Money Laundering and Terrorism Prevention Program (MLTPP)

1. About this Manual

1.1 Purpose

The Money Laundering ***and Terrorism*** Prevention Program (MLTPP) manual was created by virtue of Insurance Commission (IC) Circular No. 2017-07 implemented on January 31, 2017, which supersedes IC Circular No. 22-2012, and IC Circular No. 2018-48 implemented on September 14, 2018 to effectively implement the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as Amended otherwise known as the "Anti-Money Laundering Act of 2001" (AMLA). This is further amended Pursuant to the power of the Insurance Commission (IC) under Rule 7, Section 4.1 of the AMLA, As Amended", and Rule 27 of the 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.

The MLTPP manual provides a general guide to all employees of Fortune General Insurance Corporation ("FGen" or the "Company") to help them better understand and meet their obligations under the said laws and regulations as well as to support the overall compliance program of the Company.

1.2 Scope

The MLTPP manual applies to the Company, its head office, branches departments and authorized agents. This manual is also applicable to all products, services, and/or transactions of the Company whether or not they are discussed or included herein.

This revised version of the MLTPP manual replaces all other previous versions. It incorporates all AML advisories and internal policies and procedures issued by the regulatory bodies.

The policies and procedures in this manual are the minimum required under the rules and regulations on AMLA. Any department wishing to impose stricter controls should submit the proposed circular, bulletin, advisory or policy for review to the Quality Policy Committee. Only approved procedures can be issued as internal policy.

1.3 Review and Update Process

The MLTPP manual is maintained by the Compliance Officer (CO). The MLTPP shall be updated at least once every two (2) years to incorporate changes in anti-money laundering typologies, and latest guidelines and circulars of IC.

2. FGEN's Commitment against Money Laundering and the Financing of Terrorism

FGEN is committed to instilling a compliance culture throughout the organization.

An effectively implemented compliance program, approved by the Board of Directors (BOD), is essential to the efficient and successful operation of the Company. As a responsible corporate citizen, the Company is also committed to supporting the fight against money laundering by taking the necessary actions to comply with the applicable laws and regulations and to prevent the use of its products and services for illegal purposes.

3. Fundamentals to Combat Money Laundering

3.1 High Ethical Standards: The Company shall always conduct business on high ethical standards to protect its safety, soundness, and the integrity of the insurance industry.

3.2 Know Your Customer (KYC): The Company shall always obtain satisfactory evidence of the customer's identity and adopt effective procedures on verifying new customers. The Company shall also ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening or maintaining an account or transacting with the Company.

3.3 Compliance with Laws: Management shall ensure that business is conducted in conformity with the laws and regulations, and that service is not provided where there is good reason to suppose that transactions are associated with money laundering or terrorist financing.

3.4 Cooperation with Law Enforcement Agencies: The Company shall cooperate fully with the Anti-Money Laundering Council (AMLC) and other law enforcement agencies for the effective implementation and enforcement of the AMLA and its RIRR. This includes taking appropriate measures allowed by law if there are reasonable grounds to suspect that money is being laundered. Disclosure of information by the Company for the purposes of item c Section 9 of the AMLA shall be made to the AMLC.

3.5 Policies, Procedures and Training: The Company shall adopt and effectively implement a sound AML and terrorist financing risk management that identifies, assesses, monitors, and controls risks associated with money laundering and terrorist financing. The Company shall implement policies and procedures that are consistent with the principles set out under AMLA and other Circulars and laws of the land, and ensure that its staff, wherever located, are informed and aware of their respective responsibilities and will carry them out in accordance with superior and principled culture of compliance. To fully comply with the rules and existing laws, the Company shall further ensure that adequate training is provided to its officers and employees.

4. Implementation of the MLTPP

4.1 Roles and Responsibilities

All employees and agents play a part in the implementation of the MLTPP. Key roles and responsibilities under this program are briefly described below.

4.1.1 Board of Directors

The ultimate responsibility for ensuring compliance with AML and CFT Laws, their respective implementing rules and regulations resides with the BOD. Amongst others, the BOD:

- Adopts and approves the Company's MLTPP;
- Appoints a CO with authority and accountability; and
- Appoints another officer responsible and accountable for all record keeping requirements under AML and CFT Laws, their respective implementing rules and regulations. This officer shall also be responsible for making records or customer identification and transaction documents readily available without delay to the IC and AMLC during compliance checking or investigation.

4.1.2 Senior Management

Senior Management is responsible for:

- Overseeing the day-to-day management of the Company's business risk and effective implementation of the Company's AML/Combating of Financing Terrorism policies approved by the BOD and alignment of activities with the strategic objectives, risk profile and corporate values set by the BOD;
- Establishing a management structure that promotes accountability and transparency and upholds checks and balances;
- Promoting a compliance culture such that compliance standards are understood and observed by all Company personnel;
- Ensuring corrective action is taken where incidences of non-compliance or deficiencies in policies, procedures or controls have been identified.

4.1.3 Compliance Officer

The CO's main functions include but are not limited to:

- Managing the development and maintenance of an appropriate MLTPP and promoting their effective implementation. New/updated MLTPP duly approved by the BOD shall be submitted to IC not later than 15 days from the approval of the BOD with a sworn certification that such new/updated MLTPP has been prepared, duly noted and approved by the BOD;
- Reporting directly to the BOD or any board-level or approved committee on all matters related to AML and CFT compliance and their risk management;
- Ensuring compliance by all responsible officers and employees regarding AML and CFT Laws, their respective implementing rules and regulations
- Periodically updating the approved MLTPP to incorporate changes or issuances to regulations or industry best practices;
- Identifying, assessing, and reporting material breaches of the compliance program;
- Ensuring the integrity and accuracy of all documentary submissions to the AMLC and IC through independent validation; Maintaining the relationship with the IC and other regulatory agencies and interacting with them on compliance related matters;
- Conducting periodic compliance checking which covers, among others, evaluation of existing process, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, and record retention system through report compliance findings to the board;
- Ensuring infractions discovered either by internal audit or by special audit or regular audit compliance checking conducted by IC and/or AMLC are immediately corrected;
- Informing all responsible officers and employees of all resolutions, circulars, and other issuances by the IC and/or AMLC in relation to matters at preventing ML and TF;
- Alerting Senior Management and the Board of Directors if the institution seems to be failing to sensibly address anti-money laundering and terrorist financing issues; and
- Organizing the timing and content of AML/CFT training of officers and employees including regular refresher trainings.

4.1.4 AML Assistant

In coordination with the CO, the AML assistant develops, maintains, and promotes the effective implementation of the MLTPP by:

- Supporting business units in the development of adequate policies, procedures and controls to prevent money laundering and terrorist financing and overseeing their implementation;
- Ensuring timely and accurate reporting of the Company's covered transactions (CTs) and suspicious transactions (STs).

4.2 Hiring and Selection

On selecting new personnel, the Company shall employ the Hiring Standards which include the qualifications for employment as well as the selection process. Depending on the specific type and level of position that is being filled, additional screening processes including NBI clearance, verification of personal and employment references, and scanning against watch lists are conducted. This is to ensure that the Company attracts employees who are competent, qualified, and ethical as well as to prevent employee involvement in illegal activities.

4.4 Training

The Company shall regularly provide all of its ***directors, officers and employees*** with appropriate training on:

- Current laws, rules and regulations related to AML and Terrorism Financing Prevention
- Procedures and controls, including duties and responsibilities of officers and personnel in combating money laundering and terrorism financing

The training programs shall include relevant topics, such as:

a. Overview of the ML/TF, and the AMLA and TFPSA;
b. Roles of directors, officers and employees in ML/TF prevention;
c. Risk management;
d. Preventive measures;
e. Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC;
f. Cooperation with the AMLC and the IC; and
g. International standards and best practices.

Refresher program shall be provided by the Company at least every three (3) years.

It is the responsibility of Training and Agency Department to ensure that AMLA is included as part of the training programs conceptualized for Company employees and agents. The CO will assist in educating the ***directors, officers and employees*** on AMLA rules and regulations. ***In cases where there are new developments brought about by the new legislations, rules and regulations, and other IC and/or AMLC issuances, the Company, thru its CO and Training and Agency Department, shall immediately cascade these information to its***

responsible directors, officers and employees. Cascading of the information shall be documented.

Attendance by the Company's directors, officers and employees in all education and training programs whether internal/or external/or, organized shall be documented. Copies of AML/CTF continuing education and training programs, training certificates, attendance and materials, and shall be made available to the IC and the AMLC, upon request.

4.5 Internal Audit

Internal Audit is responsible for the periodic and independent evaluation of risk management; degree of adherence to internal control mechanisms related to the customer identification process, such as determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers; covered and suspicious transaction reporting and record keeping and retention; as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

The results of the internal audit shall be timely communicated during Management Committee meetings and to the BOD, if necessary, and shall be open for scrutiny by IC examiners in the course of the regular or special examination without prejudice to the conduct of its own evaluation whenever necessary. Results of the audit shall likewise be promptly communicated to the CO for its appropriate corrective action. The CO shall regularly submit reports during Management Committee meetings and to the BOD to inform them of Management's action to address deficiencies noted in the audit.

4.6 Sanctions and Penalties

To ensure that the Company maintains high AML standards to protect its safety and soundness, and to protect the integrity of the financial system, violations of these rules shall constitute a major violation subject to the following enforcement actions against the BOD, Senior Management, and all officers as promulgated by the AMLA, regulatory issuances and internal sanctions, not necessarily according to priority:

- Written reprimand
- Suspension, demotion or removal from the office they are currently holding
- Disqualification from holding any position in any covered institution
- Monetary penalties computed in accordance with existing regulations and in coordination with the AMLC

Penalties shall be imposed based on the over-all assessment of the Company's AML risk management.

As an insurance company, the Company is governed by the provisions of the AMLA, the Law on Secrecy of Company Deposits, as well as the other regulations issued and to be issued by the IC, the Securities & Exchange Commission (SEC), the Philippine Stock Exchange (PSE), the Department of Labor & Employment (DOLE), and by the Government of the Republic of the Philippines as a whole. It is the duty of all employees to abide by the provisions thereof lest sanctions be imposed upon the Company.

Among the requirements for compliance set by aforesaid regulations is the need to timely and accurately transmit reports. Any failure to do so is normally met with the imposition upon the Company of substantial fines and/or penalties.

The CO is authorized to recommend and/or impose sanctions for non-compliance with the rules, regulations, and policies on AMLA.

5. Definition of Terms

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

5.2 **Anti-Money Laundering Council ("AMLC")** refers to the financial intelligence unit of the Philippines which is the government agency tasked to implement the AMLA ***and The Terrorism Financing Prevention and Suppression Act (TFPSA).***

5.3 **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 funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with knowledge that are to be used, in full or in part: (1) carry out or facilitate the commission of any terrorist act; (2) by a terrorist organizations, association or group; or (3) by an individual terrorist.

5.4 **Person** refers to any natural or juridical person

5.5. **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.

5.6 **Covered Transaction**

5.6.1. A transaction in cash or other equivalent monetary instrument involving a total amount more than Five Hundred Thousand Pesos (PhP500,000) or its equivalent in any other currency; or

5.6.2. 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) or its equivalent in any other currency.

5.7 **Suspicious transaction** refers to a transaction, regardless of amount, where any of the following circumstances exists:

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

5.7.2 The customer is not properly identified;

5.7.3 The amount involved is not commensurate with the business or financial capacity of the customer;

5.7.4 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;

5.7.5 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 institution;

5.7.6 The transaction is in any way related to an unlawful activity or any money laundering activity or offense that is about to be, is being or has been committed; or

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

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

5.8 **Customer*/Clients*** refers to any person or entity that keeps an account or otherwise transacts business, with the Company. It includes the following:

5.8.1. Beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained or a transaction is conducted;

5.8.2. Transactors, agents and other authorized representatives of beneficial owners;

5.8.3. Beneficiaries;

5.8.4. A company or person whose assets are managed by an asset manager;

5.8.4. 5.***TrustorsIgrantorsIsettlorsof a trust***; and

5.8.5. Any insurance policy holder/ ***insured***, whether actual or perspective.

5.9 **Politically Exposed Persons (PEP)** refers to an individual who is or has been entrusted with prominent public positions 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. The term PEP shall include immediate family members, and close relationships and associates that are reputedly known to have:

5.9.1 Joint beneficial ownership of a legal entity or legal arrangement with main/principal PEP; or

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

5.10 **Immediate Family Member of PEPs** refers to ***individuals related to the PEP within the second degree or affinity.***

5.11 **Close *Relationship/Associates of PEPs*** refer to persons who are widely and publicly known ***socially or professionally*** 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.

5.12 **Beneficial Owner** refers to any natural person(s) who:

5.12.1 Ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted.

5.12.2 Has ultimate effective control over a legal person or ***legal*** arrangement***; or***

5.12.3 ***Owns the same percentage as prescribed in the Guidelines on the Identifying Beneficial Ownership and 2018 IRR, and its succeeding future amendments***

Control includes whether the control is exerted by means of trusts agreements, arrangements, understandings, practices and whether or not the individual can exercise control through making decisions about financial and operating policies.

5.13 ***Identification Document (ID)*** refers to any of the following ***evidence of identity***:

5.13.1 For Filipino citizens: Those issued by any of the following official authorities:

5.13.1.1 ***PhilID;***

5.13.1.2 ***Other identification issued by the*** Government of the Republic of the Philippines, including its political subdivisions, agencies and instrumentalities; ***and***

5.13.1.3 ***Other identification documents that can be verified using reliable, independent source documents data or information.***

5.13.2 For foreign nationals

5.13.2.1 ***PhilID, for resident aliens;***

5.13.2.2 ***Passport;***

5.13.2.3 ***Alien Certificate of Registration;***

5.13.2.4 ***Other identification documents that can be verified using reliable, independent source documents data or information.***

5.13.3 For Filipino students:

5.13.3.1 ***PhilID;***

5.13.3.2 ***School ID signed by the school principal or head of the educational institution; and***

5.13.3.3 ***Birth Certificate issued by the Philippine Statistics Authority; and***

5.13.4 For low-risk customers: Any document or information reduced in writing which the Company deems sufficient to establish the customer's identity (i.e. Company ID).

5.14 Monetary Instrument refers to:

5.14.1 Coins or currency of legal tender of the Philippines, or of any other country;

5.14.2 Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property;

5.14.3 Drafts, checks, and notes;

5.14.4 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;

5.14.5 A participation or interest in any non-stock, non-profit corporation;

5.14.6 Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts or deposit substitute instruments, trading orders, transaction tickets and confirmation of sale or investments and money market instruments;

5.14.7 Contracts or policies of insurance, life or non-life, and contracts of suretyship, pre-need plans and member certificates issued by mutual benefit association; and

5.14.8 Other similar instruments where title thereto passes to another by endorsement assignment or delivery.

5.15 **Property** refers to anything 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:

5.15.1 Personal property, including proceeds derived therefrom, or traceable to any unlawful activity, such as, but not limited to:

5.15.1.1 Cash

5.15.1.2 Jewelry, precious metals and stones, and other similar items;

5.15.1.3 Works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;

5.15.1.4 Perishable goods; and

5.15.1.5 Vehicles, vessels, aircraft or any other similar conveyance.

5.15.2 Personal property, used as instrumentalities in the commission of any unlawful activity, such as:

5.15.2.1 Computers, servers, and other electronic information and communication systems: and

5.15.2.2 Any conveyance, including any vehicle, vessel and aircraft.

5.15.2.3 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 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.

5.16 **Proceeds** refer to an amount derived or realized from any unlawful activity.

5.17 **Monetary Instrument or Property Related to an Unlawful Activity** refers to:

5.17.1 All proceeds of an unlawful activity;

5.17.2 All monetary, financial or economic means, devices, accounts, documents, papers, items, or things used in or having any relation to any unlawful activity;

5.17.3 All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds, and other similar items for financing, operations, and maintenance of any unlawful activity;

5.17.4 For purposes of freeze order and bank inquiry: related and materially linked accounts.

5.18 **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.

5.19 **Materially linked accounts** include but are not limited to the following:

5.19.1 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.

5.19.2 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;

5.19.3 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;

5.19.4 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;

5.19.5 ***All accounts of juridical persons or legal arrangements that are owned, controlled or ultimately effectively controlled by the natural person whose accounts, monetary instruments***

or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control; and

5.19.6 All other accounts, shares, units or monetary instruments that are similar, analogous or identical to any of the foregoing.

5.20 **Offender** refers to any person who commits a money laundering offense.

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

- Kidnapping for Ransom
- Violation against the Comprehensive Dangerous Drug Act of 2002
- Violation against Anti-Graft and Corrupt Practices Act
- Plunder
- Robbery and Extorsion
- Jueteng and Masiao
- Piracy on High Seas
- Qualified Theft
- Swindling
- Smuggling
- Violations Against Electronic Commerce Act of 2000
- Hijacking and other Violations against Republic Act No. 6235
- Terrorism and Conspiracy to Commit Terrorism
- Violations against Terrorism Financing Prevention and Suppression Act of 2012
- Bribery
- Fraud and Illegal Exactions and Transactions
- Malversation of Public Funds and Property
- Forgeries and Counterfeiting
- Violations against Anti-Trafficking in Persons Act of 2003, as amended
- Violations against Revised Forestry Code of the Philippines, as amended
- Violations against Philippine Fisheries Code of 1998
- Violations against Philippine Mining Act of 1995
- Violations against Wildlife Resources Conservation and Protection Act
- Violations against National Caves and Cave Resources Management Protection Act
- Violations against Anti-Carnapping Act of 2002, as amended
- Violations against Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition, or Disposition of Firearms, Ammunition or Explosives
- Violations against the Anti-Fencing Law
- Violations against Migrant Workers and Overseas Filipinos Act of 1995
- Violations against Intellectual Property Code of the Philippines, as amended
- Violations against Anti-Photo & Video Voyeurism Act of 2009
- Violations against Special Protection of Children against Abuse, Exploitation & Discrimination
- Violations against Anti Child Pornography Act of 2009
- Violations against Securities Regulation Code of 2000

- Felonies or offenses of a similar nature that are punishable under the penal laws of other countries.

5.22 **Money Laundering** – Money laundering is committed by:

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

5.22.1.1 Transacts said monetary instrument or property;

5.22.1.2 Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;

5.21.1.3 Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;

5.22.1.4 Attempts or conspires to commit money laundering offenses referred to in paragraphs (5.6.1.1), (5.6.1.2), or (5.6.1.3);

5.22.1.5 Aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (5.6.1.1), (5.6.1.2), or (5.6.1.3) above; and

5.22.1.6 Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraphs (5.6.1.1), (5.6.1.2), or (5.6.1.3) above.

5.22.2 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.

6. Customer Identification and Acceptance

6.1 General Guidelines

6.1.1 Customer Verification

The Company shall verify the identity of the customers through face-to-face contact or other modes of verification (i.e., video call), before or during the course of establishing a business relationship, or conducting transactions. Verification process may be completed after the establishment of the business relation provided that:

a. ***Completion*** occurs as soon as reasonably practicable;
b. ***Deferred customer verification*** is essential ***so as*** not to interrupt in the normal conduct of business; and
c. The ML/TF risks are effectively managed***, taking into consideration risk and materiality.***

For juridical or legal arrangements, the Company shall verify the customer's information through the following information:

a. Name, legal form and proof of existence
   a. The powers and other legal requirements or contracts that regulate and bind the juridical person or legal arrangements, as well as the names of the relevant persons having a senior managements position or perform significant responsibilities in the juridical person or legal arrangement
b. The address of the registered office and, if different, the principal place of business

6.1.2 ***The Company shall independently verify the collected identification information and document, through and of the following modes, unless otherwise provided in this Guidelines:***

a. Face-to-face contact
b. Use of Information and Communication Technology
c. By confirming the authenticity of the identified documents to the issuing office
d. Reliance on the third parties and service providers or
e. Such other methods of validation based on reliable and independent sources, documents, data or information.

6.1.3 Clients with multiple policies and accounts must be tagged and linked for monitoring purposes.

6.1.4 The Company shall ensure that all policies and accounts of clients are properly tagged and linked for monitoring of transactions. These include corporate accounts in which the clients are authorized signatories of those corporations, accounts in which the account holders are relatives or close associates of the clients such as PEP, and all other accounts in which the account holders are related to the clients.

6.1.5 The Company shall ensure that complete client information is obtained to establish and record the true identity of individual customers as well as to verify the legal existence of entities and identity of persons acting on their behalf.

The Company shall undertake satisfactory CDD measures:

a. Before establishing business relationship;
b. Carrying out occasional transactions above the applicable designated threshold, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
c. There is any suspicion of money laundering or terrorist financing; and
d. When the Company has doubts about the integrity or adequacy of previously obtained customer identification information.

Provided, that where the ML/TF risks are assesses as low and verification is not possible at the point of establishing the 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.

6.1.6 ***If the Company is unable to comply with the relevant CDD measures, they may:***

a. Refuse to open an account, commence business relations or perform the transaction; or shall terminate the business relationship; and

b. file STR in relation to the customer, if circumstances warrant.

6.1.7 The role of the New Business Department and Group Administration are to monitor the submission of the documentary requirements. These departments must ensure that all KYC documents are complete.

If validated during IC or Internal Audit Testing, the New Business Department and Group Administration will be accountable and liable for any noted deficiencies or exceptions which will consequently affect the performance evaluation of the responsible personnel without prejudice to the application of the

appropriate penalty under the MLTPP and existing Company's policies.

6.1.7 Completeness of the client information shall be the responsibility of both the front and back-office personnel involved in application process and their supervisors. Any liability for deficiencies noted in IC Examinations as well as those noted from requests of any court, regulatory body or agency, *i.e.*, AMLC, shall be the accountability of the personnel that processed and reviewed the application and/or account and the personnel that encoded and reviewed in the system. The supervisors of both the front office and back office shall likewise be accountable.

6.1.7.1 If validated during IC or Internal Audit testing, the responsible personnel will be accountable and liable for any noted deficiencies/exceptions which will consequently affect their performance evaluation without prejudice to the application of the appropriate penalty under the MLTPP and existing Company's policies.

6.1.9 Sanctions or penalties shall apply for inadequate and inconsistent performance of KYC duties and responsibilities as provided in this manual based on the gravity of offenses as provided in the HR Policy Manual. Below is the table of penalties per type of offense:

Type of Offense	Degree of Offenses/Disciplinary Actions			
	1st	2nd	3rd	4th
Minor	WR	15CDS	30CDS	D
Grave	D			

Legend:
Minor offense – if due to negligence and acts that results to an actual or potential loss of below P50,000.
Grave offense WR – if due to willful disobedience, gross and/or habitual negligence.
WR – Written Reprimand
CDS – Calendar Day Suspension
D – Dismissal

6.1.10 All applications received by the Company must undergo name screening to determine if the customer is high-risk (i.e., PEP, included in the OFAC list).

6.2 Risk Based Approach

The following are some of the factors taken into consideration in determining/updating the risk profile of a customer:

- Background and source of funds
- Public or high-profile position of the customer or its directors, trustees, stockholders, officers and/or authorized signatory
- Linked accounts
- Watch list of individuals and entities engaged in illegal activities or terrorist related activities as circularized by AMLC and other international entities or organizations such as United Nations Sanctions List
- Business activities
- Type of services/products/transactions to be entered with the Company

The Company shall document the client's risk profile (LOW or HIGH) and the level of due diligence applied (REDUCED or ENHANCED) in the application form. The risk profiling is confidential and should NEVER be disclosed to the public.

Except as otherwise provided in the MLTPP, those customers assessed to pose a lower risk for ML/TF shall be subject to reduced due diligence while customers assessed to pose a higher risk for ML/TF shall be subject to enhanced due diligence.

6.3 **Type of Customers**

Below are some examples of customers that are likely to pose low or high money laundering and terrorist financing risk to the Company.

Low Risk Customers

Individual
- Individual customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken.
- Individual customers with low value transactions
- Individual customers with a long-term (three years and above) and active business relationship with the Company
- Customers who are covered persons under AMLA
- Customers with consistent volume and frequency of transactions
- Customers with predictable and proportionate sources of income

Business or Corporations
- Customers with transactions consistent with business activity for businesses
- Customers with consistent volume and frequency of transactions
- Customers with source of funds from known and verifiable legitimate activities
- Corporate customers who are publicly listed on a stock exchange and subject to disclosure requirements to ensure adequate transparency of beneficial ownerships
- Corporate customers with a long-term (three years and above) and active business relationship with the Company

- Companies under the umbrella of ALC Group of Companies

High Risk Customers

- Customers with annual premium of more than PhP500,000 (regardless of mode of payment i.e., annual, semi-annual, quarterly or monthly)
- Customers with initial payment that exceeds PhP500,000
- Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests (*i.e.,* beneficial owners)
- Customers with high volume or high value transactions that deviate from the customer's profile, size and nature of business
- Customers from countries that are recognized as having inadequate internationally accepted AML standards or that do not sufficiently apply regulatory supervision or the Financial Action Task Force (FATF) recommendations
- Customers based in, or conducting business in or through a jurisdiction with known higher levels of corruption or organized crime, or drug production/distribution
- PEP as well as their immediate family members and entities related to them
- Beneficiaries who are PEP
- High net worth individuals whose origin of wealth cannot be easily verified
- Jewels, gems and precious stones dealers
- NGOs and NPOs
- Customers with suspicious claim/s (i.e., large claim with client unable to provide supporting documentation)

6.4 Standards of Customer Due Diligence

The following are the standard set of documents or forms the Company requires from all of its customers, whether individual, corporate or other juridical entities upon account opening to conduct proper due diligence:

- Application Form
- Identification Documents (ID)
- Business documents / Corporate Papers
- Client Endorsement Form

The Company will apply the following level of due diligence based on the risk profile of the customer:

- Reduced due diligence for Low-Risk Customers
- Enhanced due diligence for High-Risk Customers

6.4.1 **Reduced Due Diligence**

The Company shall obtain at the time of acceptance of applications ALL the mandatory client information, as indicated in **Appendix 1**. Beneficial owners as well as authorized signatories of corporation/juridical entities shall likewise be subjected to these requirements and properly tagged and linked

for monitoring purposes. The mandatory information shall be encoded completely and accurately in the Genweb System.

For individuals, including beneficial owner's and authorized signatories, the Company may establish relationship under the true and full name of the customer upon presentation of an acceptable original copy of at least one (1) valid photo bearing ID or official document issued by an official authority and maintain a clear copy for the Company's reference.

For entities, the Company 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-up on behalf of the entity, obtained at the time of acceptance of application.

Verification of the identity of the customer, beneficial owner or authorized signatory can be made ***before or during the course of establishing*** the business relationship.

The full list of acceptable identification documents is found in **Appendix 1** and **Appendix 2**. It is the prerogative and obligation of the Company to accept, reject or require another valid ID depending on the reliability, risk posed, and the ability to validate the information indicated on the identification document. Circumstances that may warrant the denial of business relationship with a client are found in **Appendix 4**.

There may be instances where financially or socially disadvantaged customers cannot provide the standard minimum information and documents required. Please refer to **Appendix 10** for the identification procedures that the Company has adopted to allow these customers access to financial services.

The Company shall retain copies of all reference documents, valid and legible, to verify the identity of its customer as well as authorized signatories of juridical entities. Validation guidelines are found in **Appendix 3**. The Company, through its agents, shall conduct casual interview to further verify the true and full identity of the client. Likewise, the agent shall use this interview to determine if a client is PEP as defined in **Appendix 5**. The interview and validation conducted by the agent shall be one of the means to determine whether an individual is PEP. The Company will also perform name screening to check if the client is PEP during the review of application.

6.4.2 **Enhanced Due Diligence**

For High-Risk customers, the Company must go beyond the usual KYC procedures and take additional measures to ascertain the identity of any individual or to confirm the

existence of an entity. This Enhanced Due Diligence (EDD) includes:

- Obtaining additional information other than the minimum information and/or documents required for Reduced Due Diligence

    a. Individual
        (1) list of companies where he is a director, officer/ stockholder
        (2) occupation history for the past three (3) years
        (3) volume of assets information available through public databases, internet etc.
        (4) supporting information on the intended nature of business relationship and reasons for the intended transaction (i.e., reason for getting a life insurance)
        (5) proof of source of funds/wealth (i.e., payslip, financial profile, ITR, etc.)
        (6) list of companies where he is a stockholder, director, officer or authorized signatory
        (7) other relevant information available through public database or internet
        (8) a list of banks where the individual has maintained or is maintaining an account
        (9) name, present address, date and place of birth, nationality, nature of work and source of funds of the beneficial owner and beneficiary, if applicable
        (10) clear copy of identification document of the beneficial owner
        (11) copy of the written document evidencing the relationship between account holder or transactor and beneficial owner

    b. Entities
        (1) List of banks where the entity has maintained or is maintaining an account
        (2) Verified name, present address, date and place of birth, nature of work, nationality and source of assets/funds of each of the primary officers (President, Treasurers and authorized signatory/ies), stockholders owning at least 5% of the voting stock, and directors/ trustees/ partners as well as their respective identification documents.
        (3) Volume of assets, other information available through public databases or

internet and supporting information on the intended nature of the business, source of duns or wealth of the customer (ITR, Audited Financial Statements, etc.)
(4) reasons for the intended transaction
(5) copy of the written document evidencing the identity and relationship between account holder or transactor, agent and beneficial owner

c. Legal Arrangements
(1) copy of the written document evidencing the identity and relationship between account holder or transactor, agent and beneficial owner

Note: The CEF must be used to document the additional information required from the customer.

- Conducting validation procedures on all information provided as indicated in **Appendix 3 and Appendix 11**.

- Obtaining Senior Management Approval for establishing the business relationship

- Conducting enhanced ongoing monitoring of business relationship

- Requiring the first payment to carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable

- Performing such other measures as the Company may deem reasonable or necessary

Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, the Company shall deny business relationship with the individual or entity.

Even existing customers may subsequently be subject to EDD when the Company obtains information in the course of its transaction monitoring and alerts management that:

- Raises doubt as to the accuracy of any information or document provided;
- Justifies re-classification of the customer from low risk to high risk;
- When a suspicious transaction is filed on the following grounds:

- Transacting without any underlying legal or trade obligation
- Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profile;
- Structuring of transactions in order to avoid being the subject of covered transacting reporting; or
- Knowing that a customer was or is engaged or engaging in any unlawful activity as defined in Section 5.12.

The Company shall examine also 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 maybe considered suspicious. Where the risks are high, the Company shall conduct EDD.

In this case, considering that the trigger for the EDD is transactional and not due to the risk profile of the customer, the EDD will then entail obtaining additional information and/or documents to explain or justify the transaction or incident in question. Each case may be different so the supporting documents may vary with each case. The general guidance on the conduct of EDD for transactions or incidents would be to explain or support the transaction or incident in question.

In addition thereto, if the profile or demographics of the customer is in question, the conduct of EDD would be to obtain information or documents to explain the change in circumstance of the customer.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the Company shall follow its procedures for closure of accounts and refrain from conducting further business relationship with the customer and file an STR, if the circumstances warrant (**See Appendix 7**).

In all instances, the Company shall document and maintain a record of what standard of due diligence (reduced or enhanced) was applied.

6.4.3 For personal accident insurance business, the Company, in addition to the customer due diligence measures required for the customer and the beneficial owner, conduct the following customer due diligence on the beneficiaries of personal accident insurance as soon as the beneficiary or beneficiaries are identified or designated:

6.4.3.1 for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;

6.4.3.2 for a beneficiary 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 will, obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity at the time of the pay-out but before funds are disbursed.

6.4.3.3 For both the above cases, verification of the identity of the beneficiary should occur at the time of the pay-out.

The Company shall include the beneficiary of a personal accident insurance policy as a relevant risk factor in determining whether EDD measures are applicable. If the beneficiary who is a legal person or legal arrangement presents a higher risk, the Company shall perform EDD to verify the identity of the beneficiary at the time of pay-out.

The Company shall also determine whether beneficiaries are PEP. This should occur, at the latest, at the time of pay-out. EDD shall be performed if such is the case.

When the Company is unable to comply with the foregoing, it should be consider making a suspicious transaction report.

6.5 Identification and Verification of Agents and Beneficial Ownership

A. Identification and Verification of Agents

1. General Requirement

The Company shall verify that any person purporting to act on behalf of a customer is so authorized and identify and verify the identity of that person.

2. Where an account is opened or an occasional transaction in excess of the threshold is conducted by any person on behalf of another, the Company shall establish and record the true and full identity and existence of both the account holder or person purporting to act on behalf of the customer, and the beneficial owner or the principal on whose behalf the transaction is being conducted.

3. The Company shall verify the validity of the authority of the agent. In case it entertains doubts as to whether the account holder or person purporting to act on behalf of the customer is being used as dummy in circumvention of existing laws it shall apply EDD and file an STR, if warranted.

B. Beneficial Ownership

1. The Company shall identify reasonable measures to verify the identity of the beneficial owner using the relevant information or data obtained from a reliable source, such that the Company is satisfied that it knows who the beneficial owner is.

2. Document Evidencing Relationship

The Company shall determine the true nature of the beneficial owner's capacities and duties vis-a-vis his agent 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 CDD to be applied to both.

3. Timing of Beneficial Ownership Verification.

The Company shall verify the identity of the beneficial owner before or during the course of establishing a business or professional relationship or conducting transactions for occasional customer in excess of the threshold. They may complete the BOV after the establishment of the business or professional relationship; Provided, that;

- ***a. this occurs as soon as reasonable/practicable***
- ***b. this is essential not to interrupt to the normal conduct of business, and***

C. Verification of Beneficial Ownership for Juridical Persons

For customers that are juridical persons, the Company shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

- ***a. The identity of the natural persons, if any, who ultimately have controlling ownership interest in a juridical person;***
- ***b. To the extent that there is a doubt under item (a) above, as to whether the persons with the controlling ownership interests are the beneficial owners or where no natural persons exert through ownership interest, the identity of the natural persons, if any, exercising control over the juridical person through other means; and***
- ***c. Where no natural person is identified under item (a) and (b) above, the identity of relevant natural persons who hold senior management positions.***

D. Verification of Beneficial Ownership for Legal Arrangements

For customer that are legal arrangements, the Company shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

1. For trust: the identity of the trustors/guarantors/settlers, the trustees, the beneficiaries or class of beneficiaries, the protector, if any, and any other natural person exercising the ultimate effective control over the trust agreement.

2. For beneficiaries of trust agreements that are designated by characteristics or by class; sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish

the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.
3. For other types of legal arrangements; identity of persons in equivalent or similar positions.

In determining, the reasonableness of the identity verification measures, the Company shall consider the money laundering and terrorist financing risks posed by the customer and business relationship.

E. ***Any natural person who directly or indirectly owns twenty percent (20%) or more of the legal person who is a customer of the Company (Ownership Prong) shall be considered the beneficial owner.***

F. ***Any individual who has significant responsibility to control, manage or direct the legal person (Effective Control Prong) will also be considered the beneficial owner.***

6.6 **Additional Guidelines for Higher Risk Clients, Services and Products**

6.6.1 **Politically Exposed Persons**

6.5.1.1 No case for money laundering may be filed to the prejudice of a candidate for an electoral office during an election period.

6.6.2 **Non- resident Individuals and Entities**

Same general guidelines on CDD will be applied for individuals and entities not residing in the Philippines.

6.6.3 Numbered Accounts

6.6.3.1 Peso and Foreign Currency Numbered checking accounts are **PROHIBITED**.

6.6.4 Outsourcing

6.6.4.1 AMLA allows an institution to outsource support and marketing activities subject to its provisions. However, it requires the institution to have appropriate mechanisms to ensure the effective management of attendant risks. The Company shall ensure that its agents undergo equivalent training program as to the Company's employees.

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

a. Can obtain immediately the necessary information concerning the CDD as required in this manual
b. Has an adequate CDD process
c. Has measures in place for record keeping requirements
d. Can provide the CDD information and provide copies of the relevant documentation immediately upon request

7. Prohibited Customer Accounts

Prohibited customers are those that are engaged in questionable and/or illegal activities that may expose the Company to legal, regulatory or reputational risk. Some examples include:

- Individuals or corporations who are subject to sanctions or prohibitions established by international law or local authorities (i.e., United Nations Sanctions);
- Individuals or corporations who refuse to provide all required information;
- Individuals or corporations who have provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation;
- Individuals or corporations known to be involved in criminal activity;
- Individuals or corporations whose accounts were previously closed and the business relationship terminated due to suspicious activity, suspected fraud or criminality or other unsatisfactory performance;
- Shell banks and shell companies;
- Pornography and sexual services establishments or providers;
- Manufacturers / Dealers in arms and munitions.

Given that the Company shall maintain accounts only with the true and full name of the account owner, opening the following accounts is absolutely prohibited:

- Anonymous Accounts
- Accounts under fictitious names
- Numbered Checking Accounts

8. Ongoing Monitoring of Client Relationship

Screening of existing accounts against adverse media reports shall be done within the same week as when the news article is published in a local newspaper of general circulation or broadcasted on a reputable local news network. The news report must involve the filing of a case involving an unlawful activity.

8.4 Updating Customer Information

During the course of its business relationship with the client, the Company shall ensure that information and documents of its customers are updated. This shall include all

customer identification information and documents as well as updating of the client's risk profile. Updating shall be done as follows:

Low Risk	Every 3 years
High Risk	Every year

The Company shall endeavor to update the client information within four (4) months from when the account is due for updating in accordance with the customer's risk profile.

For existing accounts that were opened prior to the adoption of the risk-based approach, risk profiling shall be conducted including periodic assessment and updating of client records.

EDD shall be applied to all existing high-risk customers. The applicable validation procedures shall be performed during the required period of updating the customer's record to determine any changes in the customer's profile which may have occurred after establishing the relationship with the Company. EDD shall be performed also for those customers whose transactions were deemed suspicious as determined by the Company even if the customer's record is not yet due for updating.

9. Covered Transaction and Suspicious Transaction Reporting

9.1 Covered or suspicious transactions are to be reported to the AMLC within five (5) working days from date of transaction. In the case of STRs, it is reckoned from date of the Company's determination of the suspicious nature of the transaction. Should a transaction be determined to be both a CT and ST, the Company shall be required ***to report it as covered first subject to updating if it is finally confirmed to be reportable as suspicious transaction.***

9.2 Deferred reporting of CT which are non-cash, no or low risk CT are allowed; thus, the following need not be reported:

- Transactions between domestic insurance companies or professional reinsurers or intermediaries licensed by the IC
- Automatic premium advance
- Collection of premium payments from telemarketing, or direct marketing or through SMS and or by way of salary deductions, where bulk settlement exceeds PhP500,000 but the individual transactions are below the reporting threshold amount
- Hospitalization or Medical insurance
- Payment of loan and or its corresponding interest regardless of the manner of payment, provided that the grant of loan was previously reported as CT
- Bulk settlement of claims on death and disability benefits of a policy where individual claims does not exceed PhP500,000
- Internal operating expenses and capital expenditures of the Company; and
    - These are necessary expenses of the Company for the normal day-to-day running of a business. These are transactions of covered institutions and, therefore, not reportable. Such as, but not limited to payment of salaries, taxes, debt service, SSS premiums, Pag-ibig contributions and employees' benefits.
- Adjusting entries or reclassification of accounts

9.3 Safe Harbor and Confidentiality Provisions

9.3.1 No administrative, criminal or civil proceedings shall lie against any person for having made a covered transaction report or suspicious transaction report in the regular performance of his duties in good faith, whether such reporting results in any criminal prosecution under the AMLA, its RIRR, or any other laws.

9.3.2 Reporting personnel are **prohibited** from communicating or disclosing ("tipping off"), directly or indirectly, in any manner or by any means, to any person or entity, the media, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. It shall not be published or aired in any manner or form by the mass media, electronic mail, or other similar devices. In case of violation, the concerned officer, employee of the covered institution, and media shall be held **criminally liable**.

9.4 STR Escalations

9.4.1 The departments are given a maximum of two (2) working days to report an STR upon knowledge of the incident and/or transaction being reported as suspicious.

9.4.2 In case of AML issues (e.g., matters which may be reportable as an STR) that may involve the higher rank employees, any Company personnel, regardless of position or rank, who are witnesses to anomalies in the workplace are obliged to speak up and report the same personally or in writing to any of the following officers:

- The Internal Audit Head
- The Human Resources and Admin Head
- The CO
- The COO
- The President

10. Freeze Order Guidelines

10.1 Upon verified *ex parte* petition by the AMLC and after determination that probable cause exists that any monetary instrument or property is in any way related to any unlawful activity, the Court of Appeals may issue a freeze order on said monetary instrument or property which shall be effective immediately**.** Upon receipt of the notice of the freeze order, the Company shall immediately freeze the monetary instrument or property and related accounts subject thereof.

10.2 The effectivity of the freeze shall likewise be applied during Civil Forfeiture cases where Asset Preservation Orders are issued.

10.3 Lifting or cancellation of the freeze order shall require prior confirmation [one day before or on the expiry of the said six (6) month period] with the AMLC through the CO. The CO shall be responsible for verifying the status of the account with the AMLC.

10.4 All existing freeze orders which the Court of Appeals has extended prior to the effectivity of R.A. No. 9194 shall remain effective, unless otherwise dissolved by the same court. There should be no lifting of freeze order without the confirmation of the AMLC and the CO. The CO shall send an e-mail notification to the concerned unit upon confirmation or advice from the AMLC of the lifting of the freeze order.

10.5 Section 16 of the AMLA and Rule 10.6 of the RIRR states that, "no case for money laundering shall be filed against and no assets shall be frozen, attached or forfeited to the prejudice of a candidate for an electoral office during an election period.

11. Record Keeping and Retention

11.1 The Company shall maintain all identification records as long as the account exists.

11.2 All transaction records, including all unusual or suspicious patterns of account activity whether or not an STR was filed with the AMLC, shall be maintained and stored for five (5) years from the date of the transaction.

11.3 Said records and files shall contain the full and true identity of the owners or holders of the accounts involved in the transactions such as ID for individuals and the KYC documents for entities and all other pertinent customer identification documents as well as transaction records. The purpose for the recordkeeping is so that any account, relationship or transaction may be reconstructed as to enable the AMLC, and/or the courts to establish an audit trail for money laundering. The same shall be converted in digital form in compliance with AMLC requirements.

11.4 In this case, the following records retention period should be observed:

- Transaction documents – 5 years from date of transaction
- Existing accounts – permanently
- Closed accounts – at least 5 years from the date of closure
- Accounts with court cases – permanently until case is closed/resolved

11.5 All records shall be retained ***in their original forms or such other forms sufficient to permit reconstruction of individual transaction so*** as admissible in court pursuant to existing laws and the applicable rules promulgated by the Supreme Court.

11.6 Company officers shall undertake necessary and adequate security measures to ensure the confidentiality of records. The Company shall designate at least two (2) custodians from the head office units who will be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA. They shall have the obligation to make these documents and records readily available without delay during IC regular or special examination as well as other regulators such as AMLC and SEC.

11.7 In addition to existing account closing procedures and policies of the Company, the officer responsible for the safekeeping of customer identification records shall ensure that the following documents are available and complete prior to allowing account closure: the photocopy of the ID for individual customers and minimum required corporation documents for entities, customer relationship form, signature card of authorized signatory/ies and other pertinent customer identification documents.

DOCUMENT CONTROL	
DOCUMENT TITLE	MONEY LAUNDERING PREVENTION PROGRAM (MLTPP)
COMPANY	FORTUNE GENERAL INSURANCE CORPORATION
OWNER	COMPLIANCE OFFICE
AUTHOR	CENON ANTONIO GERARD M. LUKBAN – AMLA COMPLIANCE OFFICER
ISSUE DATE	October 25, 2022
DATE UPDATED	December 3, 2024
NEXT REVIEW DATE	Every 2 years