internal reporting procedures which shall:

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

9.3.2 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 covered institution;

9.3.3 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;

9.3.4 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;

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

9.3.6 Maintain a register of all reports filed pursuant to Sections 7.7, 7.8 and Section 7.9 above.

CHAPTER 10
INTERNAL AUDIT

Section 10.1. 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.

Section 10.2. Frequency and Scope of Internal Audit. – The internal audit shall be responsible for the periodic (not less frequently than once every 2 years) 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.

Section 10.3. Electronic AML/CFT Monitoring System. – For covered institutions with electronic AML/CFT transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities.

Section 10.4. Reporting of Internal Audit Findings. – The results 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 appropriate monitoring of corrective actions taken by the different business units concerned. The Compliance Office shall regularly submit reports to the board to inform them of management's action to address deficiencies noted in the audit.

Section 10.5. Outsourcing of Internal Audit Functions/External Audit. – A covered institution may, due to the scale and nature of their operations, assign the internal audit function to another person (e.g. professional association, parent company or external auditors) under terms of reference approved by the institution's board of directors designed to ensure the effectiveness of the internal audit function. Where a covered institution delegates its responsibilities for internal audit, due diligence is to be exercised to ensure that the persons appointed are able to perform these functions effectively and the fact of such appointment must be relayed in writing to the Commission and to AMLC. Notwithstanding that the internal audit function may be outsourced, the covered institution's board of directors remains responsible for its effective operation.

CHAPTER 11
TRAINING

Section 11.1. Education and Continuing Training. – The covered institution shall provide education and continuing training for all its staff and personnel, including directors and officers, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and to be familiar with its system for reporting and investigating suspicious matters.

Section 11.2. Outsourcing of Training Functions/External Training Providers. – A covered institution may, due to the scale and nature of their operations, assign the training functions to another person (e.g. professional association, parent company or external training provider). Where a covered institution delegates its responsibilities for training, due diligence is to be exercised to ensure that the persons appointed are able to perform these functions effectively and the fact of such appointment must be relayed in writing to the Commission and to AMLC.

Notwithstanding that the training function may be outsourced, the covered institution's board of directors remains responsible for the effective operation of the training program.

Section 11.3. Recommended Training Programs. – Timing and content of training for various sectors of staff will need to be adapted by the covered institution to its own needs. The following training programs are recommended:

11.3.1 New Staff

A general appreciation of the background to money laundering, the need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within the covered institution. This training shall be provided to all new employees, regardless of level of seniority.

11.3.2 Cashiers/Dealers' Representatives Representatives/Advisory Staff

Personnel who deal directly with the clients are the first point of contact with potential money launderers. Their efforts are therefore vital to the covered institutions' reporting system for such transactions. They should be trained to identify suspicious transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. "Front Line" staff should be made aware of the covered institution's policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in cases under suspicious circumstances.

11.3.3 Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to supervisors and managers. This will include the offences and penalties arising from the AMLA, procedures relating to service of production and restraint orders, internal reporting procedures, and the requirements for verification of identity and the retention of records.

Section 11.4. Regular Refresher Training. – Covered institutions shall, at least once a year, make arrangements for refresher training to remind key staff of their responsibilities and to make them aware of any changes in the laws and rules relating to money laundering, as well as the internal procedures of the covered institution.

Section 11.5. Training Program and Records of Trainings Conducted. – Each covered institution's annual AML training program and records of all AML seminars and trainings conducted by the covered institution and/or attended by its personnel (internal or external), including copies of AML seminar/training materials, shall be appropriately kept by the Compliance Officer/unit/department, and made available during periodic or special SEC examinations and to self-regulatory organizations (SROs) of covered institutions, if applicable.

Section 11.6. Cascading of Updates and New Requirements. – Covered institutions 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 of the covered institutions based on any of the foregoing. Training on any such new provisions, amendments, updates or changes shall be provided as necessary.

CHAPTER 12
SANCTIONS AND PENALTIES

Section 12.1. Sanctions and Penalties. – Any violation of the requirements set forth in these Guidelines 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 Regulations Code without prejudice to the penalties that may be imposed by the AMLC RIRR. Accordingly, the Commission may impose any or all of the following sanctions as may be appropriate in the light of the facts and circumstances:

(i) Suspension or revocation of any registration for the offering of securities;
(ii) A fine of no less than Ten Thousand Pesos (Php10,000.00) nor more than One Million Pesos (Php 1,000,000.00) plus not more than Two Thousand Pesos (Php 2,000.00) for each day of continuing violation;
(iii) Other penalties within the power of the Commission to impose.

Section 12.2. Criminal Actions and Criminal Liability. – The imposition of the foregoing administrative sanctions 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.

Section 12.3. Manner of Imposition of Penalties. – The penalties shall be imposed in a manner that is effective, proportionate and dissuasive.