



Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila



Circular Letter (CL) No.:	2018-48
Date:	14 September 2018

CIRCULAR LETTER

TO : All Insurance/Reinsurance Companies, Insurance and Reinsurance Brokers, Mutual Benefit Associations, Trusts for Charitable Uses, Pre-Need Companies, Health Maintenance Organizations and other Covered Persons under the Regulation of the Insurance Commission

SUBJECT : Anti-Money Laundering and Combating the Financing of Terrorism Guidelines for Insurance Commission Regulated Entities

Pursuant to the authority vested to the Insurance Commission (IC) under Rule 18 (A) of the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act No. 9160, also known as the "Anti-Money Laundering Act of 2001 (AMLA), As Amended", and Rule 27 of the Implementing Rules and Regulations (IRR) of Republic Act No. 10168, otherwise known as "The Terrorism Financing Prevention and Suppression Act", to issue and/or update its guidelines and circulars on anti-money laundering and terrorism financing prevention and suppression, respectively, the following **Anti-Money Laundering and Combating the Financing of Terrorism Guidelines** is hereby promulgated for the guidance and strict compliance of all covered Insurance Commission Regulated Entities:

TITLE I DECLARATION OF POLICY

Section I. Declaration of Policy. – This Commission adopts the policy of the State to ensure that the Philippines and the entities regulated by the IC shall not be used as a money laundering site and conduit for the proceeds of an unlawful activity as herein defined, respectively; and to protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it and to recognize it as inimical and dangerous to national security and the welfare of the people, and to make the financing of terrorism a crime against the Filipino people, against humanity, and against the law of nations.

TITLE II GENERAL PRINCIPLES

Section 2. Policies to Combat Money Laundering and Financing of Terrorism. – Insurance Commission Regulated Entities (ICREs), as covered persons, are to be regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) proportionate to the nature, scale and complexity of the its operations in order to prevent criminals from exploiting them. Considering that money laundering and financing of terrorism are serious crimes that threatens the competitiveness and openness of the Philippine economy, ICREs must apply the following principles throughout their businesses:

- a. Conform with high ethical standards and observe good corporate governance consistent with this Guidelines in order to protect the integrity of ICREs;
- b. Know sufficiently their customers to prevent criminal elements and suspicious individuals or entities from transacting with, or establishing or maintaining relationship with the ICREs;
- c. Adopt and effectively implement an appropriate AML/CFT risk management system that identifies, understand, assesses, monitors, and controls risks associated with money laundering and terrorist financing (ML/TF);
- d. Comply fully with existing laws and regulations aimed at combating money laundering and terrorist financing by making sure that their officers and employees are aware of their respective responsibilities and carry them out in accordance with a superior and principled culture of compliance;
- e. Cooperate fully with this Commission and the Anti-Money Laundering Council (AMLC) for the effective implementation of the Anti-Money Laundering and Countering the Financing of Terrorism Laws, their respective implementing rules and regulations, and other directives, guidance and issuances from the IC and AMLC.

Section 3. Scope. – This Guidelines shall apply to the following ICREs:

- a. Insurance Companies;
- b. Pre-need Companies;
- c. Health Maintenance Organizations;
- d. Insurance and Reinsurance Brokers;
- e. Professional Reinsurers;
- f. Mutual Benefit Associations;
- g. Trust for Charitable Uses; and
- h. All other persons supervised or regulated by the IC.

TITLE III
DEFINITION OF TERMS

Section 4. Definition of Terms. – For purposes of this Guidelines, the following terms are defined as follows:

- A. **“Anti-Money Laundering Act”** (AMLA) refers to Republic Act No. 9160, as amended by Republic Act Nos. 9194, 10167, 10365 and 10927.
- B. **“Anti-Money Laundering Council”** (AMLC) refers to the financial intelligence unit of the Philippines which is the government agency tasked to implement the AMLA.
- C. **“Financing of Terrorism”** is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the inlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (i) carry out or facilitate the commission of any terrorist act; (ii) by a terrorist organizations, association or group; or (iii) by an individual terrorist.
- D. **“Person”** refers to any natural or juridical person.
- E. **“Transaction”** refers to any act establishing any right or obligation, or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person.
- F. **“Competent authorities”** refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the AMLC; the authorities that have the function of investigating and/or prosecuting money laundering, unlawful activities and terrorist financing, and seizing/freezing and confiscating any monetary instrument or property that is in any way related to an unlawful activity; authorities receiving reports on cross-border transportation of currency & bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements.
- G. **“Covered transaction”** refers to:
 - 1. A transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (Php500,000.00) or its equivalent in any other currency; or

2. A transaction, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), where the total premiums/fees paid for a policy, plan or agreement for the entire year exceeds Five Hundred Thousand Pesos (Php500,000.00) or its equivalent in any other currency.

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

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

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

I. "**Customer**" refers to any person who keeps an account, or otherwise transacts business with an ICRE. It includes the following:

1. Any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions;
2. Beneficiary of a trust, an investment fund or a pension fund;
3. A company or person whose assets are managed by an asset manager;
4. A grantor of a trust; and
5. Any insurance policy holder, pre-need plan holder or HMO enrolled member, whether actual or prospective.

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

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

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

- K. **“Immediate Family Member of PEPs”** refers to spouse or partner; children and their spouses; and parents and parents-in-law.

- L. **“Close Associates of PEPs”** refer to persons who are widely and publicly known to maintain a particularly close relationship with the PEP, and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

- M. **“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 a legal person or arrangement.

Ultimate effective control refers to situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control.

- N. **“Official Document”** refers to any of the following identification documents:

1. For Filipino citizens: Those issued by any of the following official authorities:
 - a. Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
 - b. Government-Owned or -Controlled Corporations (GOCCs);
 - c. Covered persons registered with and supervised or regulated by the BSP, SEC or IC;

2. For foreign nationals: Passport or Alien Certificate of Registration;
3. For Filipino students: School ID signed by the school principal or head of the educational institution; and
4. For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the customer's identity.

O. "**Monetary Instrument**" shall include, but is not limited to the following:

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

P. "**Property**" refers to any thing or item of value, real or personal, tangible or intangible, or any interest therein, or any benefit, privilege, claim, or right with respect thereto, including:

1. Personal property, including proceeds derived therefrom, or traceable to any unlawful activity, such as, but not limited to:
 - a. Cash;

- b. Jewelry, precious metals and stones, and other similar items;
 - c. Works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;
 - d. Perishable goods; and
 - e. Vehicles, vessels, aircraft, or any other similar conveyance.
 2. Personal property, used as instrumentalities in the commission of any unlawful activity, such as:
 - a. Computers, servers, and other electronic information and communication systems; and
 - b. Any conveyance, including any vehicle, vessel, and aircraft.
 3. Real estate, improvements constructed or crops growing thereon, or any interest therein, standing upon the record of the registry of deeds in the name of the party against whom the freeze order or asset preservation order is issued, or not appearing at all upon such records, or belonging to the party against whom the asset preservation order is issued and held by any other person, or standing on the records of the registry of deeds in the name of any other person, which are:
 - a. derived from, or traceable to, any unlawful activity; or
 - b. used as an instrumentality in the commission of any unlawful activity.
- Q. **"Proceeds"** refers to an amount derived or realized from any unlawful activity.
- R. **"Monetary Instrument or Property Related to an Unlawful Activity"** refers to:
 1. All proceeds of an unlawful activity;
 2. All monetary, financial or economic means, devices, accounts, documents, papers, items, or things used in or having any relation to any unlawful activity;
 3. All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds, and other similar items for the financing, operations, and maintenance of any unlawful activity; and
 4. For purposes of freeze order and bank inquiry: related and materially-linked accounts.

S. **“Related Accounts”** refers to those accounts, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.

T. **“Materially-linked Accounts”** shall include the following:

1. All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;
2. All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;
3. All “In Trust For” accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
4. All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry; and
5. All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing.

U. **“Offender”** refers to any person who commits a money laundering offense.

V. **“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 VI of Republic Act No. 8550, otherwise known as the "*Philippine Fisheries Code of 1998*";
22. Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the "*Philippine Mining Act of 1995*";

23. Violations of Section 27(c), (e), (f), (g) and (i) of Republic Act No. 9147, otherwise known as the "*Wildlife Resources Conservation and Protection Act*";
24. 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 1972, as amended*";
26. Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree "*Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives*";
27. Violation 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 a 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.

W. **Money Laundering.** - Money laundering is committed by:

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

- a. Transacts said monetary instrument or property;
 - b. Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
 - c. Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
 - d. Attempts or conspires to commit money laundering offenses referred to in (a), (b), or (c) above;
 - e. Aids, abets, assists in, or counsels the commission of the money laundering offenses referred to in (a), (b), or (c) above; and
 - f. Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in (a), (b), or (c) above.
2. Any covered person who, knowing that a covered or suspicious transaction is required under the AMLA to be reported to the AMLC, fails to do so.

TITLE IV COMPLIANCE FRAMEWORK

Section 5. Responsibilities of the ICREs. – The ICREs shall:

- a. Establish, implement, monitor and maintain an effective Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Compliance Program in line with this Guidelines.
- b. Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential ML/TF activities such as but not limited to the following:
 - i. Compliance Regime;
 - ii. Risk Assessment;
 - iii. Customer Due Diligence;
 - iv. Record Keeping;
 - v. Training and awareness;
 - vi. Employee screening;
 - vii. Detection of suspicious transactions; and
 - viii. Reporting of covered and suspicious transactions.
- c. Ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

- d. Establish an ongoing employee training program to ensure that those employees are kept informed of new developments, including information on current Money Laundering and Terrorist Financing risks, techniques, methods and trends.
- e. Carry out on a regular basis, independent review of their AML/CFT program, as provided in Section 12 hereof.

Section 6. Risk Management. All ICREs shall develop sound risk management policies and practices to ensure that risks associated with money laundering and terrorist financing such as counterparty, reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of this Guidelines, to the end that ICREs shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.

The four (4) areas of sound risk management practices are adequate and active board and senior management oversight, acceptable policies and procedures embodied in a money laundering and terrorist financing prevention compliance program, appropriate monitoring and Management Information System and comprehensive internal controls and audit.

Section 7. Risk Assessment. – The ICREs shall:

- a. Take appropriate steps to identify, assess and understand its AML/CFT risks in relation to its customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk-based approach. The risk assessment shall include both quantitative and qualitative factors.
- b. Institute the following processes in assessing their ML/TF risks:
 - i. Documenting risk assessments and findings;
 - ii. Considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
 - iii. Keeping the assessment up-to-date through periodic review; and
 - iv. Ensure submission of the risk assessment information as may be required by the IC.
- c. Maintain AML/CFT prevention policies, procedures, processes and controls that are relevant and up-to-date in line with the dynamic risk associated with its business, products and services and that of its customers.
- d. Establish, implement, monitor and maintain satisfactory controls that are commensurate with the level of AML/CFT risk;

- e. Conduct additional assessment as and when required by the IC; and
- f. Institutional risk assessment shall be conducted at least once every two (2) years.

Section 8. Risk Management Policies. – All ICREs shall develop sound risk management policies and practices to manage and mitigate the ML/TF risks that have been identified; monitor the implementation of those policies, controls, procedures and to enhance them if necessary; and take enhanced measures to manage and mitigate the risks where higher risks are identified.

Section 9. Active Board and Senior Management Oversight. – The ICREs' Board of Directors is ultimately responsible for ensuring compliance with this Guidelines, the AML and CFT Laws, their respective implementing rules and regulations, and other directives, guidance and issuances from the IC and AMLC.

Senior management shall oversee the day-to-day management of the ICREs, ensure effective implementation of AML/CFT policies approved by the board and alignment of activities with the strategic objectives, risk profile and corporate values set by the board. Senior management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

- a. **Compliance Office.** Management of the implementation of the ICREs' Money Laundering and Terrorist Financing Prevention Program (ML/TFPP) shall be a primary task of the compliance office. To ensure the independence of the office, it shall have a direct reporting line to the board of directors or any board-level or approved committee on all matters related to AML and CFT compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by senior management and the board, to wit:
 - i. Ensure compliance by all responsible officers and employees with this Guidelines, the AML and CFT Laws, their respective implementing rules and regulations, other directives, guidance and issuances from the IC and AMLC and its own ML/TFPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of AML and CFT transaction monitoring system and record retention system through sample testing and review of audit or checking reports. It shall also report compliance findings to the board;
 - ii. Ensure that infractions, discovered either by internally initiated audits, or by special or regular compliance checking conducted by the IC and/or AMLC are immediately corrected;

- iii. Inform all responsible officers and employees of all resolutions, circulars and other issuances by the IC and/or the AMLC in relation to matters aimed at preventing ML and TF;
 - iv. Alert senior management and the board of directors if it believes that the ICRE is failing to appropriately address AML/CFT issues; and
 - v. Organize the timing and content of AML/CFT training of officers and employees including regular refresher trainings.
- b. **Group-wide AML/CFT Compliance.** In case an ICRE has branches, subsidiaries or offices located within and/or outside the Philippines, the group-wide compliance officer or in its absence, the compliance officer of the parent entity, shall oversee the AML/CFT compliance of the entire group with reasonable authority over the compliance officers of said branches, subsidiaries or offices.

Section 10. Designation of a Compliance Officer and/or Office. – ICREs shall designate a compliance officer of senior management status with the authority and mandate to ensure day-to-day compliance with its AML/CFT obligations. The compliance officer shall have a direct line of communication to the ICRE's Board of Directors to report on matters pertaining to its AML/CFT obligations, including the ICRE's failure to manage ML/TF risks and new AML/CFT obligations issued by the IC and/or AMLC that require updates to the ICRE's compliance measures. The compliance officer shall also ensure that compliance measures reflect readily available information concerning new trends in ML and TF and detection techniques.

The ICREs shall also designate another officer to be responsible and accountable for all record keeping requirements under this Guidelines. These officers will also be responsible for making records of customer identification and transaction documents readily available without delay to the IC and AMLC during compliance checking or investigation.

Section 11. Implementation of a Money Laundering and Terrorism Financing Prevention Program (ML/TFPP). – The ICRE's Board of Directors (BOD) shall approve, and the compliance officer shall implement, a comprehensive, risk-based ML/TFPP geared towards the promotion of high ethical and professional standards and the prevention of ML and TF. The ML/TFPP shall be in writing; consistent with the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances; and its provisions shall reflect the ICRE's corporate structure and risk profile. It shall be readily available in user-friendly form, whether in hard or soft copy. Moreover, it shall be well disseminated to all officers and staff who are obligated, given their position, to implement compliance measures. The ICREs shall design procedures that ensure an audit trail evidencing the dissemination of the ML/TFPP to relevant officers and staff.

Where an ICRE operates at multiple locations in the Philippines, it shall adopt an institution-wide ML/TFPP to be implemented in a consolidated manner. Where a

ICRE has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated ML/TF risk management system to ensure the coordination and implementation of policies and procedures on a group-wide basis, taking into account local business considerations and the requirements of the host jurisdiction. Lastly, the ML/TFPP shall be updated at least once every two years or whenever necessary to reflect changes in AML/CFT obligations, ML and TF trends, detection techniques and typologies.

At a minimum, the ML/TFPP's provisions shall include:

- a. Detailed procedures of the ICREs' compliance and implementation of the following major requirements of the AMLA, as amended, and this Guidelines:
 - i. customer identification process, including acceptance policies and an on-going monitoring process;
 - ii. record keeping and retention;
 - iii. covered transaction reporting; and
 - iv. suspicious transaction reporting, including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of future reporting of such transactions to the AMLC. Suspicious transaction reporting shall include a reporting chain under which a suspicious transaction will be processed and the designation of a Board-Level approved Committee or designation of a senior officer who will ultimately decide whether or not the ICRE should file a report to the AMLC;
- b. 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 the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances, their own internal policies and procedures, and such other obligations as may be required by the IC and/or the AMLC;
- c. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personnel with no criminal record or integrity-related issues are employed or contracted by ICREs;
- d. An internal audit system and an independent audit program that will ensure the completeness and accuracy of information obtained from customers. The ICREs shall specify in writing the examination scope of independent audits, which shall include ensuring checking the accuracy and completeness of identification documents, covered transaction report (CTR) and suspicious transaction report (STR) submitted to the AMLC, and records retained in

compliance with this framework, as well as assuring adequacy and effectiveness of the ICRE's training programs;

- e. A mechanism that ensures all deficiencies noted during the audit and/or regular or special compliance checking are immediately and timely corrected and acted upon;
- f. Cooperation with the IC, AMLC and other competent authorities;
- g. Designation of a Compliance Officer, who shall, at least, be of senior management level, as the lead implementer of the ICRE's compliance program; and
- h. The identification, assessment and mitigation of ML/TF risks that may arise from new business practices, services, technologies and products.

Within one hundred eighty (180) days from the effectivity of this Guidelines, all ICREs shall prepare and have available for inspection their new/updated and BOD-approved ML/TFPP embodying the principles and provisions stated in this Guidelines.

In case of newly licensed ICRE, it shall have one hundred eighty (180) days from receipt of Certificate of Authority to formulate its ML/TFPP consistent with the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances.

Each MLPP shall be regularly updated at least once every two (2) years to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent IC and/or AMLC issuances. Any revision or update in the ML/TFPP shall likewise be approved by the BOD.

The compliance officer shall submit to the IC not later than fifteen (15) days from the approval of the Board of Director of the new/updated ML/TFPP a sworn certification that a new/updated ML/TFPP has been prepared, duly noted and approved by the ICREs' BOD.

Section 12. Internal Controls and Internal Audit Program. – The ICREs shall establish internal controls to ensure day-to-day compliance with its AML/CFT obligations under the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances, taking into consideration the size and complexity of its operations.

Qualified personnel who are independent of the unit being audited shall conduct internal audits for the ICREs. The auditors shall have the support and a direct line of communication to the ICREs' Board of Directors. The ICREs' internal audit program shall include periodic and independent evaluation of the ICREs' risk management, as well as the sufficiency and degree of adherence to its

compliance measures. Internal audit examination scope shall cover the accuracy of customer identification information, covered and suspicious transaction reports, and all other records and internal controls pertaining to compliance with AML/CFT obligations. Internal audits shall be conducted at least once every year or at such frequency as necessary, consistent with the risk assessment of the ICREs.

The results of the internal audit shall be timely and directly communicated to the ICREs' Board of Directors, senior management and the compliance officer. There shall also be a written procedure by which deficiencies in a compliance program are promptly remedied once identified by an internal audit. Moreover, audit results relative to AML/CFT compliance shall promptly be made available to the IC upon request during compliance checking.

Section 13. Customer Due Diligence. – ICRE shall adopt a policy that before a business relationship is established, it should take steps to identify its customers and verify his/her identity on the basis of documents, data and information obtained from the customer and from reliable independent sources, and obtain information that should enable them to assess the extent of risk to which the customer may expose them.

Section 14. Monitoring and Reporting System. – All ICRE shall adopt an ML/TF monitoring system, including a name screening mechanism, whether electronic or manual, that is appropriate for their risk-profile and business complexity in accordance with this Guidelines. The system shall be capable of generating timely, accurate and complete reports, including CTRs and STRs, and to regularly apprise the ICREs' Board of Directors on AML/CFT compliance.

All insurance and reinsurance companies shall adopt an electronic AML/CFT system capable of monitoring risks associated with ML/TF as well as generating timely reports for the guidance and information of its board of directors and senior management.

Section 15. Record Keeping. – All ICREs shall adopt a policy to keep records of their customer's transactions and documents obtained during the customer due diligence for at least five (5) years.

Section 16. Employee Training Program. – ICRE shall create employee training programs that detail ML and TF prevention roles and hiring standards that promote high ethical standards in order to protect the safety and integrity of the ICREs' business.

Training programs shall be ongoing programs that alert directors, officers, and employees on their collective and distinct roles in preventing ML and TF. The ICREs shall also provide for refresher trainings to review updates to compliance measures as they arise from new legislation, IC and/or AMLC issuances, internal audit findings, and discoveries in ML/TF trends and detection techniques. In particular, the AML/CFT trainings shall explain the customer identification process, record keeping requirements, covered and suspicious transaction reporting, and the internal processes/chain of command for reporting and

cooperation with the IC.

Attendance by ICREs' personnel at all training programs and seminars, whether internally or externally organized shall be recorded. Copies of training materials shall be kept and submitted to the compliance officer, which shall be made available to the IC upon request during compliance checking.

ICREs' annual AML/CFT training program and records of all AML/CFT seminars and trainings conducted by the ICREs and/or attended by its directors, officers, and employees (internal or external), including copies of AML/CFT seminar/training materials, shall be appropriately kept and submitted to compliance officer, and should be made available during periodic or special IC compliance checking.

Section 17. Investigative, Administrative and Judicial Compliance. – The ICREs shall have written procedures for cooperating and complying with investigations, assessments, directives and orders of the IC, the AMLC, other competent authorities and the courts, as the case may be. When the ICREs receive a request for information from any competent authority regarding inquiries into potential ML or TF activity carried on, the ICREs shall promptly inform the IC in writing.

Section 18. New Products and Business Practices. – The ICREs are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

TITLE V CUSTOMER DUE DILIGENCE

Section 19. Customer Due Diligence (CDD). – The ICREs shall know their customers and, to the extent possible, the person or entity on whose behalf the transaction is being conducted. The ICREs shall create a system that will first establish and then record the full identity of their customers and risk assessment results. In addition to using all information available to them, the ICREs shall require customers to furnish the required Identification Documents.

Section 20. Risk-Based CDD Standards. – Consistent with all AML/CFT compliance measures, ICREs' CDD procedures shall be risk-based, requiring enhanced diligence for customers posing a high-risk of ML/TF and permitting reduced due diligence for customers posing a low-risk of ML/TF. The ICREs shall therefore document clear policies and procedures, including guidelines and criteria for determining which customers pose low, normal, or high risk of ML and TF. The ICREs' internal risk classifications shall reflect the idiosyncratic risks to its operations, requiring an intimate knowledge of the risks inherent to their operations and the acquisition of relevant expertise to make such risk assessments.

The customer's risk classification, on risk-based approach, may include the customer's source of funds, occupation, residence or origin, status as PEPs, adverse media exposure, appearance on government, international and industry watch lists; the types of services, products, and transactions sought by the customer; and the presence of linked accounts. The ICREs shall document the risk classification and level of CDD applied to each customer.

Section 21. When to Conduct CDD. – The ICREs shall undertake satisfactory CDD measures:

- a. Before establishing business relationship;
- b. There is any suspicion of Money Laundering or Terrorist Financing; and
- c. The ICREs have doubts about the integrity or adequacy of previously obtained customer identification information.

Provided, that where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the ICREs may complete verification after the establishment of business relationship so as not to interrupt normal conduct of business. The verification of the identity of the customer shall be conducted during the duration of the policy/plan/agreement or at the time the customer files his/her claim, as the case may be.

Section 22. CDD Standards. – The ICREs shall implement the following standards of CDD. –

- a. Identify and verify the identity of a customer using reliable, independent source documents, data or information.
- b. Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
- c. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the information or data obtained from a reliable source, such that identity of the beneficial owners is established;
- d. Understand and, where relevant, obtain information on, the purpose and intended nature of the business relationship; and
- e. Conduct ongoing due diligence on the business relationship.

Section 23. Customer Identification. – The ICREs shall establish appropriate systems and methods, and adequate internal controls, compliant with the AMLA, as amended, this Guidelines, and other applicable IC and AMLC issuances for verifying and recording the true and full identity of their customers based on reliable, independent sources, documents, data or information, as defined under Section 4 (M) of this Guidelines, before establishment of a business relationship.

In the case of corporate customers, including a trustee, agent, nominee, or intermediary arrangements, the ICREs are required to maintain a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf.

Section 24. Minimum Customer Information and Identification Documents when Conducting Customer Due Diligence. – The following are the minimum customer information and identification documents required in the conduct of CDD:

A. For New Individual Customer. The ICREs shall develop a systematic procedure for establishing the true and full identity of new individual customers, and shall open and maintain the business relationship only in the true and full name of the account owner/s. Unless otherwise stated in this Guidelines, average customer due diligence requires that the ICREs obtain from individual customers, before establishing the business relationship, the following minimum information and confirming these information with the official or valid identification documents:

1. Name of customer;
2. Date and place of birth;
3. Name of beneficial owner, if applicable;
4. Name of beneficiary;
5. Present address;
6. Permanent address;
7. Contact number or information;
8. Nationality;
9. Specimen signature or biometrics of the customer;
10. Proof of Identification and Identification Number;
11. Nature of work and name of employer or nature of self-employment/ business, if applicable;
12. Sources of funds or property; and
13. Tax Identification Number (TIN), Social Security System (SSS) number, or Government Service Insurance System (GSIS) number, if applicable.

Customers who transact business with the ICREs shall be required to present an identification document and to submit a clear copy thereof.

Where the customer or authorized representative is a foreign national, the ICREs shall require said foreign national to present valid passport, Alien Certificate of Registration, Alien Employment Permit, or any government issued identification document bearing the photograph of the customer or beneficial owner, provided that the ICREs can be satisfied with the authenticity of the document.

B. For New Corporate and Juridical Entities/Sole Proprietorships. The ICREs shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities, as well as their stockholders/ partners/ owners, directors, officers and authorized signatories. It shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in

the process of being dissolved, struck-off, wound-up, terminated or otherwise placed under receivership or liquidation.

Unless otherwise stated in this Guidelines, average due diligence requires that the ICREs obtain the following before establishing business relationships:

Minimum information:

1. Name of the entity;
2. Name, present address, date and place of birth, nationality, nature of work and source of funds of the beneficial owner, beneficiary, if applicable, and authorized signatories;
3. Official address;
4. Contact number or information;
5. Nature of business;
6. Specimen signature or biometrics of the authorized signatory;
7. Verified identification of the entity as a corporation, partnership, sole proprietorship;
8. Verified identification of the entity's source of funds and business nature of the entity;
9. Verification that the entity has not been or is not in the process of being dissolved, struck-off, wound-up, terminated, placed under receivership, or undergoing liquidation; and
10. Verifying with the relevant supervisory authority the status of the entity.

Corporate documents:

1. Certificates of registration issued by the Department of Trade and Industry (DTI) for single proprietors; and the SEC for corporations and partnerships;
2. Secondary License or Certificate of Authority issued by the Supervising Authority or other government agency;
3. Articles of incorporation or association and the entity's by-laws;
4. A resolution by the ownership (board of directors or other governing body, partners, sole proprietor, etc.), authorizing the signatory to sign on behalf of the entity;
5. Latest General Information sheet which lists the names of directors/trustees/partners, principal stockholders owning at least twenty five percent (25%) of the outstanding capital stock and primary officers such as the President and Treasurer;
6. Identification documents of the owners, partners, directors, principal officers, authorized signatories and stockholders owning at least twenty five percent (25%) of the business or outstanding capital stock, as the case may be.

For entities registered or incorporated outside the Philippines, equivalent documents/information duly authenticated by the Philippine Consulate where

said entities are registered shall be obtained.

The ICREs should be able to understand the nature of the customer's business, its ownership and control structure.

C. Legal Arrangements

For legal arrangements, the ICREs are required to identify and verify the identity of the beneficial owners through the following information:

1. For trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);
2. For other types of legal arrangements, the identity of persons in equivalent or similar positions.

The ICREs should be able to understand the nature of the customer's business, its ownership and control structure.

D. Valid Identification Documents.

1. Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with the ICREs for the first time shall be required to present official identification document which shall include any of the official documents as defined in this Guidelines or other identification information which can be verified from reliable, independent source, documents, data or information, such as third-party verified customer information database.
2. The ICREs may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer. Whenever it deems necessary, the ICREs may accept other IDs not provided herein: Provided, That it shall not be the sole means of identification.

In case the identification document presented does not bear any photo of the customer or authorized signatory, or the photo-bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory, the ICREs may utilize its own technology to take the photo of the customer or authorized signatory.

Section 25. Identification and Verification of a Beneficial Owner, Trustee, Nominee, or Agent. – The ICREs shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing

their relationship and apply the same standards for assessing the risk profile and determining the standard of due diligence to be applied to both. In case it entertains doubts as to whether the account holder or transactor is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence or file a suspicious transaction report, if warranted.

Section 26. Customer Risk Assessment. – The ICREs shall develop clear, written and graduated customer acceptance policies and procedures, including a set of criteria for customers that are likely to pose low, normal, or high risk to their operations.

The ICREs 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 refusal to conduct the transaction.

Enhanced due diligence shall be applied to customers that are assessed by the ICREs or under this Guidelines as high risk for ML/TF. For customers assessed to be of low risk, the ICREs may apply reduced due diligence.

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:

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

Section 27. High-Risk Customers. – High-risk customers include those that originate from a country that is recognized as having inadequate internationally-accepted anti-money laundering standards; does not sufficiently regulate businesses to counteract money-laundering; fails to incorporate Financial Action Task Force (FATF) recommendations into its regulatory regimes; or exhibits a relatively high prevalence or risk of crime, corruption, or terrorist financing.

A customer from a foreign jurisdiction that is recognized as having inadequate internationally accepted AML/CFT standards, or presents greater risk for ML/TF

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

Section 28. Shell Company. The ICREs shall undertake business relationship with a shell company with extreme caution and shall always apply enhanced due diligence on both the entity and its beneficial owner/s.

Section 29. Enhanced Due Diligence (EDD). – The ICREs should employ EDD if it acquire information that:

- A. Raises doubt as to the accuracy of any information or document provided by the customer or the ownership of the entity;
- B. Justifies re-classification of the customer from low or normal risk to high-risk;
- C. When establishing business relationship with any person from countries identified by the FATF or AMLC as having on-going or substantial ML/TF risks;
- D. Warrants the filing of a Suspicious Transaction Report (STR) exists, including information that:
 - 1. The customer is transacting without any purpose, economic justification, or underlying legal or trade obligation;
 - 2. The customer is transacting an amount that is not commensurate to the business or financial capacity of the customer or deviates from the profile of that customer;
 - 3. The customer might have structured transactions to avoid being the subject of a Covered Transaction Report;
 - 4. The customer has been or is currently engaged in any unlawful activity; or
 - 5. Raises suspicions that an intermediary is being used to circumvent anti-money laundering compliance measures.

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

- A. Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of average due diligence:
 - 1. 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 is a stockholder,

director, officer, or authorized signatory; iv. other relevant information available through public databases or internet; v. a list of banks where the individual has maintained or is maintaining an account; vi. name, present address, date and place of birth, nationality, nature of work and source of funds of the beneficial owner and beneficiary, if applicable; vii. clear copy of identification document of beneficial owner; and viii. obtaining a copy of the written document evidencing the relationship between account holder or transactor and beneficial owner.

2. In case of legal entities – i. list of banks where the entity has maintained or is maintaining an account; ii. the verified name, nationality, present address, date and place of birth, nature of work, and sources of assets of the primary officers of the entity (i.e. President, Treasurer, authorized signatories, etc.), directors, trustees, partners, as well as all stockholders owning five percent (5%) or more of the business or voting stock of the entity, as the case may be; 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 statement, etc.); iv. reasons for intended or performed transactions; and vii. obtaining a copy of the written document evidencing the relationship between account holder or transactor and beneficial owner.

- B. Conduct validation procedures on all of the information provided;
- C. Secure senior management approval to commence or continue business relationship/transacting with the customer;
- D. 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;
- E. 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
- F. Perform such other measures as the ICRES may deem reasonable or necessary.

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 ICRES shall deny the application of the customer without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

The ICRES should ensure that it is aware of new or developing technologies that might favor anonymity and take measures to prevent their use to carry out ML or TF.

The ICRES shall make appropriate use of relevant findings issued by the AMLC concerning any named individuals, groups or entities that are the subject of

money laundering or terrorist financing investigations or included in sanctions lists issued by international competent authorities. Regarding various individuals and entities, the ICREs shall know prior to establishing a customer relationship:

- A. The identity of the person;
- B. The type of activity/relationship he/she wants to conduct with the ICREs;
- C. The complexity of the transaction;
- D. Whether or not the customer is representing a third party; and
- E. How to verify the information presented.

The customer data of high risk customer shall be updated more regularly.

Section 30. Minimum Validation Procedures for EDD. The procedures performed must enable the ICREs to achieve a reasonable confidence and assurance that the informations 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 documents;
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 email;
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. 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 email.

Section 31. Reduced Due Diligence. Where lower risks of ML/TF have been identified, through an adequate analysis of risk by the ICREs, reduced due diligence procedures may be applied. The reduced due diligence procedures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

Whenever reduced due diligence is applied as provided in this Guidelines or in

the ICRES' customer acceptance policy, the following rules shall apply:

1. For individual customers, the ICRES may establish relationship under the true and full name of the customers upon presentation of an acceptable identification card (ID) or official document as defined in this Guidelines or other reliable, independent source documents, data or information.
2. For corporate, partnership, and sole proprietorship entities, the ICRES may establish relationship under the official name of these entities by presenting a Board Resolution duly certified by the Corporate Secretary, or equivalent document, authorizing the signatory to sign on behalf of the entity, obtained at the time of account opening.

Verification of the identity of the customer, beneficial owner or authorized signatory can be made after the establishment of the business relationship.

Section 32. New Technologies. The ICRES shall take reasonable measures to prevent the use of new technologies for ML/TF purposes.

The ICRES shall conduct ML/TF risk assessment:

- a. Prior to the introduction of a new product, new business practice or new technology for both new and pre-existing products;
- b. So as to assess ML/TF risks in relation to:
 - i. A new product and a new business practice, including a new delivery mechanism; and
 - ii. New or developing technologies for both new and preexisting products.

The outcome of such assessment shall be documented and be available to the IC upon request during compliance checking.

Section 33. Life Insurance Related Business. For life or other investment-related insurance business, insurance companies shall, in addition to the customer due diligence measures required for the customer and the beneficial owner, conduct the following customer due diligence measures on the beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiary or beneficiaries are identified or designated, for a beneficiary:

- a. That is identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;
- b. That is a legal arrangement or designated by characteristics or by category such as spouse or children, at the time that the insured event occurs or by other means such as under a will, obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be

able to establish the identity of the beneficiary at the time of the pay-out but before funds are disbursed.

In both cases, the identity of the beneficiary should be verified at the time of the payout. The beneficiary, if known, should be part of the risk factors on the basis of which the life insurer or intermediary will determine if the relationship is higher risk and enhanced due diligence measures should be applied.

The information collected shall be recorded and maintained in accordance with the requirements under Title VI of this Guidelines.

Section 34. Ongoing Monitoring of Customers, Accounts and Transactions.

– The ICREs are required to conduct on-going due diligence on the business relationship with its customers.

- a. The ICREs shall scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and
- b. Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

The ICREs shall also provide for a mechanism by which customers' transactions and identification information will be continuously monitored and updated. They shall create a system that will enable them to understand the normal and reasonable account activity of their customers given the customer's activities, risk profile, and source of funds and to thereby detect unusual or suspicious patterns of activities or behaviors.

Section 35. Ongoing CDD and Monitoring of Existing Customers. –

- A. The ICREs shall ensure that they have established the true and full identity of their customers and shall, on the basis of materiality and risk, update, no later than once every two (2) years, all customer identification information and documents, including photo, required to be obtained this Guidelines, unless enhanced ongoing monitoring is warranted.

The ICREs shall establish a system that will enable them to understand the normal and reasonable account or business activity of customers to ensure that the customers' accounts and transactions are consistent with their knowledge of the customers, and the latter's commercial activities, risk profile, and source of funds and detect unusual or suspicious patterns of account activity. Thus, a risk-and-materiality-based on-going monitoring of customer's accounts and transactions should be part of a ICREs' customer due diligence.

- B. The ICREs shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions, which

have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. The ICREs shall apply enhanced due diligence on the customer if they acquire information in the course of customer account or transaction monitoring that:

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

If the ICREs fail to satisfactorily complete the enhanced due diligence procedures or reasonably believes that performing the enhanced due diligence process will tip-off the customer, it shall file a suspicious transaction report, and closely monitor the account and review the business relationship.

Section 36. Face-to-Face Contact. – The ICREs shall conduct face-to-face contact at the time of establishment of the business 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 ML and TF risks are effectively managed. Provided further, that no transaction shall be processed without conducting a face-to-face contact.

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

Section 37. Third Party Reliance. – ICRE may rely on a third party to perform customer identification and face-to-face contact. The third party shall be a covered person as defined under Section 3 (a) of the AMLA, as amended or a financial institution operating outside the Philippines that is covered by equivalent customer identification and face-to-face requirements.

Where the third party is a covered person defined under the AMLA, as amended, and its RIRR, the ICREs shall obtain from the third party a written sworn

certification containing the following:

- a. The third party has conducted the prescribed customer identification procedures in accordance with this part and its own ML/TFPP, including the face-to-face contact requirement, to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and
- b. The relying ICREs shall have the ability to obtain identification documents from the third party upon request without delay.

Where the third party is a financial institution operating outside the Philippines that is other than covered persons as defined under Section 3 (A) of the AMLA but conducts business operations and activities similar to them, all the contents required in the sworn certification mentioned above shall apply, with the additional requirement that the laws of the country where the third party is operating has equal or more stringent customer identification process requirement and that it has not been cited for violation thereof. The ICREs shall, in addition to performing normal due diligence measures, do the following:

- a. Gather sufficient information about the third party and the group to which it belongs to understand fully the nature of its business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to ML or TF investigation or regulatory action;
- b. Document the respective responsibilities of each institution; and
- c. Obtain approval from senior management at inception of relationship before relying on the third party.

Notwithstanding the foregoing, the ultimate responsibility and accountability for identifying the customer and conducting CDD remains with the ICREs relying on the third party. Provided that, in cases of high-risk customers, the ICREs relying on the third person shall also conduct enhanced due diligence procedure.

Section 38. Outsourcing the Conduct of Customer Identification and Due Diligence. – The ICREs may outsource the conduct of customer identification and due diligence, including face-to-face contact, to a counterparty, intermediary or agent. The customer identification and due diligence performed by the counterparty or intermediary shall be regarded as those of the ICREs itself. The ultimate responsibility and accountability for identifying the customer and keeping the identification documents remains with the ICREs.

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

The ICREs are, however, prohibited from relying on third parties located in countries that have been identified as having on-going or substantial ML/TF risks.

The ICREs and counterparty, intermediary or agent shall enter into an agreement clearly specifying the following minimum responsibilities of the latter:

- a. can obtain immediately the necessary information concerning CDD as required under this Guidelines;
- b. has an adequate CDD process;
- c. has measures in place for record keeping requirements; and
- d. can provide the CDD information and provide copies of the relevant documentation immediately upon request.

The counterparty, intermediary or agent in performing the conduct of customer identification and due diligence, as a minimum, must comply with the requirements provided under the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances.

Section 39. Trustee, Nominee, Agent or Intermediary Account. Where an account is opened by, relationship is established through, or any transaction is conducted by a trustee, nominee, agent or intermediary, either as an individual or through a fiduciary relationship or similar arrangements, the ICREs shall establish and record the true and full identity and existence of both the (1) trustee, nominee, agent or intermediary; and (2) trustor, principal, beneficial owner or person on whose behalf the account/business relationship/transaction is being opened/established/conducted. The ICREs shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of due diligence to be applied to both.

In case of several trustors, principals, beneficial owners, or persons on whose behalf the account is being opened/ business relationship is being established, where the trustee, nominee, agent or intermediary opens a single account but keeps therein sub-accounts that may be attributable to each trustor, principal, or beneficial owner, the ICREs shall, at the minimum, obtain the true and full name, place and date of birth or date of registration, as the case may be, present address, nature of work or business and source of funds as if the account was opened by them separately. Where the ICREs is required to report a covered transaction or circumstances warrant the filing of a suspicious transaction, it shall obtain such information on every trustor, principal, beneficial owner, or person on whose behalf the account is being opened in order that a complete and accurate report may be filed with the AMLC.

In case ICREs have doubts as to whether the trustee, nominee, agent, or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence and file a suspicious transaction report, if warranted.

Section 40. Trust Accounts. Where trusts or similar arrangements are used,

particular care will be taken in understanding the substance and form of the entity. Where the customer is a trust, the ICREs will verify the identity of the trustees, any other person exercising effective control over the trust property, the settlors and the beneficiaries. Verification of the beneficiaries will be carried out prior to any payments being made to them.

Section 41. Politically Exposed Persons. – In addition to establishing the full identities of PEPs, the ICREs shall also establish and record the identities of the immediate family members and entities if publicly known to be related to the PEP. The ICREs shall carefully consider a PEP's position and the position's attendant risks with respect to money laundering and terrorist financing in determining what standard of due diligence shall apply to them.

- a. 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, the ICREs shall:
 - i. Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
 - ii. In cases when there is a higher risk business relationship, adopt measures under paragraphs b(ii), b(iii) and b(iv) below.

- b. In relation to foreign PEPs or their immediate family members or close associates, in addition to performing the applicable customer due diligence measures, the ICREs shall:
 - i. Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
 - ii. Obtain senior management approval before establishing (or continuing, for existing customers) such business relationship;
 - iii. Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
 - iv. Conduct enhanced ongoing monitoring on that relationship.

Section 42. Customer Acceptance Policies. – The ICREs shall have clear, written and graduated acceptance policies and procedures that will seek to prevent suspicious individuals or entities from transacting with, establishing or maintaining business relationship with them. The ICREs shall develop guidelines to assist personnel to assess whether a customer's profile warrants refusal of service to protect the security and integrity of the business.

Section 43. Customer Refusal Policies. – The ICREs should have written guidelines on when a customer's risk profile warrants refusal of service to protect the security and integrity of the ICREs' business. Thus, if the prospective customer is unable to comply with any of the CDD measures, the ICREs shall not commence business relations, accept instructions or perform any transaction. If

necessary, the ICREs should file an STR with the AMLC.

Section 44. Prohibited Accounts. – Anonymous accounts and accounts under fictitious names shall be prohibited, and the ICREs shall maintain customers' account only in the true and full name of the account owner or holder.

Where an account is opened or a transaction is conducted by any person in behalf of another, the ICREs shall establish and record the true and full identity and existence of both the account holder or transactor and the beneficial owner or person on whose behalf the transaction is being conducted.

Section 45. Termination of Business Relationship. – Where CDD obligations for existing business relationships and customers are not met, as a result of the customer's refusal to comply or where the customer causes unacceptable delays, the ICREs shall terminate the business relationship and consider the filing of Suspicious Transaction Report (STR) to the AMLC.

Section 46. Tipping Off – In case where the ICREs form a suspicion of ML/TF and reasonably believes that performing CDD process would tip off the customer, the ICREs is permitted not to pursue the CDD process. In such circumstances, the ICREs may proceed with the transaction and immediately file a Suspicious Transaction Report with the AMLC.

TITLE VI RECORD KEEPING

Section 47. Record Keeping Management and Requirements. – The ICREs shall retain all records as originals or in such forms as are admissible in court, pursuant to existing laws, such as the E-Commerce Act, and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court.

The ICREs shall maintain records in an organized and confidential manner, which allows the IC, AMLC, other competent authorities and the courts to establish an audit trail for money laundering and terrorism financing.

The ICREs shall ensure that all CDD information and transaction records are available swiftly to the IC, AMLC and other competent authorities upon appropriate authority.

Section 48. Period to Keep Records. – The ICREs shall maintain and safely store for at least five (5) years from the dates of transactions all records of customer identification and transaction documents, or as long as the business relationship exists. If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5) -year periods, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

The ICREs shall also maintain and safely store for at least five (5) years from the

dates the accounts were terminated, all records of customer identification and transaction documents. The ICREs shall likewise keep the electronic copies of all covered and suspicious transaction reports for at least five (5) years from the dates of submission to the AMLC.

Section 49. Records of Information on Covered and Suspicious Transaction Reports (CTRs and STRs). – The ICREs shall maintain records concerning its internal reporting of CTRs and STRs, and decision-making whether to file or not to file said reports with the AMLC, for at least a period of five (5) years after the date of transaction.

Section 50. Access to Data. – The ICREs shall ensure that there are no secrecy or data protection issues that would restrict prompt access:

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

TITLE VII COVERED AND SUSPICIOUS TRANSACTION REPORTING

Section 51. Reporting of Covered and Suspicious Transactions. – The ICREs shall report to the AMLC all covered transactions and suspicious transactions within five (5) working days from the occurrence thereof, unless the AMLC prescribes a different period not exceeding fifteen (15) working days.

When the total amount of the premiums/fees for a policy, plan or agreement for the entire year, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), exceeds Five Hundred Thousand pesos (Php500,000.00), such amount shall be reported as a covered transaction, even if the amounts of the amortizations are less than the threshold amount. The CTR shall be filed upon payment of the first premium/fee amount, regardless of the frequency of payment. Under this rule, the ICREs shall file the CTR only once every year until the policy, plan or agreement matures or rescinded, whichever comes first.

For suspicious transactions, “*occurrence*” refers to the date of determination of the suspicious nature of the transaction, which determination shall be made not exceeding ten (10) calendar days from date of transaction.

In cases where the transaction is in any way related to an unlawful activity, or the person transacting is involved in or connected to an unlawful activity or money laundering offense, the ten (10) calendar day determination period shall be reckoned from the date the ICREs knew of, or should have known, the suspicious transaction indicator. To determine whether the ICREs knew or should have known the suspicious transaction indicator, it shall be given a reasonable period of time, which in no case shall exceed sixty (60) calendar days, to gather facts in order to enable the submission of a meaningful STR.

The ICREs shall take note and record instances where a transaction is initially flagged as potentially suspicious, even if they do not ultimately report the transaction through an STR, to facilitate ongoing monitoring of a given customer's transactions.

Should a transaction be determined to be both a covered transaction and a suspicious transaction, it shall be reported by the ICREs as a suspicious transaction.

The ICREs shall ensure the accuracy and completeness of covered and suspicious transaction report, which shall be filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.

Section 52. Guidelines in Reporting of Covered and Suspicious Transactions. – The filing of CTRs and STRs shall be in accordance with the AMLC Registration and Reporting Guidelines (ARRG) and any amendments thereto.

Section 53. STR Framework. – The ICREs shall observe the following rules in reporting suspicious transactions:

- a. The ICREs shall have relevant policies, procedures, processes and controls in place that would enable an employee to report to the Compliance Officer any suspicion or knowledge of ML or TF activity and/or transaction that is detected or identified;
- b. If the ICREs suspect or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity or are related to Money Laundering or Terrorist Financing, the Compliance Officer shall promptly file an STR with the AMLC as provided for under the ARRG;
- c. The Compliance Officer shall ensure that every employee is aware of his role and duty to receive or submit internal STRs;
- d. The Compliance Officer shall investigate STRs internally, build an internal report outlining the outcome of his investigation including the decision on whether or not to file an STR with the AMLC;
- e. Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing;
- f. In the event the Compliance Officer concludes that no external report should be submitted to the AMLC, the justification of such a decision should be documented;
- g. The ICREs shall institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there is evidence for him/her to do so; and
- h. The ICREs shall monitor indicators of suspicious activities, such as, but not

limited to those listed in **Annex A** hereof, and perform EDD as necessary.

Section 54. Deferred Reporting of Certain Covered Transactions. The ICREs shall refer to the issuances of the AMLC from time to time on transactions that are considered as "*non-cash, no/low risk covered transactions*", hence subject to deferred reporting.

The IC may consider other transactions as "*no/low risk covered transactions*" and propose to the AMLC that they be likewise subject to deferred reporting by the ICREs.

Section 55. Electronic Monitoring Systems for AML/CFT. The ICRE's electronic monitoring system must have at least the following automated functionalities:

- a. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
- b. Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
- c. Investigation – checks for given names throughout the history of payment stored in the system;
- d. Can generate all the CTRs of the ICREs accurately and completely with all the mandatory field properly filled up;
- e. Must provide a complete audit trail;
- f. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
- g. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

The ICREs required to have an electronic monitoring system for AML/CFT shall be given one hundred eighty (180) days from the effectivity of this Guidelines to adopt and make their system fully operational and automated with all the functionalities stated above.

The ICREs with existing electronic system of flagging and monitoring transactions already in place shall ensure that their existing system is updated to be fully compliant with functionalities as those required herein.

Section 56. Manual Monitoring. The ICREs that are not required under this Guidelines to have an electronic system of flagging and monitoring transactions shall ensure that they have the means of flagging and monitoring the transactions mentioned above. They shall maintain a register of all STs that have been brought to the attention of senior management whether or not the same was reported to the AMLC.

Section 57. Electronic Submission of Reports and Registration with the

AMLC. The CTR and STR shall be submitted to the AMLC in a secured manner, in electronic form and in accordance with the ARRG. The ICREs shall provide complete and accurate information of all the mandatory fields required in the report. In order to provide accurate information, the ICREs shall regularly update customer identification information at least once every two (2) years.

For the purpose of reporting in a secured manner, all ICREs shall register and/or update their registration within the period prescribed by the AMLC by directly coordinating with the latter. All ICREs that have previously registered need not re-register.

In the case of newly-licensed ICREs, registration must be done not later than thirty (30) days from receipt of their Certificate of Authority from the IC.

Only their respective compliance officers or duly authorized officers shall electronically sign their covered transaction reports and suspicious transaction reports.

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

Section 58. Confidentiality of Reporting - When reporting covered or suspicious transactions, the ICREs and 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 has been or is about to be reported, the contents of the report, or any other information in relation thereto.

Any information about such reporting shall not be published or aired, in any manner or form, by the mass media, or through electronic mail, or other similar devices.

In case of violation thereof, the concerned officer and employee of the ICREs and media shall be held criminally liable.

Section 59. Safe Harbor Provision. - No administrative, criminal or civil proceedings shall lie against any person for having made a covered transaction or suspicious transaction report in the regular performance of his/her duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law.

TITLE VIII COMPLIANCE CHECKING

Section 60. Authority to Check Compliance – The IC shall have the authority to conduct compliance checking to validate the compliance of the ICREs with the requirements of the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines, and other applicable IC and AMLC issuances.

For the said purpose, the ICREs shall immediately make available, give full access and submit to the compliance checker any and all information and documents, including customer identification, account opening and transaction documents, as he or she may require and the latter shall also have the power to interview the officers and staffs of the ICREs during compliance checking.

**TITLE IX
ADMINISTRATIVE ACTIONS**

Section 61. Administrative Actions. – The IC shall impose administrative sanctions upon any ICREs, including its board of directors, senior management and officers, for violation of this Guidelines, or for failure or refusal to comply with the orders, resolutions and other issuances of the IC.

Section 62. Enforcement Action. In line with the objective of ensuring that the ICREs maintain high anti-money laundering standards in order to protect its safety and soundness, violation of this Guidelines shall constitute a major violation subject to the following enforcement actions against the board of directors, senior management and officers, not necessarily according to priority and whenever applicable:

- a. Written reprimand;
- b. Suspension or removal from the office they are currently holding; or
- c. Disqualification from holding any position in any covered persons.

Further, failure to comply with the requirements under this Guidelines shall be taken into account in the renewal of the ICREs' Certificate of Authority.

Section 63. Table of Violations and Corresponding Fines. – In addition to the non-monetary sanctions stated above, the IC shall also impose monetary penalties against the ICREs based on the following specific violations and their corresponding fines:

GRAVE VIOLATION	FINE
Non-compliance with the requirement to immediately make available, give full access and submit to the compliance checker any and all information and documents, including customer identification, account opening and transaction documents, as he or she may require and/or to allow the officers and staffs of the ICREs be interviewed during compliance checking	P200,000.00 per account
MAJOR VIOLATIONS	FINES
Non-compliance with the requirement to establish and record the true identity of each customer and/or the person on	P150,000.00 per customer

whose behalf the transaction is being conducted	
Non-compliance with the requirement to retain and safely keep records beyond the five (5)-year period, where the account is the subject of a case, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality	P150,000.00 per account
Non-compliance with the requirement to report to the AMLC covered and suspicious transactions. Reporting of covered and suspicious transactions to the AMLC beyond the prescribed period shall constitute non-compliance with the requirement to report	P150,000.00 per transaction
SERIOUS VIOLATIONS	FINES
Non-compliance with the requirements on Face-to-Face Contact	P100,000.00 per account
Non-compliance with the requirements on customer risk assessment	P100,000.00 per account
Non-compliance with the requirements on institutional risk assessment at least once every two (2) years	P100,000.00
Non-compliance with the requirements on new product, new business practice or new technology risk assessment	P100,000.00 per new product, new business practice or new technology
Non-compliance with the requirements of the provisions on Politically-Exposed Persons	P100,000.00 per customer
Non-compliance with the requirements of the provisions on Customer from High-Risk Jurisdiction	P100,000.00 per customer
Non-compliance with the requirement to monitor and update all information and identification documents of existing customers	P100,000.00 per customer
Non-compliance with the requirement to establish a monitoring system for AML/CFT	P100,000.00
Allowing the opening of anonymous accounts, accounts under fictitious names, and all other similar accounts	P100,000.00 per account
Non-compliance with the requirement to maintain and safely store for at least five (5) years from the dates of transactions, or from dates the accounts were closed, all records of transactions, including customer	P100,000.00 per account

identification documents	
Non-compliance with the requirement to register with the AMLC's electronic reporting system within within the period prescribed by the AMLC	P5,000.00 per day of delay
Non-compliance with the requirement to register with the AMLC's electronic reporting system registration not later than thirty (30) days from receipt of newly-licensed ICREs of their Certificate of Authority from the IC	P5,000.00 per day of delay
Non-compliance with the requirement to update registration with the AMLC's electronic reporting system as required under the ARRG	P5,000.00 per day of delay
Non-compliance with the requirement to formulate or update the ML/TFPP in accordance with the provisions of the AML and CFT Laws, their respective implementing rules and regulations, this Guidelines and applicable IC and AMLC issuances	P100,000.00 per compliance checking period
LESS SERIOUS VIOLATIONS	FINES
Non-compliance with the requirement to obtain all the minimum information required from individual customers and juridical entities	P50,000.00 per account
Non-compliance with the requirement to provide all responsible officers and personnel with efficient and effective anti-money laundering training and continuing education programs	P50,000.00 per compliance checking period
LIGHT VIOLATIONS	FINES
Non-compliance with the requirement to keep electronic copies of all CTRs or STRs for at least five (5) years from the dates of submission to the AMLC	P50,000.00 per violation
Non-compliance with the requirement to submit to the IC not later than fifteen (15) days from the approval of the BOD of the new/updated ML/TFPP a sworn certification that a new/updated ML/TFPP has been prepared, duly noted and approved by the ICREs' BOD	P5,000.00 per day of delay
Non-submission of an acceptable BOD-approved plan within the deadline or failure to implement its action plan	P5,000.00 per day of delay

However, in no case shall the aggregate fine exceed 1% of the total asset based on latest IC approved financial condition of the concerned ICREs.

Further, the monetary penalties on the foregoing specific violations shall not be imposed in case the specific acts or omissions constituting the violations have already been:

- a. Penalized by the AMLC;
- b. Corrected/rectified by the ICRE; and
- c. Corresponding fines thereof were fully paid by the concerned ICRE.

Non-payment of the penalty imposed for violating this Guidelines shall be taken into account in the renewal of the Certificate of Authority.


TITLE X MISCELLANEOUS PROVISIONS

Section 64. Applicability of the AML and CFT Laws and their Respective Implementing Rules and Regulations. – The provisions of the AMLA, as amended, The Terrorism Financing Prevention and Suppression Act, their respective implementing rules and regulations, and any amendments thereto shall apply in analogous and suppletory character whenever practical and convenient.

Section 65. Separability Clause. – If any provision of this Guidelines is declared unconstitutional, the same shall not affect the validity and effectivity of other provisions hereof.

Section 66. Repealing Clause. – All IC circular letters, rules, regulations and other issuances, or parts thereof, that are inconsistent with this Guidelines are hereby repealed, amended or modified accordingly.

Section 67. Effectivity. – This Guidelines shall take effect fifteen (15) days following its publication in a newspaper of general circulation.


DENNIS B. FUNA
Insurance Commissioner



ANNEX "A"

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s), pre-need plan(s) or HMO agreement(s) where the source of the funds is unclear or not consistent with the customer's apparent standing;
2. A sudden request for a significant purchase of a lump sum contract with an existing customer whose current contracts are small and of regular payments only;
3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment;
4. A proposal to purchase and settle by cash;
5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer;
6. The prospective customer who does not wish to know about investment performance but does enquire on the early cancellation/surrender of the particular contract;
7. A customer establishes a • large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party;
8. Early termination of a product, especially in a loss;
9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business;
10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need;
11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments;
12. A customer refuse's, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue;
13. A customer is reluctant to provide normal information when applying for an insurance policy, pre-need plan or HMO agreement, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify;

14. Delay in the provision-of information to enable verification to be completed;
15. Opening accounts with the customer's address outside the local service area;
16. Opening accounts with names similar to other established business entities;
17. Attempting to open or operating accounts under a false name;
18. Any transaction involving an undisclosed party;
19. A transfer of the benefit of a product to an apparently unrelated third party;
20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer or the right to payment could be transferred simply by signing an endorsement on the policy);
21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder;
22. The customer accepts very unfavourable conditions unrelated to his health or age;
23. An atypical incidence of pre-payment of insurance premiums;
24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;
25. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. (For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity);
26. Any unusual employment of an intermediary in the course of some usual transaction or formal activity e.g. payment of claims or high commission to an unusual intermediary;
27. A customer appears to have insurance policies, pre-need plans or HMO agreements with several institutions;
28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy;

29. The customer who is based in non-co-operative countries designated by the FATF from time to time or in countries where the production of drugs, or drug trafficking may be prevalent;
30. The customer who is introduced by an overseas agent, affiliate or other company that is based in non-co-operating countries designated by the FATF from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent;
31. Unexpected changes in employee characteristics, e.g. lavish lifestyle or avoiding taking holidays;
32. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance;
33. Consistently high activity levels of single premium business far in excess of any average company expectation;
34. The use of an address which is not the customer's permanent address, e.g. utilization of the salesman's office or home address for the dispatch of customer documentation; and
35. Any other indicator as may be detected by the ICREs from time to time.