MAESTRO HOLDINGS, INC.
Group of Companies

2024 Money Laundering and Terrorist Financing Prevention Program

(MTPP Manual)

January 2024

TABLE OF CONTENTS

1. Introduction

The Anti-Money Laundering Council comprised of the Bangko Sentral ng Pilipinas, Security and Exchange Commission and Insurance Commission provide rules and regulations to covered institutions relative to the implementation of R.A. 9160 also known as The Anti-Money Laundering Act (AMLA) of 2001, as amended by R.A. 9194, R.A. 10167, R.A. 10365 and RA 10927, and R.A 10168 also known as The Terrorism Financing Prevention and Suppression Act (TFPSA) of 2012. The manual also considers the Updated AMLA and TFPSA Rules and Regulations under BSP Circular 1022 dated November 26, 2018 and the Security and Exchange Commission Certification Examination AML Module issued on March 28, 2019, AML risk and AML risk management, internal policies and procedures and industry sound practices.

This manual is designed to ensure that all operating units of the organization and its service providers shall comply with the AML and Countering of Terrorist Financing (CTF) requirements and obligations set out in Philippine legislation, rules,regulations, government regulatory bodies and agencies' guidance, global best practices; and that adequate systems and controls are in place to mitigate the AML risks and that the organization is notused to facilitate financial crime.

The Maestro Group of Companies (hereinafter, "**MAESTRO**") is a conglomerate of corporate entities involved in various enterprises, mostly focused on the insurance and financial investment industries. The entities in the Group that are under the regulatory jurisdiction and oversight of the Insurance Commission, and thus subject to AML and CTF guidelines and rules, are:

PHILPLANS FIRST, INC. (Philplans) - a pre-need company engaged in the sale of pre-need pension, education and memorial plans.

PHILHEALTHCARE, INC. (PhilCare) – a health maintenance organization (HMO) engaged in the sale of medical insurance coverage and various services related to physical and mental health.

PHILIPPINE LIFE FINANCIAL ASSURANCE, INC. (PhilLife) – a life insurance company that also engages in the business of providing loans to employees of the Department of Education and other special interest groups.

2. Definition of terms

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 Philippines' central AML/CTF authority and financial intelligence unit, which is the government instrumentality mandated to implement the AMLA and TFPSA. It also refers to the official name of the Council, which is the governing body of the said government agency.

For purposes of this Manual, the government agency shall be referred hereafter as the "AMLC", while the governing body shall be referred hereafter as the "Council".

c. "**Asset**" refers to a monetary instrument, property, or both.

d. "**Average Due Diligence**" (ADD) refers to the normal level of customer due diligence that is appropriate in cases where there is medium risk of money laundering or terrorism financing.

e. "**Beneficiary**" refers to:

(1) For pre-need plans: the person who will be paid the proceeds of the insurance policy component, where relevant, as well as the person who will receive the proceeds of the investment component of the pre-need plan in the absence of the planholder.
(2) For life insurance policies: any person who will be paid the policy proceeds.

f. "**Beneficiary Financial Institution**" refers to the financial institution, which receives the wire transfer from the originating/ordering financial institution, directly or through an intermediary financial institution, and makes the funds available to the beneficiary.

g. "**Biometric Information**" refers to front facing photograph, fingerprint, iris scan, and/or such other unique identifiable features of an individual.

h. "**Covered Transaction**" (CT) refers to:

A transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (PHP500,000.00).

i. "**Covered Transaction Report**" (CTR) refers to a report on a covered transaction, as herein defined, filed by a covered person before the AMLC.

j. "**Customer/Member Client**" refers to any person or entity who keeps an account, or otherwise transacts business with a covered person. It includes the following:

(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;
(2) Transactors, agents and other authorized representatives of beneficial owners;
(3) Beneficiaries of insurance policies, and remittance transactions;
(4) Insurance policy holders, whether actual or prospective.
(5) Pre-need planholders, whether actual or prospective.
(6) HMO product clients and members, whether actual or prospective.

k. "**Customer Due Diligence**" (CDD) refers to the procedure of identifying and verifying the true identity, of customers, and their agents and beneficial owners, including understanding and monitoring of their transactions and activities.

l. "**Customer Identification Process**" (CIP) refers to the process of determining the identity of the customer vis-à-vis the valid and acceptable identification document submitted to, and/or presented before, the covered person.

m. "**Customer Verification Process**" (CVP) refers to the process of validating the truthfulness of the information, and confirming the authenticity of the identification documents, presented, submitted and provided by the customer; or other ways of verifying the identity and assessing the risk profile of customers, and their agents and beneficial owners, through the use of reliable and independent sources, documents, data or information.

n. "**Designated Non-Financial Businesses and Professions**" (DNFBP) refer to businesses and professions, which are not under the supervision or regulation of the BSP, SEC and IC, and designated as covered persons under the AMLA.

o. "**Determination of the Purpose of Relationship**" (DPR) refers to the process of identifying the purpose and intended nature of the account, transaction, or business or professional relationship.

p. "**Demographic Data**" refers to a person's full name, sex, date and place of birth, address, citizenship or nationality, and such other personal information from which the identity of a person can be ascertained.

q. "**Enhanced Due Diligence**" (EDD) refers to the enhanced level of scrutiny intended to provide a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate risks presented.

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

s. "**Information and Communication Technology**" (ICT) refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present and disseminate information.

t. "**Institutional Risk Assessment**" refers to a comprehensive exercise to identify, assess and understand a covered person's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

u. "**Insurance Commission**" (IC) refers to the Philippine regulator of the insurance, HMO and pre-need industries.

v. "**Law Enforcement Agency**" (LEA) refers to the Philippine National Police, National Bureau of Investigation, and other government agencies that are responsible for the prevention, investigation, apprehension, and/or detention of individuals suspected of, or convicted for, violations of criminal laws.

w. "**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.

x. "**Money Laundering**" is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

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

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

aa. "**Money Laundering/Terrorism Financing Prevention Program**" (MTPP) refers to a covered person's comprehensive, risk-based, and written internal policies, control and procedures to implement the relevant laws, rules and regulations, and best practices to prevent and combat ML/TF and associated unlawful activities in the operational level.

bb. "**Money or Value Transfer Service**" (MVTS) refers to financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value, and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the service provider belongs.

cc. "**Monetary instrument or property related to an unlawful activity**" refers to all proceeds, instrumentalities and monetary instruments of an unlawful activity;

dd. "**Mutual Legal Assistance**" (MLA) refers to the formal method of cooperation between two jurisdictions for purposes of seeking assistance in the production of documents, asset freezing and forfeiture, extradition, enforcement of foreign judgment, and other kinds of legal assistance in criminal matters.

ee. "**National Risk Assessment**" (NRA) refers to a comprehensive exercise to identify, assess and understand a country's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

ff. "**Non-Profit Organization**" (NPO) refers to a juridical person, legal arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying of other types of "good works".

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

hh. "**Official/Identification 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); or
   c) Covered persons registered with and supervised or regulated by the Bangko Sentral ng Pilipinas, SEC or IC;
   d) Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys)
(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;
(4) For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity; and
(5) Other identification document that can be verified using reliable, independent source documents, data or information.

ii. "**On-going Monitoring Process**" (OMP) refers to the process of conducting continuing due diligence, including continually assessing the risks, understanding the transactions and activities, and updating, based on risk and materiality, the identification information and/or identification documents, of customers, their agents and beneficial owners.

jj. "**Person/Entity**" refers to any natural or juridical person.

kk. "**Philippine Identification Card**" (PhilID) refers to the non-transferrable identification cardissued by the Philippine Statistics Authority (PSA) to all citizens and resident aliens registered under the Philippine Identification System. It shall serve as the official government-issued identification document of cardholders in dealing with all government agencies, local government units, government and controlled corporations, government financial institutions, and all private sector entities.

ll. "**Philippine Identification System**" (PhilSys) refers to the Philippine Government's central identification platform, established under Republic Act No. 11055, otherwise known as the "Philippine Identification System Act" (PhilSys Act), for all citizens and resident aliens of the Philippines.

mm. "**PhilSys Number**" (PSN) refers to the randomly generated, unique and permanent identification number assigned to every citizen or resident alien, upon birth or registration, by the PSA.

nn. "**Politically Exposed Person**" (PEP) refers to an individual who is or has been entrustedwith 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.

Immediate family members of PEPs refer to individuals related to the PEP within the second degree of consanguinity or affinity;

Close relationship/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.

oo. **"Product"** refers to any policy, plan or other service sold by the company.

pp. "**Proceeds**" refers to an amount derived or realized from any unlawful activity.

qq. "**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 personal properties.

rr. "**Reduced Due Diligence**" (RDD) refers to the lowest level of customer due diligence that is appropriate in cases where there is low risk of money laundering or terrorism financing.

ss. "**Risk**" refers to risk of loss arising from ML/TF activities.

tt. "**Risk-Based Approach**" refers to the process by which countries, competent authorities, and covered persons identify, assess, and understand the ML/TF risks to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. This includes prioritization and efficient allocation of resources by the relevant key players and stakeholders in applying AML/CTF measures in their operations in a way that ensures that they are commensurate with the risks involved.

uu. "**Sectoral Risk Assessment**" refers to a comprehensive exercise to identify, assess and understand an industry's, or business or professional sector's, threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

vv. "**Securities and Exchange Commission**" (SEC) refers to the Philippines' company register and regulator of the securities industry.

ww. "**Source of Fund**" refers to the origin of the funds or other monetary instrument that is the subject of the transaction or business or professional relationship between a covered person and its customer, such as cash on hand, safety deposit box with a covered person, and a particular bank or investment account.

xx. "**Source of Wealth**" refers to the resource from which the customer's wealth, including all monetary instruments and properties, came, comes, or will come from, such as employment, business, investment, foreign remittance, inheritance, donation, and winnings.

yy. "**Supervising Authority**" (SA) refers to the BSP, the SEC, the IC, MNRC or other government agencies designated by law to supervise or regulate a particular financial institution, MFIs, or DNFBP.

zz. "**Suspicion**" refers to a person's state of mind—based on his skills, experience, and/or understanding of the customer profile—which considers that there is a possibility that any of the suspicious circumstances exists.

zz. "**Suspicious transaction**" (ST) refers to a transaction with a covered person, regardless of the amount involved, where any of the following circumstances exists:

(1) There is no underlying legal or trade obligation, purpose or economic justification;

(2) The client is not properly identified;
(3) The amount involved is not commensurate with the business or financial capacity of the client;
(4) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA, as amended;
(5) Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
(6) The transaction is in any way related to an unlawful activity or any money laundering activity or offense, that is about to be 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 a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as suspicious transaction.

aaa. **"Suspicious transaction"** (ST) refers to a transaction with a covered person, regardlessof the amount involved that is, in any way, related to terrorism financing or terrorist acts.

Per Implementing Rules and Regulations (IRR) of Republic Act No. 10168 rule 3.a.15, in determining whether a transaction is suspicious, covered institutions should consider the following circumstances:

(1) Wire transfers between accounts, without visible legal, economic or business purpose, especially if the wire transfers are effected through countries which are identified or connected with terrorist activities;
(2) Sources and/or beneficiaries of wire transfers are citizens of countries which are identified or connected with terrorist activities;
(3) Client was reported and/or mentioned in the news to be involved in terrorist activities;
(4) Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;
(5) Transactions of individuals, companies or Non-government Organizations (NGOs)/ non-Profit Organization (NPOs) that are affiliated or related to people suspected of having connected with a terrorist individual, organization or group of persons;
(6) Transactions of individuals, companies or NGOS/NPOs that are suspected of being used to pay or receive funds from a terrorist individual, organization or group of persons;
(7) It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or group of persons.

bbb. "**Suspicious Transaction Report**" (STR) refers to a report on a suspicious transaction, as herein defined, filed by a covered person before the AMLC.

ccc. "**Terrorism Financing Prevention and Suppression Act**" (TFPSA) refers to Republic Act No. 10168.

ddd. "**Transaction**" refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the covered person and its customer. It also includes any movement of funds, by any means, in the ordinary course of business with a covered person.

eee. "**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, 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 R.A. No. 9208, otherwise known as the Anti-Trafficking in Persons Act of 2003, as amended;
(20) Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
(21) Violations of Sections 86 to 106 of Chapter IV, of Republic Act No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
(22) Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the Philippine Mining Act of 1995;
(23) Violations of Section 27(c), (e), (f), (g) and (i), of Republic Act No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;
(24) Violation of Section 7(b) of Republic Act No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act.
(25) Violation of R.A. No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;
(26) Violations of Sections 1, 3 and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree Codifying the Laws on Illegal/Unlawful Possession,

Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives;
(27) Violation of Presidential Decree No. 1612, otherwise known as the Anti-Fencing Law;
(28) Violation of Section 6 of R.A. No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995;
(29) Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;
(30) Violation of Section 4 of Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;
(31) Violation of Section 4 of Republic Act No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;
(32) Violations of Sections 5, 7, 8, 9, 10 (c), (d) and (e), 11, 12 and 14 of Republic Act. No. 7610, otherwise known as the Special Protection of Children against Abuse, Exploitation and Discrimination;
(33) Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the Securities Regulation Code of 2000; and
(34) Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

In determining whether or not a felony or offense punishable under the penal laws of other countries is "of a similar nature" so as to constitute an unlawful activity under the AMLA, it is sufficient that both the Philippines and the other jurisdiction criminalize the conduct or activity underlying the offense, regardless of whether both countries place the offense within the same category or denominate the offense under the same nomenclature.

zz. Money Laundering and its Stages

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions; in this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent stages, namely: placement, layering and integration that can occur simultaneously:

Placement. The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution.

Layering. The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts or wiring or transferring funds to and through numerous accounts in oneor more financial institutions.

Integration. The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a believable explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

aaa. Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations.

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking have played a role in moving terrorist funds. Transactions through informal banking are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

bbb. Cybercrime

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computer for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyber-terrorism are also of significant concern.

The cybercrime law of the Philippines (Cybercrime Prevention Act of 2012- RA 10175) defines and punishes certain acts, generally classified as:

- Offenses against the confidentiality, integrity and availability of computer data and systems
- Computer-related offenses
- Content-related offenses

ccc. Importance of this Manual to the Employee and to MAESTRO, Its Business Entities – and Service Providers

In adhering to this Manual, as with every aspect of its business vehicles, the organization expects that its employees nationwide and the employees of its accredited service providers will conduct themselves in accordance with the highest ethical and professional standards. The organization also expects its employees and its third-party service providers to conduct business in accordance with applicable AML laws. Employees shall not knowingly provide advice or other assistance to individuals who attempt to violate or avoid anti-money laundering laws.

Anti-money laundering laws apply not only to criminals who try to launder their ill-gotten gains but also to product employees who participate in those transactions, if the employees know that the property is criminally derived. "Knowledge" includes the concept of "willful blindness" and "conscious avoidance of knowledge." Thus, employees of the organization whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, may be considered under the law to have the requisite "knowledge". MAESTRO employees who suspect money laundering activities should refer the matter to appropriate personnel, such as their immediate supervisor, the designated Compliance AML and CTF Officer, the Group Head and Senior Management.

ddd. Penalties for Violation of the AMLA and TF Suppression Act

Failure to adhere to this Manual may subject MAESTRO employees to disciplinary action up to the extent oftermination of employment while the contracts or business relationships with accredited third-party service providers may be suspended and if necessary, termination of the contract subject to prescribed notification requirements. Penalties for money laundering and terrorist financing can be severe. Underthe Philippine AML Law RA 9160 as amended, a person convicted of money laundering can face up to 14 years in prison and a fine of up to P3, 000,000 or twice the amount of the property involved. Anyproperty involved in a transaction or traceable to the proceeds of the criminal activity, including propertysuch as client equity, member collateral, personal property, and, under certain conditions, entire member client accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. In addition, the MAESTRO companies risk losing their charters and/or licenses to operate, and their employees risk being subjected to AML criminal investigation.

eee. Rules on the Imposition of Administrative Sanctions under republic Act No. 9160, as amended

The AMLC shall, at its discretion, impose administrative sanctions upon any covered person for the violation of the AMLA and its RIRR, or for failure or refusal to comply with the orders, resolutions and other issuances of the AMLC.

Fines shall be in amounts as may be determined by the AMLC to be appropriate, which shall not be more than Five Hundred Thousand Pesos (Php500,000) per violation. In no case shall the aggregate fine exceed five percent (5%) of the asset size of the respondent.

Fines – The following are the fines (in Philippine Peso) per violation based on the entity size and gravity of violations:

Violations	Micro	Small	Medium	Large A	Large B
Grave	50,000	125,000	250,000	375,000	500,000
Major	30,000	75,000	150,000	225,000	300,000
Serious	20,000	50,000	100,000	150,000	200,000
Less Serious	10,000	25,000	50,000	75,000	100,000
Light	5,000	12,500	25,000	37,500	50,000

fff. Reporting Protection under AMLA

When reporting covered or suspicious transactions to the Anti-Money Laundering Council (AMLC), the organization and its officers and employees shall not be deemed to have violated R.A. No. 1405, as amended, (Bank Secrecy Law) R.A. No. 6426, as amended, (FCDU Law), R.A. No. 8791 (General Banking Law), and other related laws (BSP 706 subsection X807.5 – Exemption from Bank Secrecy Laws).

No administrative, criminal or civil proceedings shall be imposed against any person for having made a covered or a suspicious transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under this Act or any other law (RIRR Rule 9c.3. – Safe Harbor Provisions).

ggg. Notice to Clients for AMLA Requirements

In compliance with SEC Circular Memo No. 2 dated May 20, 2010, the following NOTICE TO CLIENTS FOR AMLA REQUIREMENT ON THE SUBMISSION OF SUPPORTING DOCUMENTS shall be posted in the conspicuous area of the branch.

The notice shall be as follows:

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

In this regard, the organization shall obtain information such as name, address, date of birth, business, TIN, SSS or GSIS Nos. and presentation of acceptable valid IDs or other competent evidence of identity bearing your photograph and signature when you transact with us.

Kindly be assured that we shall continue to observe full compliance with the provisions of the Data Privacy Act of 2012 and shall not disclose or process any information collected except in accordance with the law and for official purposes."

hhh. Customer Acceptance Policy

It is the policy of MAESTRO that no product account shall be opened or the transaction shall be cancelled if any of the following circumstances exists:

11.1. New member client account to be opened or transaction to be conducted is under anonymous or fictitious names.

11.2. Where the branch, unit or office is unable to verify the identity of the member client

11.3. Where the branch, unit or office is unable to obtain the required information and/or documents due to non-cooperation of the member client or non-reliability of the data or information furnished to MAESTRO or to the accredited Service Provider. In all cases, decision to close an account should be taken at the next higher level of authority.

11.4. Positive match vs. OFAC/SDN/Internal Negative File or with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available from BSP, AMLC Circulars, host country regulatory or enforcement agencies and other reputable/reliable sources.

NON –DISCRIMINATION AGAINST CERTAIN TYPES OF CUSTOMERS

MAESTRO shall not decline any transaction from any customer, such us PEPs, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the

only basis to deny the person access to MAESTRO products and services. However, all member client shallbe subject to:

1. Know Your Customer (KYC)
2. Submission of valid IDs
3. Customer Risk Rating
4. OFAC and Other Watch list Validation
5. Enhanced Due Diligence, if warranted.

And, the member client shall cooperate with MAESTRO in the submission of supporting document to determine the underlying trade or economic purpose of the transaction/s, if needed. And shall abide with the terms and conditions set by MAESTRO to its products and services.

iii. Sharing of Customer Information among MAESTRO Group

MAESTRO allows the sharing of information among its branches and offices located nationwide when conducting Customer Due Diligence provided the needed information shall be requested by the designated Compliance Officer.

jjj. Risk Assessment

13.1. National Risk Assessment and Management

National Risk Assessment (NRA) is a comprehensive exercise to identify, assess and understand a country's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions. The Anti-Money Laundering Council, together with relevant government, public and private offices and sectors, shall conduct a National Risk Assessment (2018 IRR Chapter IV Rule 13 Section 1) in compliance with the Financial Action Task Force (FATF) Recommendation 1. It should apply a risk-based approach to ensure the mechanisms and measures to prevent ML/TF risks are commensurate to the risks and context identified.

The NRA shall be updated once every three years or as often as the AMLC may deem necessary.

13.2. MAESTRO Risk Assessment and Management

It is the responsibility of organizations registered with the Securities and Exchange Commission and the Insurance Commission to conduct AML risk assessment of customers, products, services, delivery channels and geographical locations to understand its risk exposure to money laundering and terrorism financing risks.

MAESTRO reviews the results of the National Risk Assessment on the Money Laundering and Terrorist Financing in the risk assessment process and implements appropriate risk-based measures to manage and mitigate identified risks.

At minimum, clients are enrolled with proper KYC documentation, customer verification and regular monitoring of the low ticket size transactions. On a regular basis, MAESTRO shall monitor the various risks that could directly impact the quality of implementation of the Money Laundering and Terrorism Financing Prevention Program of the MAESTRO companies.

The MAESTRO Risk Assessment process shall be conducted at least every two (2) years, or as often as the board or senior management, the AMLC or government bodies and government agenciesmay direct and aligned with new AML/CFT developments that may impact the operations.

13.2.1. MAESTRO Risk Assessment Methodology

MAESTRO shall conduct AML risk assessment at least every two years to assist in identifying the organization's AML risk profile. Understanding the risk profile enables the organization to apply appropriate risk management processes to the AML and CTF compliance program to mitigate risks. The risk assessment process enables the Board and Senior Management to have a clear understanding of identified gaps in the existing mitigating controls and the corrective actions implemented. The risk assessment provides a comprehensive analysis of the AML and CTF risks in a concise and organized manner.

The development of the AML risk assessment involves two steps. First is to identify the specific risk categories (i.e. product as to services, customers, entities, transactions, and geographic locations) unique to the organization; and second, is to conduct a more detailed analysis of the data gathered as basis for the risk assessment within certain categories.

The organization has adapted a methodology generally used by financial institutions towards a risk-based approach in AML risk assessment. The risk-based approach involved identifying and categorizing money laundering risks and establishing reasonable controls based on risk identified. Using the risk-based approach, the organization is able to determine potential money laundering and terrorist financing risk and to exercise reasonable business judgment in the formulation of policies and procedures that will effectively manage servicing of its member clients.

The AML risk-assessment process covers the following steps:

1. Identify specific risk categories. This includes the organization's services, customers/member clients, entities, channels, transactions and geographic locations.
2. Conduct a more detailed analysis of the data gathered for at least 12 months as basis for the assessment of risk within the categories and determines the residual risk, the related mitigating factors and management of such risks.
3. Use retrospective and quantitative techniques in risk assessment or combination. Historical data in risk assessment has the benefit of drawing on data from past events to help anticipate future problems. Although the past is not always a reliable indicator of the future, consistent patterns can be usedto analyze data associated with AML and/or CTF suspicious transactions, if any. To enhance the review and analysis, the number and volume of transactions, the nature of the customer relationships are considered in the risk assessment.

13.3. AML Risk Rating Methodology

It is the policy of the organization to conduct risk assessment of its member clients during loan application and product enrollment. This is to ensure the organization can properly identify, evaluate and estimate the levels of AML risk involved in the transaction and determine acceptable level of risk, appropriate monitoring controls to detect and report suspicious transaction in a timely manner.

When to conduct Customer Risk Rating

Customer Risk Rating is assigned to member clients at account application or account enrollment stage based on several components considered including the documentary and non-documentary evidence in knowing/identifying the customer and subject to periodic review pursuant to the provisions hereof.

13.3.1. Risk Rating Classification

After identifying, evaluating and estimating the levels of risk that a member client is likely to engage in money laundering or terrorist financing, customers are classified as follows:

1. Low Risk – member client or customer pose a minor risk compared to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities and is an ideal level of risk;

2. Normal Risk – member client or customer does not pose a significant risk compared to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities and is an acceptable level of risk;

3. High Risk – member client or customer pose a major risk comparable to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities although within tolerable level of risk, but subject to enhanced monitoring.

13.3.2. Periodic Risk Assessment

After the initial risk rating is assigned to each member client, customer risk rating shall be periodically undertaken by the branch as follows:

- Low risk - At least every 36 months
- Normal risk - At least every 24months
- High risk - At least every 12 months

The designated AML and CTF Compliance Officer, whenever necessary, may trigger the periodic review.

Risk rating may be conducted as frequently as necessary when adverse information or knowledge relating to an account is acquired by the branch that, based on reasonable judgment, will warrant the accelerated re-assessment of the said member client.

The member client or customer's initial or current risk rating can be affected by a change in circumstances as well as the unusual transactions monitoring results. Therefore, customer risk rating may change over time.

13.3.3. Basic Risk Parameters

The risk parameters are generally classified into 3 categories, namely:

Account/Entity Risk - specific risk associated with the member client's type, nature of business, occupation or declared/anticipated transaction activity.

Geographic Risk - specific risk associated with doing business in, granting loans or product enrollment for member clients from a certain province or region, or facilitating transactions involving certain geographiclocations.

Products, Services, Transactions and Delivery Channel Risk - risk associated with the nature of specific loan and other financial products or services offered that can facilitate a higher degree of anonymity or involve thehandling of high volume of currency or currency equivalent or instantaneous transfer of funds from one account to another account for deposit or withdrawals.

1. Account/Entity Risk

   Existing and potential member clients and entities are categorized and described as follows:

   a. Individual. Natural person who purchases a product from MAESTRO company. May or may not be a Filipino citizen.

   b. Juridical. Corporation, partnership, association that may infuse funds in the form of donations or grants to the organization.

   c. Philippine Government Agency or Instrumentality. A government owned or controlled corporation (GOCC), local government unit, agency, police, military, judiciary or legislative.

   d. Non-Governmental Organization/Non-Profit Organization/Foundation or religious organization shall refer to a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works”.

   e. Remittance Agent. A natural person or entity that offers to remit, transfer or transmit money on behalf of any person and/or entity. These include money or cash couriers, money transmission agents, remittance companies and the like.

   f. Designated Non-Financial Business and Profession (DNFBP)
      1. Company service providers.

      2. Persons, including lawyers and accountant, who provide any of the following services:
         1. Managing client money, securities and other assets;
         2. Management of bank, savings, securities or accounts
         3. Organization of contributions for the creation, operation, or management of companies; and
         4. Creation, operation or management of juridical persons or arrangement, and buying and selling business entities.

g. Politically Exposed Person (PEP). An individual who is or has been entrusted with prominent public positions in the Philippines or in a foreign state including heads of state or of government, senior politicians, senior national or local government, judicial or military officials, senior executives of government or state owned or controlled corporations, important political party officials, their family members by consanguinity or affinity up to the sixth degree, and close personal and professional associates.

2. Geography Risk

Geography includes the geographic location of the branch, the geographic regions of the member clients' customer base.

High Risk Philippine areas due to reported cases of kidnapping and concerns related to peace and order situation with a perception of terrorist financing, cybercrime activities, New People's Army (NPA) rebel areas, Islamic extremists' activities, and presence of alleged narco-politicians based on the intelligence information from law enforcement agencies.

13.3.4. Default Risk Classification of Select Member Client Accounts

Regardless of the result of the Customer Risk Rating, the following are considered HIGH RISK and shall be subject to Enhanced Due Diligence and require appropriate Senior Officer, Management Committee or Board Committee approval:

Enhanced Due Diligence Review must be performed by the designated AML andCTF Compliance Officer to ensure transactions with persons classified as Politically Exposed Persons are for legitimate purposes and funded through legal means proportionate to the declared wealth and resources of said persons. Particular scrutiny is to be practiced over the review of **local government officials, which are known to have close relationships with prominent PEPs.**

- Barangay Chairman
- Kagawads
- LGU staff

"Senior Officer" shall refer to the next higher authority of the approving officer (i.e., Area Heads, Sector Heads or Regional Heads of branches or Group Heads.

13.3.5. Customer Risk Rating – Risk Factors

Risk Factor Numeric Weight

RISK FACTOR RATING	NUMERIC WEIGHT
Low Risk	1
Normal Risk	2
High Risk	3

Individual:

RISK FACTOR	RATIONALE/REMARKS
Risk Classification of Person **Notes:** • If risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH	To identify Account/Customer/Entity Risk, classified as follows based on numeric weights: 1. Individual is Filipino 2. Individual Person acting as collecting agent 3. Has relationship with prominent PEPs, its immediate family members, close relationships and close associates
Citizenship **Notes:** • If risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH Risk •	To identify Account/Customer/Entity Risk and Geographic Risk, classified as follows based on numeric weights: 1. Filipino Citizen, resident 2. Filipino Citizen, non-resident 3. Filipino Citizen with affiliation with entities operating with no legitimate business or economic reason
Geographical Address *Ref: Annex B – High Risk and Very High Risk Philippine Areas* **Notes:** • If present or permanent address is included in the FATF Identified Jurisdiction with AML/CFT Deficiencies risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH RISK	To identify Geographic Risk, classified as follows based on numeric weights: 1. Present or permanent address is within the branch/operating unit vicinity known to branch/operating unit personnel and properly identified thru KYC Documents 2. Present or permanent address is not falling under any of the High Risk Philippine Areas or outside the branch/operating unit vicinity. 3. Present or permanent address is within the High Risk Philippine Areas and outside the branch/operating unit vicinity, or Non-Philippine address. Present or permanent address is included in the FATF Identified Jurisdiction with AML/CFT Deficiencies

<table>
<tr><th>RISK FACTOR</th><th>RATIONALE/REMARKS</th></tr>
<tr><td>Individual identification</td><td>To identify Account/Customer/Entity Risk, classified as follows based on numeric weights:

1. Use of primary and secondary photo-bearing Philippine Government issued IDs
2. Use of primary or secondary photo-bearing Philippine Government issued IDs:
3. Use of Foreign government photo-bearing issued ID</td></tr>
<tr><td>Occupation/Nature of work or self-employment</td><td>To identify Account/Entity Risk, classified as follows based on numeric weights:

1. Employed locally; retired employee; pensioner, OFW; beneficiary of an OFW
2. Student; self-employed or unemployed but with spouse income
3. Unemployed but income is not derived from spouse or immediate family member (father, mother, son, daughter, brother or sister).</td></tr>
<tr><td>Source of Funds</td><td>To identify Account/Customer/Entity Risk, classified as follows based on numeric weights:

1. Salary, Property, Pension, Financial Products

<table>
<tr><th>TYPE</th><th>DESCRIPTION</th></tr>
<tr><td>Salary</td><td>Income from employment, professional fees (tutorial, therapy)</td></tr>
<tr><td>Property</td><td>Lease/rent, sale of property, inheritance</td></tr>
<tr><td>Pension</td><td>Retirement fund, payment drawn to support a person’s retirement (SSS, GSIS)</td></tr>
<tr><td>Financial Products</td><td>Insurance proceeds, investments, accounts with other banks)</td></tr>
</table>

2. Business, commission, allotment

<table>
<tr><th>TYPE</th><th>DESCRIPTION</th></tr>
<tr><td>Business</td><td>Income from business(any form of legal trade/business)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>RISK FACTOR</th><th>RATIONALE/REMARKS</th></tr>
<tr><td></td><td>
<table>
<tr><td>Commission</td><td>Agent or Sales Persons percentage from sales (e.g. property, product, insurance)</td></tr>
<tr><td>Allotment</td><td>Allowance, remittance (e.g. medical, education, domestic expenses, IRA)</td></tr>
</table>
3. Donations, gaming
<table>
<tr><th>TYPE</th><th>DESCRIPTION</th></tr>
<tr><td>Donation</td><td>Contribution, aids, tithes, church collection, stipend, love gift</td></tr>
<tr><td>Gaming</td><td>Winnings (gaming, lottery)</td></tr>
</table>
</td></tr>
<tr><td>Account Opening Method: MFI Loan Application and Micro-insurance Enrollment Form</td><td>To identify Account/Entity Risk, classified as follows based on numeric weights:

1. Face-to-face with (all) product applicants
2. Face-to-face with some product applicants but authenticated by maintaining MAESTRO branch/operating unit officer
3. Product applicants are otherwise authenticated by another sufficiently authorized and competent MAESTRO branch/office Officer</td></tr>
<tr><td>Declared Monthly Transaction Volume (MTV)</td><td>To identify Account/Customer/Entity Risk and Products and Services Risks, classified as follows based on numeric weights:

1. Individuals with Declared Monthly Transaction Volume up to P100,000
2. Individual/s with declared monthly transaction volume of over P100,000 to P500,000
3. Individual/s with declared monthly transaction volume of over P500,000</td></tr>
<tr><td>Actual Gross Monthly Volume of Transaction (GMVT) - to be used during risk assessment</td><td>To identify Products and Services Risk during re-assessment based on actual gross account movements (credits only), classified as follows based on numeric weights:

1. GMVT up to P100,000
2. GMVT is over P100,000 and up to P500,000
3. GMVT – is over P500,000</td></tr>
</table>

RISK FACTOR	RATIONALE/REMARKS
Length of Relationship	To identify Account/Customer/Entity Risk and Products and Services Risk, classified as follows based on numeric weights: 1. Existing customer with relationship of at least 1 year 2. Existing customer with relationship of less than 1 year 3. No prior relationship

Non-individual (Corporations, Partnerships, Associations, Charitable Institutions):

RISK FACTOR	RATIONALE/REMARKS
Designated Authorized Signatories **Notes:**	To identify Account/Entity Risk, classified as follows based on numeric weights: Citizenship 1. Resident Filipino Citizen 2. Non-Resident Filipino Citizen 3. Resident and non-resident Filipino affiliated with prominent PEPs Individual Identification 1. Use of primary and secondary photo-bearing Phil. Government issued ID 2. Use of primary or secondary photo-bearing Phil. Government issued IDs 3. Use of Foreign government photo-bearing issued ID Risk Classification of Person 1. Individual/s other than those listed as designated professionals 2. Designated Professionals (Lawyers and Accountants acting as Independent Professionals) 3. PEP, its immediate family members and close associates; non-accredited Remittance Agent

RISK FACTOR	RATIONALE/REMARKS
Nature/Type of Industry Business **Notes:** • If risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH	To identify Account/Entity Risk, classified as follows based on numeric weights: 1. Simple micro-entrepreneur 2. With Complex business exposure 3. Complex exposure linked to high risk businesses Remittance Companies/ Agents, LGUs listed under the High Risk Philippine Areas
Place of Incorporation/Registration (applicable to accreditation of third party service providers) **Notes:** • If risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH	To identify Account/Entity Risk, classified as follows based on numeric weights: 1. Incorporated/registered in the Philippines 2. Incorporated/registered outside the Philippines **but** country is not listed in FATF list. 3. Incorporated/registered outside the Philippines **and** country is listed in the FATF list or GTI to be with highest impact of terrorism
Corporate address/Principal Headquarters/Head office **Notes:** • If present or permanent address is included in the FATF Identified Jurisdiction with AML/CFT Deficiencies risk rating is 3 (High Risk), CRR shall be automatically tagged as HIGH	To identify Account/Entity Risk, classified as follows based on numeric weights: 1. Present or permanent address is within the branch/operating unit vicinity known to branch/operating unit personnel and properly identified thru KYC Documents 2. Present or permanent address is not falling under any of the High Risk Philippine Areas or outside the branch/operating unit vicinity. 3. Present or permanent address is within the High Risk Philippine Areas and outside the branch/operating unit vicinity, or Non-Philippine address. Present or permanent address is included in the FATF Identified Jurisdiction with AML/CFT Deficiencies or in Global Terrorism Index (GTI)
Corporate/Organization Documents	To identify Account/Entity Risk, classified as follows based on numeric weights: 1. Use of Philippine issued registration/ incorporation documents; 2. Use of non-Philippine incorporation/ registration papers duly authenticated by Philippine Consulate Office/s

RISK FACTOR	RATIONALE/REMARKS
	3. Use of registration documents as a Remittance Agent or Money Service Business.

13.3.6. Customer Risk Rating Process

Customer Risk Rating Range

Customer Risk Rating Total (CRRT) refers to the overall result when all the Risk Factors are summed up according to each of their relative numeric weights. The risk rating range is as follows:

Risk Rating	Numeric Range
Low Risk	25 or less
Normal Risk	26-35
High Risk	36 or higher

MAESTRO member clients are typically classified “LOW RISK” unless there is confirmed information that will require higher numeric range to classify as “NORMAL RISK”or will automatically qualify tagging the member client as “HIGH RISK.”

a. Individual - this CRR tool is used for individuals when opening and during periodic risk assessment of Loans and Product applications
b. Non-Individual – this CRR tool is used to non-individuals entering into third party service provider business relationships with MAESTRO.

13.3.7. Customer Risk Rating Tagging of Member Client

Tagging shall be performed by the designated branch personnel and approved by the authorized bank officer/s only. Random Day 2 validation of customer information encoded in the system vis-a-vis properly accomplished forms and identification documents is necessary to ensure customer data integrity in the system.

The customer risk ratings are subject to periodic reviews based on defined "cycles" for high risk, normal risk and low risk customers.

1. MAESTRO Employees

   All new and existing employees of MAESTRO are classified “LOW RISK”. However, if MAESTRO employee has been a subject of investigation related to internal fraud or AML related financial crimes, account should be classified “HIGH RISK.”

2. Remittance Agent - shall refer to persons or entities that offer to remit, transfer or transmit money on behalf of any person to another person and/or entity. These include money or cash couriers, money transmission agents, remittance companies and the like. Remittance Agents are generally HIGH RISK.

3. Pawnshop Business shall refer to the business of lending money on personal property that is physically delivered to the control and possession of the

pawnshop operator as loan collateral. Pawnshop Business are generally "HIGH RISK."

4. Pawnshop with MSB License shall refer to the business of lending money on personal property that is physically delivered to the control and possession of the pawnshop operator as loan collateral with BSP registered corollary business activities including remittance operations. (Circular No. 938) Pawnshop with MSB License are generally "HIGH RISK".

13.3.8. Persons Ultimately Responsible for High Risk Member Client Accounts and Transactions

In all instances of acceptance of a HIGH RISK member client or customer requires senior officer approval.

Senior Officer shall mean:

1. Sector Head, Region Head, MFI Strategic Head (for Branches)
2. Group Head for Head Office Units

The above-mentioned Senior Officers shall be ultimately responsible in the effective implementation of the following policies/procedures when dealing with HIGH RISK customers:

a. Gathering of the minimum information and documents required from individual member clients and corporate or juridical persons.
b. Perform Negative List verification.
c. Conduct face-to-face interview and review of Customer Risk Rating
d. Approval of Senior Officer for HIGH Risk member client.
e. Conduct second level transaction annually to validate and support the reviews conducted at branch/business unit level.
f. Issue AML Compliance Quarterly Certification to the effect that HIGH RISK KYC records and transactions were reviewed, unusual transactions were escalated to designated AML and CTF Compliance Officer and STRs were filed for transactions found to be indeed suspicious, if there is any.

kkk. Enhanced Due Diligence

EDD for High Risk customers is especially critical in understanding their transactions and implementing a suspicious transaction monitoring and reporting system. High Risk member clients and their transactions should be reviewed more closely at loan application or product enrollment or and more frequently throughout the term of their relationship with MAESTRO.

14.1. Enhanced Due Diligence

Branches and Business Units shall apply EDD when any of the following circumstance exists/occurs:

14.1.1. Raises doubt as to the accuracy of any information or document provided or the ownership of the entity;

14.1.2. Justifies re-classification of the customer from low or normal risk to high-risk pursuant to AMLC, IC, SEC and BSP rules and regulations or MAESTRO's policy or when there is knowledge in the activity changes (e. g, low risk rate upon openingbut later subject of suspicious transaction reporting but change to High Risk or

vice versa and the like). Should there be a need to maintain and change customer risk rating (e.g., expected account activity, change in employment or business relations), approval of a Senior Officer is required.

14.1.3. Any of the circumstance for the filing of suspicious transaction exists but not limited to the following:

1. Transacting without any underlying legal trade, purpose or economic justification;
2. Member client is not properly identified;
3. Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profile and/ or client's past transactions;
4. Structuring transactions in order to avoid being the subject of covered transaction reporting; or
5. Knowing that a customer was or is engaged or engaging in any unlawful activity defined under the AMLA
6. Any transaction that is similar, analogous or identical to any of the foregoing.

14.1.4. Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by the BSP, AMLC and other international entities or organizations such as Office of Foreign Asset s Control (OFAC) of the US Department of Treasury and United Nations Security Council that requires Senior Officer's approval.

14.1.5. All complex, unusually large transactions, all unusual patterns of transactions, which have no apparent economic or unlawful purpose, and other transactions that may be considered suspicious.

When Conducting EDD, gather documents to support the following:

1. Sources of wealth and funds;
2. Nature of occupation and/or business;
3. Reason for intended of performed transaction; and
4. Other identification information, which the covered person deems necessary to verify the identity of the customer, and their agents and beneficial owners.

14.2. Validation Procedures

Verification of procedures for individual member clients shall include but not limited to the following:

14.2.1 Confirming the date of birth from a duly authenticated official/identification document.

14.2.2 Verifying the address through evaluation of utility bills, bank credit card statement, or other documents showing permanent address or through on-site visitation.

14.2.3 Contacting the customer by phone, email or letter

14.2.4 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.

14.2.5 Determining the veracity of the declared source of funds.

14.2.6 Validation procedures for corporate or juridical person shall include but not limited to the following:

1. Require the submission of audited financial statements conducted by a reputable accounting/auditing firm;
2. Inquiring from the supervising authority the status of the entity
3. Obtaining bank references;
4. Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address;
5. Contacting the entity by phone or email.

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 Branch or Business Unit shall not allow a product purchase or transaction to proceed or initiate termination of the relationship with the individual or entity without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

14.3. Enhanced Due Diligence when Dealing and Remittance Agents (RAs)

In compliance with BSP Memorandum No. M–2016–004, when dealing with and RAs, Business Unit must perform the following:

14.3.1 Require submission of duly accomplished AML Due Diligence Questionnaire and AML/CFT program of RAs. This must be reviewed by Designated AML and CTF Compliance Officer and approved by a Senior Officer.

14.3.2 Obtain registration certificate issued by BSP and verify registration status in the list of BSP registered FXDs, MCs and RAs posted at BSP website.

14.3.3 Require submission of proof of registration with the AMLC;

14.3.4 Obtain additional information and conduct validation procedures, as needed.

14.3.5 Evaluate the business operation and determine if there exists derogatory information;

14.3.6 Deny business relationship if result of due diligence is unsatisfactory.

III. Customer Identification

Customer Identification Process has to be carried out at different stages:

- While establishing a member client or business relationship
- While undertaking any occasional but relevant business transaction for any member client who has not otherwise established relationship with MAESTRO.
- When the Branch or Business Unit has doubts about the veracity or the adequacy of thepreviously obtained member client information or identification data.

Customer identification shall mean establishing and recording the true identity of the member client based on valid identification documents. Branch or Business Unit needs to obtain sufficient information necessary to establish the identity of each member client and the purpose of the intended nature of business relationship. The following shall be taken into account during the customer identification stage.

- Nature of the service or product to be availed of by the member client and the purpose of the product purchase

- Source of funds/nature of business activities
- Residence of operations or member client came from high risk Philippine Areas.
- Affiliation with PEPs or high profile public position by the member client or corporations with the directors/trustees, stockholders, officers and/or authorized signatories
- Watch list of individuals and entities engaged in illegal activities or terrorist financing related activities as circularized by BSP, IC, SEC and AMLC and other international entities or organizations such as the OFAC and UN Sanctions List
- Business activities

In all instances, approving Officers must ensure the KYC process for a specific customer was documented; the required information and documents were complied with.

15.1. Minimum Information and Documents Required for Individual Member Clients and Authorized Signatory/ies of Corporate/Juridical Person

Individual member clients shal. For sole proprietorship entities, the organization must establish the relationship of the trade name with the registered owner and the member client account.

The following minimum information shall be required to be obtained from individual member client or authorized signatory/ies of corporate or juridical person. The information shall be confirmed with the valid identification documents.

- Name of customer and/or PhilSys number
- Date and place of birth
- Sex
- Address
- Contact number or information
- Citizenship or Nationality
- Specimen signature or biometrics of the customer
- Name, address, date and place of birth, contact number or information and citizenship or nationality of beneficiary or beneficial owner, whenever applicable.

Business or trade related transactions shall mean transactions of covered persons natural or juridical referred to below:

1. Banks, quasi-banks, trust entities, pawnshops, non-stock savings and loans associations, other non-bank financial institutions which under special laws are subject to BSP supervision and/or regulation, remittance and transfer companies and other similar entities and all other persons and their subsidiaries and affiliates supervised or regulated by the Bangko Sentral ng Pilipinas (BSP);

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

3. Securities dealers, brokers, salesmen, investment houses and all other similar persons managing securities or rendering services as investment agent, advisor or consultant, (ii) mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities, and (iii) other entities administering or otherwise dealing in commodities or financial derivatives based

thereon, valuable objects, cash substitutes and other similar monetary instruments or properties supervised or regulated by the Securities and Exchange Commission (SEC);

4. Company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; and

5. Persons, including lawyers, accountants and other professionals, who provide any of the following services:

    a) Managing of client money, securities or other assets;

    b) Management of bank, savings or securities accounts;

    c) Organization of contributions for the creation, operation or management of companies; and

    d) Creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

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

15.2. Minimum Information and Documents Required for Juridical Person

The following minimum information shall be required to be obtained from juridical person:

1. Customer Information

    - Name of juridical person/s;
    - Name, address, citizenship or nationality of beneficial owner, if applicable, and authorized signatories;
    - Official Address
    - Contact numbers or information;
    - Nature of business; and
    - Specimen signature of the authorized signatory.

2. Identification Documents

    - Certificates of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, Certificate of Incorporation or Partnership issued by the Securities and Exchange Commission for

corporations and partnerships respectively, and by the BSP for remittance agents by AMLC for covered persons;
- Proof of registration with the Anti-Money Laundering Council (AMLC) for remittance agents.
- Secondary license or certificate of authority issued by the supervising authority or government agency;
- Articles of incorporation/Partnership
- Registration Data Sheet/Latest General Information Sheet;
- Secretary's Certificate citing the pertinent portion of the Board or Partners' resolution, authorizing the signatory to sign on behalf of the entity; and
- For entities registered outside of the Philippines, similar documents and/or information shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

Approving Officers shall have the primary responsibility of requesting credit investigation on the business activity and validation of business registration documents to ensure that the entity has not been or in the process of being, dissolved, struck-off, wound up, terminated, or otherwise placed under receivership or liquidation. In instances wherein, the bank officer is not comfortable and/or fully satisfied with the information provided, additional verification may be conducted by requesting credit investigation on business operations and authorized signatories of the company. Credit investigation is optional for companies listed in the Philippine Stock Exchange or in the Top 1000 Corporations in the Philippines.

15.3. Valid IDs

The following guidelines govern the acceptance of valid ID cards for all types of financial transaction by a member client and the authorized signatory/ies of a corporate or juridical person.

a. Member clients and authorized signatory/ies of a corporate or juridical person who engage in a financial transaction with MAESTRO for the first time shall be required to present the original copy and submit clear copy of valid photo-bearing IDs with signature issued by an official authority.

LOW/NORMAL RISK	HIGH RISK
• Any 1 of the valid IDs (primary or secondary ID)	• 2 valid IDs - 1 primary **and** 1 secondary; or 2 primary IDs **and** • Submission of any 1 of the following: – Latest bank/broker's/ insurance statements – Latest telephone bills – Latest utility/cable bills – Latest credit card bills – Latest club membership bills – Latest GIS submitted to SEC as proof of being a Director/ Officer of an entity

Valid IDs include the following:

Primary:
- Philippine Identification Card (PhilID) issued by the Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys)
- Valid Passport
- Driver's license with Official Receipt

- Unified Multi-Purpose ID
- Digitized BIR TIN Card
- SSS ID
- GSIS e-Card
- PRC ID
- IBP Lifetime Membership ID
- NBI Clearance
- Work permit issued by DOLE for foreign nationals

Secondary:

- Police Clearance
- Digitized Postal ID
- Voter's ID
- Tax Identification Number Card
- Barangay Certification
- Senior Citizen Card
- MARINA Professional Identification Card
- OWWA ID
- OFW ID
- Seaman's book
- Alien Certification of Registration/Immigrant Certificate of Registration
- Government Office and GOCC ID (e.g. AFP, HDMF IDs)
- Certification from NCWDP
- DSWD Certification or DSWD 4Ps ID
- IBP ID
- Phil-Health ID Health Insurance Card ng Bayan
- Company IDs issued by private entities or institutions registered with or supervised or regulated either by the BSP, SEC or IC"

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

c. Where the member client or authorized signatory is a non-Philippine resident, similar IDs duly issued by the foreign government where the customer is a resident or a citizen may be presented.

d. MAESTRO shall require their member clients or authorized signatory to submit a clear copyof one (1) valid ID on a one-time basis only at the commencement of business relationship. Member clients shall be required to submit an updated photo and other relevant information on the basis of risk and materiality.

e. MAESTRO may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the member client.

f. Whenever it deems necessary, MAESTRO may accept other IDs not enumerated above provided that it shall not be the sole means of identification.

g. In case the identification documents mentioned above or other identification documents acceptable to the organization do 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, MAESTRO may utilize its own technologyto take the photo of the customer or authorized signatory.

It is encouraged that the customer submits at least two valid IDs, one of which must be photo bearing and with signature.

15.4. Conducting the Interview and Establishing Identity

ACCOUNT OFFICER OR INSURANCE OFFICER:

15.4.1 Briefs the prospective member client on the requirements and features of MAESTRO products and services being applied and/or transaction being conducted.

15.4.2 Conducts an initial Interview and performs exploratory questioning to establish information pertaining to:

- Personal circumstances
- Purpose of or product enrollmentand/or transaction applied for
- Nature of Business
- Source of funds/source of wealth
- Identification of Beneficiaries
- Expected Transaction Amount
- Expected Transaction Volume/Count
- Reason for choosing MAESTRO particularly when the residence of member clientis outside the territorial jurisdiction of the concerned branch

15.4.3 Observes unusual behavior of member client during the conduct of interview and looks for the following warning signs:

- Member client has unusual or nervous demeanor
- Member client uses unusual or suspicious identification documents that cannot be readily verified.
- Member client is reluctant when establishing a new product application, to provide complete information about the nature and purpose of its business, anticipated transaction activity, prior other MFI relationships, names of its officers and directors, or information on its business location.
- Member client home/business telephone is disconnected.
- Member client uses a temporary address.
- Customer's background differs from that which would be expected based on his or her business activities.
- A business or new member client asks to be exempted from reporting or record-keeping requirements.

15.4.4 Requests member client to produce the original of documents of identity issued by an official authority bearing his photograph such as passport, driver's license, company identification cards, SSS card, GSIS card, Philhealth, DSWD, Voter's ID, and other valid IDs.

15.4.5 Examines carefully the documents of identity presented looking for any sign of erasures, alterations and tampering.

15.4.6 Interviews member client to validate information/data elicited during the initial interview and exploratory questioning against the presented identity documents.

15.4.7 Observes the following steps if the member client lacks the proper documents and/or results of the interview and exploratory questioning are poor.

15.4.8 Requests the member client to submit acceptable IDs before allowing the opening of the MAESTRO product account or product enrollment or processing the transaction/service applied for if he lacks the proper documents.

15.4.9 Courteously decline the application for product or service transaction –

- if the member customer fails to satisfactorily explain discrepancies between the information elicited during the preliminary interview/questioning and documents presented
- There are signs of erasures and tampering of documents presented.
- Displayed suspicious and questionable behavior.

15.4.10 Requests member client to fill out product application forms and micro-insurance enrollment form of MAESTRO with photocopy of documents of identity presented if he/she satisfactorily meet the requirements and passed the initial interview and questions. Ensures that the forms are properly accomplished.

15.4.11 Determine the member client AML customer risk rating (i.e. Low Risk, Normal Risk, High Risk)

15.4.12 Forwards all documents to Senior Account Officer/Branch Manager or Area Head for review and approval.

15.5. Conducting Final Interview and Approval of Account and/or Requested Transaction

SENIOR ACCOUNT OFFICER, BRANCH MANAGER or SENIOR INSURANCE OFFICER

In the event there are doubts to the accuracy and completeness of member client information and document, conducts final interview of the member client and validates information/data gathered against documents presented. Reviews the accuracy of data and completeness of opening documents.

15.5.1 Checks if the name of the customer, corporation including its incorporators and officers, and/or beneficial owners appears on the negative lists of known or suspected terrorists or terrorists' organizations available in AMLC and BSP website.

In the event of "name match" print the result with date and time and refer to Area Head or Sector Head for guidance and subject to EDD. If upon further verification of the Area Head or Sector Head confirmed positive match, the transaction should not proceed. Responsible branch should submit STR within 48 hours to the designated AML and CTF Compliance Officer for endorsement to STR filing with the Executive Director of AMLC. The printed results shall be part of KYC and/or EDD documentation.

15.5.2 Courteously decline product application and enrollment if the member client fails to satisfactorily meet requirements or pass the final interview and ensure if circumstances warrant, filing of a suspicious transaction report.

15.5.3 For High Risk member client or customer secure approval from Senior Officer.

15.5.4 Branch Account Officer or Insurance Branch Account Officer or Insurance Officer approves processing of product application if everything is in order.

Endorses the application and product enrollment forms toappropriate authority.

15.6. Encoding AML CIF Mandatory Information

The Account Officer or Insurance Officer should ensure that the following mandatory information are encoded immediately upon product account opening or enrollment.

Minimum Information
FULL NAME
PRESENT ADDRESS
PERMANENT ADDRESS
DATE OF BIRTH
PLACE OF BIRTH
NATURE OF WORK
CONTACT NUMBERS (mobile, fb account)
TIN, SSS, GSIS, DSWD, Postal ID, MAESTRO ID (other IDS presented)
SOURCE OF FUNDS
Other Relevant Information (if applicable)
Customer Risk Rating (Low, Normal or High Risk)
Individual or Non-Corporate Customer Details

15.7. Face-to-face Contact

No new loan or product account shall be opened and created withoutface-to-face contact and personal interview of MAESTRO's duly authorized employee.

The use of Information and Communication Technology (ICT) in the conduct of face-to-face contact and interview may be allowed; provided, MAESTRO is in possession of and has verified the identification documents submitted by the prospective member client prior to the interview and the entire procedure is documented.

MAESTRO shall clearly define the instances when the conduct of face-to-face is reasonably practicable, depending on the product, type of business and risk involved, or when the useof ICT shall apply. Also, the covered person should adopt policies and procedures to address any specific risk associated with deferred or technology-aided face-to-face verification and personal interview.

15.8. Updating of Customer Identification Information and Documents based on Materiality and Risk

It is the policy of MAESTRO to update customer's identification information and documents at least every three (3) years. However, an earlier update may be warranted in certain circumstances.

The updating of customer information and documents may be triggered by, but not limited to the following scenarios:

a) Alerts from media and news
b) An unusual activity was identified and EDD was conducted; and
c) Upgrading and downgrading of member client AML Customer Risk Rating (CRR)

For customers with no updates the branch shall certify in a call report to the effect that all information indicated in the CID file are current and updating is not needed.

However, where additional information cannot be obtained, or any information or document provided is false or falsified or result of the validation process is unsatisfactory, branch and business units shall deny business relationship with member client without prejudice to filing of STR with the AMLC, when circumstances warrant.

The following are the information for updating:

Individual	Juridical Persons
1. Address 2. Occupation/ Nature of work 3. Contact number or information 4. Source of fund /Source of Wealth 5. Expired ID with Photo 6. Specimen Signatures	1. Official Address 2. Articles of Incorporation and By-Laws 3. General Information Sheet 4. Secretary Certificate of Authorized Signatories and signature 5. Beneficial Owners & Authorized Signatories (same with individual document requirements) 6. Specimen Signatures 7. Regulating Government Agency Certification (i.e. BSP Certificate and AMLC Certificate for MSBs) 8. Nature of Business 9. Source of fund /Source of Wealth

15.9. Accreditation of Remittance Agents

A remittance tie-up and/or pay-out arrangement is a partnership between MAESTRO and a business entity engaged in money transfer operations, presently in possession of valid business and remittance licenses. The system of the accredited remittance partner may be interfaced with MAESTRO's system.

Potential remittance tie-up partners must undergo the proper accreditation process in accordance with AML/CFT regulations. The Head Office Officer handling remittance tie-up arrangements and the designated AML and CTF Compliance Officer must establish the true and full identity of the potential remittance partner and ensure that it was able to meet the established minimum requirements and conditions prior to endorsement and approval.

15.11.1. Documentary Requirements for Tie-ups

In order to manage the risks involved in agent relationship, the following requirements prior to endorsement of agents/agencies for approval by Senior Management, the following documents are submitted by the prospective agents/agencies prior to establishment of remittance tie-up relationship with MAESTRO.

- Certificate of Registration with the appropriate host country regulatory unit in addition to the minimum information and documents required from individuals and corporate entities;
- Proof of registration with the Anti-Money Laundering Council (AMLC) to comply with the reporting requirements, or its equivalent and if applicable;
- Photocopy of valid (not expired) business license permit;
- Certifications that its officers and personnel have attended AML Training or will participate in AML Training within six (6) months from date of accreditation;

- Duly accomplished AML Due Diligence Questionnaire reviewed by the Head Office Officer and approved by the designated AML and CTF Compliance Officer;
- Signed and Notarized Memorandum of Agreement (MOA) that covers the remittance tie-up of which provisions for the renewal and termination of the arrangement must be included;
- Service Level Agreement (SLA) that defines, specifies and/or limits the services the remittance partners shall provide;
- Approval from Senior Management;
- Updated and approved AML/CFT program that contains policies and procedures observed by the remittance partners for the prevention of money laundering and terrorist financing;
- Non-disclosure agreement that defines, executes and encompasses the totality of handling confidential information that could be shared by both parties;
- Articles of Incorporation or Association and By-Laws;
- Board or Partner's Resolution duly certified by the corporate or partner secretary authorizing the signatory to sign on behalf of the entity, or its equivalent and if applicable;
- Company Profile;
- Audited Financial Statements for the previous two years of operation prepared by an independent Certified Public Accountant;
- Credit Investigation Report covering Philippine tie-ups or credit rating/scoring for overseas tie-ups and;

For entities registered outside the Philippines, similar documents and/or information shall be obtained, duly authenticated by the Philippine Consulate where said entities are registered.

To further strengthen MAESTRO's compliance, remittance entities shall be required to accomplish the AML Due Diligence Questionnaire for Remittance Agents. The replies of the remittance partners to the said questionnaire must be updated annually. No settlement accounts shall be opened without Senior Officer's approval and accomplished AML Due Diligence Questionnaire reviewed and approved by the designated AML and CTF Compliance Officer.

All remittance relationships of MAESTRO must be covered by a signed memorandum of agreement.

The accreditation of the remittance agents shall be reviewed annually and if with adverse findings, remittance tie-up relationship with the agent may be terminated subject to written notice and terms and conditions of the signed agency agreement. Renewal of the agency agreement must be approved by Senior Management.

MAESTRO may provide AMLA Compliance Awareness Seminar with its remittance tie-ups/agents to reiterate awareness of their obligations and AML compliance responsibilities.

15.11.2. Documentary Requirements for Pay-out Partners

- Remittance License from BSP;
- Proof of registration with the Anti-Money Laundering Council (AMLC);
- Photocopy of valid (not expired) business license permit;

- Duly accomplished and updated AML Due Diligence Questionnaire reviewed by designated AML and CTF Compliance Officer.
- Updated and approved AML/CFT Program;
- Approval of Senior Management and the President;
- Certification of AML Training;
- Signed and Notarized Memorandum of Agreement (MOA) between MAESTROand the payout partner
- Credit Investigation Report including checking with reputable credit agencies and regulatory body/agency website.
- Corporate Write-up;
- SEC Registration Certificate;
- Articles of Incorporation and By-Laws;
- Latest copy of Annual Report;
- Profile of Directors and Senior Management;
- Brief background on the shareholders of the company; and Last three (3) years of audited financial statements.

15.10. Management of Remittance Agents

MAESTRO shall adopt policies and procedures for the management of RAs to serve as referenceguides for the employees. The development of these policies and procedures further emphasizes MAESTRO's commitment to adhere to the requirements set by regulatory agenciesand adopt to best practices for the prevention and detection of money laundering and terrorist financing.

Remittance agents shall refer to persons or entities that offer to remit, transfer or transmit money on behalf of any person to another person and/or entity. These include money or cash couriers, money transmission agents, remittance companies and the like. (Section 4511N.1 MORNBFI).

15.12.1. Customer Identification

The customer identification process is undertaken to establish and record the true identity of RA through business documents and valid identification documents for its authorized signatories.

In establishing business relationships with remittance agents, the following are taken into account, to establish the customer's identity, purpose and intended nature of the business relationship:

- Background and source of funds;
- Country of origin and place of operations;
- Public or high profile position of directors, trustees, stockholders, officers and/or authorized signatory/ies;
- Verification of entity name, its signatories and key officers in the watch list of individuals and entities engaged in illegal activities or terrorist financing-related activities as circularized by BSP, AMLC and other international entities or organizations such as OFAC, Dow Jones and UN Sanctions List;
- Business activities; and
- Types of services / products and transactions to be entered with MAESTRO.

15.12.2. Minimum Information and Documents Required for Sole Proprietorships or Authorized Signatory/ies of Corporate / Juridical person which are RAs

The following minimum information and documents must be obtained:

- Certificate of Registration issued the Department of Trade and Industry (DTI) for single proprietors and by the Securities and Exchange Commission for corporations and partnerships,
- Proof of registration with BSP as RA;
- Proof of registration with AMLC;
- Business Permits;
- Articles of Incorporation or Association and By-Laws;
- Official address (The registered place of business of the RA, as indicated in the BSP Certificate of Registration it submitted, must be within the city / municipality of the branch. If an RA is known to the officers of the branch but is not within the city / municipality where the branch is located, proper documentation must be prepared, certified by a senior officer):
- Board or Partners' Resolution duly certified by the Corporate/Partners' Secretary authorizing the signatory to sign on behalf of the entity;
- Latest General Information Sheet which lists the names of directors / trustees / partners, principal stockholders owning at least 20% of the outstanding capital stock and primary officers such as the President and Treasurer;
- Contact numbers of the entity and its authorized signatory/ies;
- Source of funds and nature of business;
- Name, present and permanent address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, if applicable; and
- For entities registered outside the Philippines, similar documents and/or information shall be obtained, duly authenticated by the Bank's branch officer, authorized bank representative or the Philippine Consulate where the entities are registered.
- For RAs who are sub agents-Endorsement letter from principal agent

15.12.3. Enhanced Due Diligence

The increased exposure to money laundering and terrorist financing due to the risks inherent to business activity of RAs warrants enhanced measures. As such, the following EDD procedures may be performed that are consistent with BSP Memorandum M-004-2016 dated April 5, 2016 when dealing with these types of business relationships.

1. Require submission of duly accomplished AML Due Diligence Questionnaire and/or AML/CFT program of RAs. This must be reviewed and approved by Designated AML and CTF Compliance Officer.
2. The status of registration of the RA with BSP and AMLC must be verified and periodically checked against the electronic registry of BSP and AMLC.
3. Require submission of proof of registration with the AMLC
4. Evaluate the business operation and determine if the purpose is consistent with the RA profile.
5. Deny business relationship if result of due diligence is unsatisfactory.
6. A business call with RA must be conducted at least annually and in case of any adverse information, document through a business call report prepared by the Head Office Officer and approved by a senior officer.

7. RAs are required to present proof that they have undergone AML/CFT training conducted internally or by reputable financial institution/organization within the last two (2) years.

No new business relationship shall be opened with RAs without complying with the requirements of Items stated above.

mmm. Reporting of Covered Transactions

Covered Transaction (CT) is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of FIVE HUNDRED THOUSAND PESOS (Php 500,000.00) within one (1) banking day.

All covered transactions shall be reported to AMLC within five (5) working days from occurrence thereof, unless the AMLC prescribes a longer period not exceeding fifteen (15) working days.

16.1. Deferred Reporting of Certain Covered Transactions

Pursuant to AMLC Resolution No. 10 dated January 24, 2013, the following are considered "non-cash, no/low risk covered transactions" the reporting of which to the AMLC are deferred:

16.1.1. For entities/units supervised by Securities and Exchange Commission (SEC)

a. Transactions between banks and quasi-banks operating in the Philippines;

b. Roll-over of client's investments or deposit substitutes;

c. Transactions between parent bank and its subsidiary or associate financing company or affiliates;

d. Payment of loan and/or its corresponding interest regardless of the manner of payment (cash/fund transfer, debit of account, check), provided that the grant of loan was previously reported as covered transaction;

e. Loan repricing, loan renewal, loan restructuring, provided that there is no change in borrower's name, otherwise, the loan shall be considered as new loan, hence, reportable;

f. Investment or Divestment of Mutual Funds;

g. Internal operating expenses and capital expenditures of covered institutions (these are necessary expenses of covered institutions for the normal day-to-day running of a business. These are transactions of covered institutions and, therefore, not reportable. These may include payment of salaries, taxes, debt service, SSS premiums, Pag-IBIG contributions and employee's benefits).

h. Adjusting entries or reclassification of accounts

i. Service fees, proprietary revenue fees, arrangement fees, loan syndication fees and other form of fees incidental to loans granted or investments sold, provided that the loans granted or the sale of investment was reported at gross or at its principal amount.

16.1.2. For entities supervised by the Insurance Commission (IC)

a. Transactions between domestic insurance companies/professional re-insurers/intermediaries licensed by the Insurance Commission;

b. Renewal of non-life insurance policies under the same terms and conditions provided that a CTR has been previously filed;

c. Automatic premium advance;

d. Collection of premium payments from telemarketing, or direct marketing or through SMS and/or by way of salary deductions, where the bulk settlement exceeds P500,000.00 but the individual transactions are below the reporting threshold amount;

e. Group life insurance and hospitalization insurance;

f. Transaction of members of Mutual Benefit Associations pertaining to basic benefits;

g. Payment of loan and/or its corresponding interest regardless of the manner of payment, provided that the grant of loan was previously reported as covered all transaction;

h. Bulk settlement of claims on death and disability benefits of a policy where individual claim does not exceed P500,000.00;

i. Transactions coursed through brokers, agents and other intermediaries, in which case, however, the insurance company (principal) shall report the said transactions;

j. Internal operating and capital expenditures of covered institutions (*these are necessary expenses of covered institutions for the normal day-to-day running of a business. These are transactions of covered institutions and, therefore, not reportable. These may include payment of salaries, taxes, debt service, SSS premiums, Pag-IBIG contributions and employee's benefits).*

16.1.3. Adjusting entries or reclassification of accounts.

nnn. Detection and Monitoring of Suspicious Transactions

Area Managers Program Manager, Senior Account Officer, Account Officer, Insurance Officer and Senior Insurance Supervisor

A. Conducts due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the Branch knowledge of the member client's business and risk profile.

B. Upon receipt of information and confirmed knowledge, reviews, analyzes transactions processed based on the following sources of information/data:

i. Transaction Report

Conducts due diligence on the business relationship and scrutiny of transactions. This is to ensure transactions conducted are consistent with the Branch knowledge of the member client's business and risk profile. Any unusual transaction observed must be immediately escalated to the Group Head and the designated AML and CTF Compliance Officer.

ii. Source documents of transactions processed for the period.

iii. Randomly checks if the name of member client, corporation including its incorporators and officers, and/or beneficial owners appears of known or suspected terrorists or terrorist organizations made available by regulatory agencies or bodies such as the Anti-Money Laundering Council, Bangko Sentral Ng Pilipinas and Anti-Money Laundering Council of any foreign government agency like the Office of Foreign Assets Control (OFAC).

The review process may be done by analyzing member client's transactions within a specified rolling period of at least 90 days.

C. Notes down and examines the background and purpose of all complex, unusually large transactions and all unusual patterns of transaction. Validation with external parties may be conducted to determine source of funds, purpose and confirmation of client profile and relationship of the beneficiaries with the member client.

D. Takes into account clues or early warnings signs or red flags to which member client and transactions warrant additional or extra attention.

E. If confirmed qualified for STR filing, prepares the Suspicious Transaction (STR) Report for submission to the Executive Director of the Anti-Money Laundering Council (AMLC).

ooo. Reporting Suspicious Transactions

Suspicious transactions (ST) are transactions with covered institutions, regardless of the amount involved, where any of the following circumstances exist:

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

Unlawful activities under the AMLA (Predicate Offenses)

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, 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 R.A. No. 9208, otherwise known as the Anti-Trafficking in Persons Act of 2003, as amended;
20. Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
21. Violations of Sections 86 to 106 of Chapter IV, of Republic Act No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
22. Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the Philippine Mining Act of 1995;
23. Violations of Section 27(c), (e), (f), (g) and (i), of Republic Act No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;
24. Violation of Section 7(b) of Republic Act No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act.
25. Violation of R.A. No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;
26. Violations of Sections 1, 3 and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives;
27. Violation of Presidential Decree No. 1612, otherwise known as the Anti-Fencing Law;
28. Violation of Section 6 of R.A. No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995;
29. Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;

30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;
31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;
32. Violations of Sections 5, 7, 8, 9, 10 (c), (d) and (e), 11, 12 and 14 of Republic Act. No. 7610, otherwise known as the Special Protection of Children against Abuse, Exploitation and Discrimination;
33. Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the Securities Regulation Code of 2000; and
34. Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

Reporting of suspicious transactions to the Anti-Money Laundering Council (AMLC) shall be the responsibility of the designated AML and CTF Compliance Officer.

Transactions which, in the judgment of branches/offices other than the maintaining branch, are deemed suspicious shall document and submit their findings to the branch maintaining the account for additional verification measures and/or reporting to the AMLC.

Cyber fraud cases require Suspicious Transaction Report (STR) because such cases are among the predicate offenses under the Anti-Money Laundering Act.

Cyber Fraud is a deliberate act of omission or commission by any person carried out using the Internet and/or other electronic channels, in order to communicate false or fraudulent representations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to FIs connected with the perpetrator. Examples of cyber fraud in the financial industry may include, but are not limited to the following: a) ATM skimming, b) Theft of credit card data, c) computer hacking, d) electronic identity theft and e) Phishing scams.

AMLC Resolution No. 61 dated 20 July 2016: - “Covered and Suspicious Transaction Report – Covered institutions shall report x x x”, the filing of an STR with the AMLC shall be done within five (5) working days from confirmed knowledge and approval by the designated AML and CTF Compliance Officer.

In the case of suspicious transactions (STR), the five working day period shall be reckoned from the determination of the suspicious nature of the transaction, which determination should be made not exceeding ten (10) calendar days from date of transactions.

However, if the transaction is in any way related to, or the person transacting is involved or connected to, an unlawful activity under Section 3 (i) or 4 of RA 9160, as amended, the 10-day period for determination shall be reckoned from the date the knowledge, or should have known, under the circumstances, the suspicious indicator.

18.1. Procedure in Filing Suspicious Transaction

Branch/ Support Unit

1. Investigate unusual transaction/s based on any of the trigger below or alerts/red flags
    a. Adverse News i.e. National, Local and Foreign
    b. Fraudulent Remittance
    c. AMLC Letter
    d. Court Orders (Freeze Order/Provisional Asset Preservation Order)
    e. Customer Complaint
    f. Presentation of fake KYC documents

g. Attempt to defraud the organization

2. Gather sufficient information and perform the following:

    a. Know-Your-Client (KYC) Verification

        i. Verify if all mandatory information were obtained.
        ii. Validate the information provided in Member Client Loan Application Form or Product Enrollment Form if consistent with the submitted valid IDs.
        iii. Check if Customer Risk Rating (CRR) is appropriate. If CRR is High Risk, must be reviewed and approved by a Senior Officer

            "Senior Officer" shall refer to the next higher authority of the approving officer (Area Managers, Sector Heads or Regional Heads and the MFI Strategic Head)
        iv. Assess deficiencies/lapses observed.
        v. Document observations and actions taken to address to issues.

3. Identification of Account with the organization

    a. Check the MAESTRO Polaris Core System to identify the member client accounts with the organization.

    b. Get the following account details:

        i. Customer Identification number
        ii. Date opened
        iii. Total Debits with date range
        iv. Total Credits with date range
        v. Outstanding Balance and Status (as of date)
        vi. Maintaining Branch

    c. Assess if total debits and credits indicated in the system are commensurate with the member client profile.

        Note: A year on year total debits and credits may be done to identify period/s of spikes.

    d. Document data/information gathered.

4. Analysis of Transactions

    a. Assess total debits and credits if consistent with the profile of member client.

        i. Identify in the generated summary of transactions that warrants further review.
        ii. For closer scrutiny, do a year on year total debits/credits to determine the period that needs to be prioritized for review.

5. Other Documents and Other Non-Documentary Verification

    a. Verify name vs Internal Negative File and Google for any adverse findings.

b. For Sole Proprietor and juridical persons, verify trade name with Department of Trade and Industry (DTI), Securities and Exchange Commission (SEC) and Bangko Sentral ng Pilipinas (BSP) list of Remittance Agents (RAs), if applicable.

c. Request verification from Account Officer or Insurance Officer, Program Manager and Area Manager as necessary.

i. Home and business address
ii. Business activities
iii. Business documents
iv. IDs presented

d. Conduct client visitation and document using the Call Report.

Note: Supporting documents to include but not limited to:
a. Know-Your-Client (KYC) documents
b. Enhance Due Diligence (EDD)
c. Statement of Account (SOA)
d. Other supporting documents, if any

6. Review completeness, accuracy of supporting documents and evaluate as follows:

a. Reason of suspicion/unusual transaction/s
b. Type of transaction/s that is/are unusual
c. Date and time the transaction occurred
d. Place where the unusual transaction occurred, if applicable
e. Details to describe the basis of suspicion
- Pattern of transaction
- Description of the information in the member client application form
- Nature of business
- Source of income
- Affiliations
- Red flags that triggered the investigation

7. Discuss, evaluate, deliberate and decide if “Filing or Not Filing of STR” for the reported transactions include the following details:

a. Trigger of the review
b. Account Name
c. Reason for Filing/Not Filing based on AMLC Portal
- Circumstances (SI1 to SI6)
- Predicate Crime (PC1 to P34)
d. Case Description
e. Amount of Debit/Credit with inclusive dates
f. Branch/Unit
g. Account Status
h. Customer Information
- Individual
  Account name, place and date of birth, nationality, address, contact number, source of fund, nature of business, type of account, account number, date opened, outstanding balance, status and maintaining branch/unit
- Juridical Persons

Account name, license, nature of business, address, contact number, source of fund/wealth, type of account, account number, date opened, outstanding balance, status and maintaining branch/unit, name of the authorized signatories, date and place of birth, address, source of fund, contact number, nationality, name of the beneficial owner, date and place of birth and address

i. Description of transaction and STR Narrative.
j. The reporting *organization must strictly comply with the new reporting requirements as per new AMLC regulatory issuance (A) No. 1 Series of 2018 re: Amendments to the AMLC Registration and Reporting Guidelines (ARRG), Section 4 – Revision of Data Elements, which provides that time of transaction will be included in the CTR/STR format, effective October 30, 2018.*

18.1.1. Fraud-Related Suspicious Transactions:

1. Suspicious transactions indicator must be fraud-related involving different member client that is related to:

   a. ATM Skimming/Cash Card Skimming;
   b. Mail order/Telephone order;
   c. Unauthorized withdrawals;
   d. Point of sale-debit; and
   e. Spurious Check

2. The designated AML and CTF Compliance Officer must file the STR which should conform with AMLC requirements. In the narrative field of the STR, the first line should contain the keyword “(no. of STRs)” and total amount, e.g. “6 STRs”, “total amount of 410,000.00”.

18.2 AML and CTF Compliance Officer Duties and Responsibilities

- Evaluate and endorse filing a Suspicious Transaction Report/s (STR).
- Provide a training program to branches on AML/CTF compliance awareness and give priority to high risk branches, if any to ensure effective implementation of the AML MTPP Program.
- Coordinate with branches and provide necessary information pertaining to any AMLC queries and guide the branch on the necessary actions to take pursuant to the advisory from the Legal Group;
- Coordinate with the branches to oversee its compliance with the AML law, rules and regulations, bank policies and procedures; and

19. AML Training and Countering of Terrorist Financing Training Program

It is the policy of the organization to ensure that all its directors, officers and employees are informed and adequately trained in matters covered by the Money Laundering and Terrorist Financing Prevention Program to enable them to fully comply with their obligations and responsibilities under the AMLA as amended, its Revised Implementing Rules and Regulations, TF Suppression Act and its Implementing Rules and Regulations - AMLC, Bangko Sentral ng Pilipinas, Security and Exchange Commission and Insurance Commission Circulars, Letters, Memoranda.

The MAESTRO Compliance Office in close coordination with the Human Resource Services Group is required to conduct Anti-Money Laundering (AML) training to all its Employees. Ongoing education of personnel is an important element in the compliance function to maintain a sound compliance program. The purpose of the training is to make all personnel aware of the Philippine AML laws and regulations

as well as the organization's policies and procedures that affect their areas of responsibilities. The number of AML trainings and frequency will depend on the business needs and priorities of the organization. All new hires must undergo compliance and AML awareness training prior assumptionof duties while existing employees are required to participate in refresher courses within a period of 24to 36 months. AML trainings shall be in the form of classroom trainings, e-learning modular workshops, branch / unit meetings, compliance reviews, home study and surveys.

19.1. Training Methods

MAESTRO Compliance Office and Human Resource Group shall roll out various AML trainings. The basic AML training module aims to achieve consistency in the level of understanding and compliance awareness across branches and business units.

For customized AML training, the objective is to ensure that staff members are familiar with the rules and regulations that are relevant to their job requirement. For branch operations, the training is focused on member client loan application opening, filing of suspicious transaction reports, periodic monitoring of accounts, enhanced due diligence on high risk accounts. For certain support units, the training focuses more on KYC for specific products and documentation required under AMLA law.

All newly hired employees are required to undergo Mandatory Compliance and AML Awareness Training for New Hires. The new employee may either attend the scheduled classroom training conducted by certified trainers or participate in the Compliance and AML Awareness Walkthrough Program. This must be complied by the new employee prior to assumption of duty but not to exceed six months from date of employment.

A Certificate of Attendance or Certificate of Completion signed by the designated AML and CTF Compliance Officer to the employee that must pass the written examination with a grade of at least 80%. For any employee that fail the written examination, the employee is required to undergo remedial classroom training or one-on-one training under the supervision of the designated AML and CTF Compliance Officer until the employee completes a written examination with the passing grade of 80%. Copy of the Certificate of Attendance or Certificate of Completion must be sent to the Human Resources for the 201 file.

19.2. Evaluation

Several tools are being used to evaluate the effectiveness of the training. They include:

1. Feedback Survey Form

   This evaluation form is used at the conclusion of the training. The objective of the survey is to gauge how the participants view training as a whole: the overall satisfaction of the training material contents, competence of the speaker, what they have learned and the relevance of the topic to their everyday working environment. This will provide Compliance Office the basis to determine whether the training program met the training objectives and the specific needs of a particular group.

2. Written Examination

   Each Participant is required to take a written examination to test the level of understanding. The examination consists of at least ten (10) questions of which the acceptable passing score is eighty (80%) or 8/10. The examination was developed to emphasize the basic principles of Anti-Money Laundering Act and recent circulars issued by Bangko Sentral ng Pilipinas, Securities and Exchange Commission, Insurance Commission and Anti-Money Laundering Council.

3. Certification

   The AMLA policies and procedures may require periodic AML certification process for a Branch or Business Support Unit to be submitted to the Compliance Office. The objective of the certification is to strengthen AML/CTF awareness among employees. The commitment of the organization is to provide AML training periodically for its employees to be updated of the legal, regulatory and policy requirements applicable to their job assignments, as each employee will be held accountable for carrying out his compliance responsibilities. All of the Directors and the employees must be well informed of the consequences of non-compliance which may lead to penalties and sanctions.

20. Screening and Recruitment Process of Personnel

Recruitment Process – Know Your Employee (KYE)

Selection, management and development of employees are line management functions. However, the overall responsibility for control and coordination of all recruitment and placement activities shall be exercised by the Human Resources Services Group by ensuring that a pool of qualified personnel who fit the requirements of the organization are readily available and by providing valuable assistance to line management in the effective selection, management and development of employees.

HR shall screen candidates for employment using valid and reliable measures and procedures. As a rule, HR shall screen candidates for organization-person fit, i.e., to determine overall suitability of the candidate to MAESTRO organizational culture and requirements.

As a matter of Policy, job openings shall be filled from within provided a qualified and suitable candidate is available.

Applicants shall be sourced outside the organization only if there are no qualified applicants from within and provided that the external candidates meet the qualifications required for the position and comply with the employment requirements.

The sources of external candidates for a particular position are the following: (a) “Walk-In" Applicants; (b) Applicants on "Active File"; (c) Placement Offices of Schools; (d) School Job Fairs; (e) Advertising and Public Job Posting; (f) Former Student Trainees; (g) Recruitment Agencies and Executive Search Consultants; (h) Next-of-Kin

A. General Qualification Requirements for Applicants

   The general qualification standards for applicants are as follows:

   1. For Staff Position

      Unless otherwise specified, an applicant must:

      a. be of legal age, provided that he meets the requirements of the vacant position;
      b. be a graduate of a vocational course or a graduate/holder of a Bachelor’s degree, preferably in Commerce, Business Administration, Economics, Accountancy, Computer Science, Social Work and other fields related to loans or financial products;

c. pass the General Intelligence Test and the Aptitude Test. Likewise, he must take the Personality Test to determine suitability for the position;
d. not charged with and/or convicted of any criminal offense;
e. not previously dismissed or convicted with prejudice by a former employer; and
f. not have obtained failing marks/grades in more than three (3) subjects.

2. For Officer Position

As for officer position, depending on its organizational needs, may recruit highly qualified applicants for immediate appointment to officer position. To qualify for appointment to an officer position, an applicant must:

a. be of legal age;
b. be fit and proper for the position he is being appointed to. In determining whether a person is fit and proper for a particular position, integrity/probity, education/training and possession of competencies relevant to the function such as knowledge and experience, skills and diligence; and
c. meet the other general qualification requirements mentioned above for staff position including the taking of exams for officer candidates.

B. Medical Examination and Drug Testing

HR shall advise the chosen candidate to undergo the required pre-employment medical/laboratory examinations in a designated private clinic. In no case shall an applicant be hired if he has not been declared physically fit to work by the physician of the designated private clinic or by the HMO doctor, as the case may be.

C. Pre-Employment Requirements

HR shall require the prospective new employee to submit all necessary pre-employment requirements as listed in the Pre-Employment Requirements Checklist, as follows:

a. NBI Clearance (original copy)
b. Previous Employer's Clearance (original copy), if applicable
c. Birth Certificate or Affidavit of Birth
d. Birth Certificate of Dependents
e. Marriage Contract/Certificate, if applicable
f. Diploma, Certificate of Graduation
g. Transcript of Records
h. CPA Rating/PRC Identification, if applicable
i. Tax Identification Number and 1905 received by BIR, if applicable
j. Social Security Membership Form (E1/E4) or SSS ID
k. SSS Employee Static Information - List of Contributions/Loan Information
l. Phil health – Member’s Data Record or MDR (with updated list of dependents)
m. Three (3) copies of 1"x1" size pictures (WHITE background)
n. W2 (BIR Form – Tax Withheld from Previous Employer) for the current year
o. Personal History Statement Form
p. Pag-ibig Membership ID/MDF
q. Medical and Dental Clearance

The employment application form, medical/dental and laboratory examination results, pre-employment requirements, appointment paper, including acknowledgement receipt of the MAESTRO Code of Conduct and other pertinent papers

shall be compiled to form part of the employee's 201 file which shall be maintained at HR.

Compliance with pre-employment requirements shall be a pre-condition for continued employment with MAESTRO, unless a specific item requirement is deferred.

D. Reference Check

The candidate shall be subjected to a discreet reference check and verification of records/information to be conducted by MAESTRO. For this purpose, the candidate mustsign and fully accomplish the Authorization Form authorizing MAESTRO to confirm/validate information, records, accounts or other data that the Bank may gather in connection with the applicant's employment with MAESTRO.

The discreet reference check shall cover checking on family and neighborhood background, verification of school records through the school Registrar's Office and performance in previous jobs, under conditions of utmost confidentiality. In-house checking with certain regulatory agencies shall also be conducted of any past due loans, improper handling of checking account, adverse loan account, cancelled credit card, loan dealings with other financial institutions, internal negative file and court cases.

E. Hiring Recommendation and Approval

After a particular candidate has been selected for hiring, the Head of Office or the Group Head, as the case may be, shall accomplish the applicable Hiring Recommendation and Approval Form which shall be routed for endorsement/approval of the following approving authorities in accordance with the Manual of Signing Authority.

F. Employee Orientation Program

The new hire shall be required to attend the Employee Orientation Program although officers may be required to report for work/assume duties on any working day of the month due to business exigencies. The Employee Orientation Program shall be conducted by HR for new hires of the Head Office and Metro Manila branches.

For new hires who will assume duties in provincial branches, who, due to distance/proximity, could not attend the aforementioned Employee Orientation Program, the Branch Manager or Head of Office concerned shall be tasked to give the new hire a similar briefing/lecture (i.e., personnel policies, house rules, etc.) by referring to the Code of Conduct, Employee Check List and Manuals (if applicable).

Thru the Employee Orientation Program, the organization is assured that new employees are fully oriented and have familiarized themselves on the various regulatory and internal policies particularly those that pertain to internal control measures.

G. Required Employment Forms/Documents

The new hire shall be required to fill-up and accomplish the following documents/forms in:

1. BIR Form (No. 1902 / No. 1905)
2. SSS Membership Form
3. Philhealth Member Registration Form (PMRF)

4. Pag-IBIG Member's Data Form
5. List of Beneficiaries Form (Insular Life Insurance, Inc.)
6. List of Beneficiaries Form (MBAI product)
7. Signature and Handwriting Specimen
8. Fingerprints Specimen and other biographical data
9. Issuance of ID for New Hires Form

H. Employment Contract and Letter of Introduction (LOI) for Staff and Appointment Letter for Officers

After the new hire for staff position orientation is completed and has complied with all the required documentation, HR shall issue an Employment Contract and a Letter of Introduction (LOI) for him to present to the Head of Office upon assumption of duties to his place of assignment. The LOI and the Employment Contract for new hires who will be assigned to provincial branches shall be sent thru the fastest means of delivery, together with the pertinent documents.

A newly hired officer need not be given a Letter of Introduction. Instead, HRG shall issue him the appropriate appointment letter.

21. Internal Audit System

21.1. Internal Audit Function

The internal audit function associated with money laundering and terrorist financing should be conducted by qualified personnel who are independent of the office being audited. It must have the support of the Board of Directors and Senior Management and have direct reporting line to the Board or to a board level Audit Committee.

21.2. Risk Based Work Program

Internal Audit Unit shall develop a AML Risk-Based Work Program for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms and policies and procedures related to customer identification process, suspicious transaction reporting and record keeping and retention, the effectiveness of the employee's execution of the controls, the adequacy and effectiveness of the compliance oversight and quality controls, and the effectiveness of the training as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. Audits should be properly scoped to evaluate the effectiveness of the program and should proactively follow up on their findings and recommendations.

21.3. Compliance Testing and Review

The Compliance Office may be tasked to conduct periodic review and assessment of a unit's compliance on applicable rules and regulations including anti-money laundering and terrorist financing rules and regulations as well as to test the appropriateness/reliability of existing processes and adequacy of controls to mitigate the risks.

Annually, the Compliance Office shall conduct an overall compliance and control environment including AML-CFT area to identify high risk areas to which unit/branch are most likely be exposed to money laundering and terrorist financing risk. If there is identified high risk unit/branch, Compliance Office may conduct compliance testing to determine additional AML/CTF mitigating controls required that must be implemented and submit compliance review results to the Board Audit and Compliance Committee.

21.4. Compliance Testing and Review Manual

Compliance Office shall develop a Compliance Testing & Review Manual which incorporates compliance review program for AML and CTF Framework and AML system.

The result of the overall assessment of the AML and CTF compliance review conducted by Compliance Office shall adopt a Certification Risk Rating.

5 components of AML Compliance Risk:

1. Board and Senior Management Oversight – reflects the efficiency and capability of the unit/entity to escalate to Board/Senior Management money laundering/terrorist financing issues and concerns as well as resolution of findings/exceptions noted by the internal/external auditors and regulators.

2. Policies and Procedures – reflects the unit's/entity's adequacy of AML/CFT policies and procedures vis-à-vis Philippine/host-country laws and regulations, adequacy of access to MTPP, AML and CTF Policy Guidelines.

3. Internal control and MIS – reflect adequacy and soundness of the monitoring and compliance testing conducted by the AML and CTF Compliance Officer to identify, measure, monitor and control money laundering risks as well as compliance with the Philippine AML laws and regulations.

4. Implementation – reflects the level of effectiveness in the implementation of the MTPP which include customer acceptance and identification, covered and suspicious transaction reporting, transaction monitoring, record-keeping and retention.

5. Training – reflects the level of awareness and understanding of Unit's/entity's personnel to AML laws, rules, regulations, policies and procedures.

22. Monitoring of all Deficiencies noted during the Audit and External Independent Reviews or Regulatory Body Examination

22.1. Internal Audit Examination Report

Internal Audit has the responsibility to follow-up and determine whether or not the auditee/s has taken steps to adequately, effectively and timely address the matters reported in the audit findings/recommendations. Internal Audit therefore monitors on a monthly basis the status of corrective actions implemented on outstanding/open issues/recommendations until fully resolved. However, the implementation of corrective actions in a timely manner is the shared and direct responsibility of line management including the Group Head.

22.2. Regulatory Body Regular and/or Special Examination

Compliance Monitoring of Report of Examination (ROE) Findings/Recommendations

Compliance Office shall monitor external audit findings and recommendations and the preventive corrective action plans taken by the business units to close all issues/comments. Results of which are reported to the President, Executive Director, Senior Management and to the Board Audit and Compliance Committee periodically.

All critical issues must be escalated to concerned Group Head of the business unit for immediate appropriate action. Initial findings and comments including resolutions,

corrective actions and commitment dates are presented to Senior Management, President, Executive Director and Board Audit and Compliance Committee.

22.3. External Auditor and Examination Report Compliance Monitoring

It is important to monitor timely release of the external auditor reports related to independent assessment of the AML practices of the companies.

Compliance Monitoring Open Items Report shall be prepared by the Compliance Office and provided to the President, Executive Director and concerned Group Head/s on a quarterly basis summarizing the closed issues/comments and highlighting the open items for appropriate action until all issues are closed. Recurring items and unresolved open items shall be reported to the Board Audit and Compliance Committee.

22.4. AML and CTF Compliance Review

AML Compliance Review of offices/units which were assessed at least "Needs Improvement" or "Less than Satisfactory" and below or "High Risk" by External Auditors and Internal Audit may be subjected to AML and CTF Compliance Review to support line management in addressing the risk and sustaining corrective actions.

The report of the review indicates the period when the review commenced and ended, period covered, objective, methodology, observations, recommendations, actions taken or to be taken and conclusion/overall assessment. A memo addressed to the Head of Office shall be prepared by the Compliance Office with copy to the Chief Audit Executive, Risk Officer, President, Executive Director and Senior Management. Moreover, an Open Item Tracking Report is prepared shall be submitted to the Board Audit and Compliance Committee periodically to effectively manage the actions being required from business and operating units/branches on findings or observations.

23. AML Compliance Certification Process

The Compliance Office shall develop the AML Compliance Certification patterned after the BSP-AML Risk Rating System (ARRS) issued on April 4, 2012 under BSP Memorandum No. M-2012-017 and intended to maintain a thorough understanding of the organization's level of AML compliance thru self-assessment.

Under a AML Compliance Certification, the organization shall undergo an AML and CFT self-assessment on the 5 components of AML Compliance Risk. The component factors are as follows:

1. Board and Senior Management Oversight – the rating reflects the efficiency and capability of the unit to escalate to Senior Management money laundering/terrorist financing issues and concerns as well as resolution of findings/exceptions noted by the internal/external auditors and regulators.
2. Policies and Procedures – the rating reflects line management adequacy of access to AML and CTF policies and procedures, MTPP and interim AMLCFT Policy Guidelines.
3. Internal Control and MIS – the rating reflects the adequacy and soundness of the monitoring and compliance testing and reviews to identify, measure, monitor and control money laundering risks as well as compliance with the AMLA, its IRR and rules and regulations issued by BSP, SEC and IC;
4. Implementation – the rating reflects the level of effectiveness in the implementation of the MTPP which include customer acceptance and identification, covered and suspicious transaction reporting, record-keeping and retention and updating of customer records, among others;
5. Training – the rating reflects the level of awareness and understanding of employees personnel to AML and CTF laws, rules, regulations, policies and procedures.

Composite rating is assigned based on a 1 to 4 numerical scale. The highest rating of 4 indicates the strongest risk management system and most effective operational practices that entail the least degree of supervision. The lowest rating of 1 on the other hand signifies the weakest risk management system and defective implementation which requires the highest degree of management concern

The Composite Ratings are defined as follows:

Overall Rating	Description
4	Sound. High level of effectiveness. All or mostly 4 with no sub-component rating less than 3
3	Adequately Sound. Acceptable level of effectiveness. All or mostly 3 but no sub-component rating of 2.
2	Vulnerable. Implementation needs improvement. All 2 and no sub-component rating of 1
1	Grossly inadequate. Poor implementation. All or mostly 1

24. Cooperation with Regulatory Bodies and Examination Teams

All officers and employees shall provide full cooperation and support during examination conducted by regulatory bodies and government agencies' examination teams (i.e., AMLC, SEC, IC).

25. Cooperation with the AMLC

Anti-Money Laundering Council Documentary Requirements for Individuals & Entities subject of a CTR and/or STR

The covered transaction report (CTR) and the suspicious transaction report (STR) files, if any, submitted to the AMLC may trigger the council to require presentation of customer KYC documents and copies of customer IDs. Upon receipt of the AMLC letter, Compliance Office and Legal Counsel shall forward the same to maintaining business unit concerned for the requested customer documents. Once completed, Compliance Office shall obtain legal clearance prior to submission to AMLC. Compliance Office shall ensure delivery of the letter with the required documents within the deadline set by AMLC.

26. Record Keeping and Retention Period

The organization shall develop a robust system of record keeping, retention and disposal. Under a Records Retention and Disposal Program, each branch or business unit follows a Records Retention and Disposal Schedule which contain the list of all the records/files being maintained by the branch or office unit.

The schedule shall prescribe the duration or retention period (e.g. number of years) each record/file is to be kept in a particular are (i.e. work area/file room or central storage) prior to each disposal or destruction.

Records/files maintained/stored in the work area or file room are orderly filed and arranged in filing cabinets or peerless boxes and under the custody of a duly designated Records Custodian who is responsible for the safekeeping, control and accounting of all records and files of the division. Records/files are kept in storage areas which are fire resistant, well ventilated, well-lighted and free from dampness.

26.1. Customer records and documents

26.1.1. Group Heads shall designate at least two (2) officers who will be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA as amended.

26.1.2. The designated two officers shall have the obligation to make the customer records and documents available without delay during regular or special examinations and/or AMLC requests for customer records.

Designation of Officers shall be:
Branches: Branch Head and 1 Officer
Business Units and Support Departments: Department Head and 1 Officer

26.1.3. Group Heads must ensure the designation in the safekeeping of records is reviewed and update periodically or least annually every 5th day of January.

26.2. Accounts reported as suspicious and/or subject of court action

DESIGNATED AML AND CTF COMPLIANCE OFFICER

26.2.1. Safe keeps in a vault all records related to accounts reported as suspicious and/or subject of court action as follows:

1. Duplicate copy of the Suspicious Transaction Report (STR)
2. Original copy of all transaction records to support the STR
3. Original copy of subject member account application forms, transaction forms including supporting documents
4. All other communications related to subject transactions received from Management, AMLC and the courts.

26.2.2. Provides back-up copies of said files on electronic form, the custody of which shall be in accordance with the implementing guidelines under the Recovery Program.

26.2.3. Undertakes necessary measures to ensure the confidentiality of such files.

26.2.4. Ensures that said files are retained and safe kept beyond the period stipulated by the AMLA Implementing Rules and Regulations until it is confirmed that the case has been finally resolved or terminated by the court.

26.2.5. Allows AMLC authorized officers and representatives full access to said records.

26.3. Guidelines on Digitization of Member Client Records

The organization shall develop and implement the Digitization Member Client Record Program. All member client records and transaction documents shall be digitized in compliance with the AMLC issued AMLC Regulatory Issuance A, B and C No. 2 Series of 2018.

The following procedures must be complied:

1. Branches shall:

a. Perform daily scanning of member client records on a per Client basis using CID number. The prescribe filename convention shall be as follows:

1111@AAAAA@MM-DD-YYYY@88888888

Where:

1111	-	represents the Branch Code
AAAAA	-	represents the Document Code
MM-DD-YYYY	-	represents the Transaction Date
@	-	represents field separator
88888888	-	represents the CID No.

This filename convention shall be adopted when scanning

b. Upload on or before 8:00 PM, the clear and complete scanned/digitized files to a newly created Document Archives Department (DAD) (FTP) folder. This process shall be subject of an automated process for scanned/digitized files.

2. DAD must check the clarity of the digitized customer files and transfer the same to each branch or business unit folder on a daily basis.

3. Information Technology Department must develop and install a program to auto-push the digitized customer records.

4. The responsible Group Head and designated Records Custodian shall approve the access of authorized officers to the digitized customer records.

27. Lead Implementor of the MTPP

The lead implementor of the MTPP is the Compliance Office.

Compliance Office

The Compliance Office shall appoint the designated AML and CTF Compliance Officer in the effective implementation of the MTPP. Compliance Office shall liaise and maintain good working relationship between the organization and regulators on AML matters.

This MTPP shall be regularly updated at least one every two (2) years to incorporate changes in AML policies and procedures, latest trends in money laundering and terrorist financing typologies and latest pertinent regulatory issuances. Any revision or update in the MTPP shall likewise be approved by the Board of Directors.

28. Program Owner

The owner of the Program is the Compliance Office. Any deviation request shall be reviewed, approved and endorsed by AML and CTF Compliance Officer including the presentation to the Board Audit and Compliance Committee for approval.

29. Effectivity

This MTPP shall take effect immediately upon approval of the Board.