ANTI-MONEY LAUNDERING COUNCIL

2018 IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 9160, OTHERWISE KNOWN AS THE ANTI-MONEY LAUNDERING ACT OF 2001, AS AMENDED

In accordance with Section 7(7) of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001", as amended (AMLA), the following rules and regulations are hereby promulgated:

CHAPTER I
GENERAL PROVISIONS

RULE 1 – PURPOSE, POLICIES AND PRINCIPLES

Section 1. Title and Purpose.

1.1. This set of rules and regulations shall be known as the "2018 Implementing Rules and Regulations" (IRR) of the AMLA.

1.2. This IRR was promulgated to provide the details of implementation of the AMLA, as well as to assist all covered persons, supervising authorities, law enforcement and other government agencies, and other stakeholders by prescribing the rules and regulations to combat money laundering, terrorism financing being a predicate offense to money laundering, and other associated unlawful activities.

Section 2. State Policies on AML/CTF.

The provisions of this IRR are in line with the following State Policies:

(a) To protect and preserve the integrity of the Philippine financial system, including the confidentiality of bank accounts.

(b) To ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity.

(c) To extend cooperation, consistent with Philippines' foreign policy, in transnational investigations and prosecutions of persons involved in money laundering activities wherever committed.

(d) To protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it; and to recognize it as inimical and dangerous to national security and the welfare of the people; and to make the financing of terrorism a crime against the Filipino people, against humanity and against the law of nations.

(e) To recognize and to adhere to international commitments to combat the financing of terrorism, specifically to the *International Convention for the Suppression of the Financing of Terrorism*, as well as other binding terrorism related resolutions of the United Nations Security Council, pursuant to Chapter 7 of the United Nations Charter.

(f) To reinforce the fight against terrorism by preventing and suppressing the commission of said offenses through freezing and forfeiture of property or funds while protecting human rights.

Section 3. Governing Principles.

The anti-money laundering/counter-terrorism financing (AML/CTF) regime of the Philippines shall be governed by the following principles:

(a) The AMLC, as the country's financial intelligence unit, is vested by law with independence to perform its mandate. It upholds the continuous development of a team of highly ethical and professional personnel and implements efficient processes in the delivery of its mandate.

(b) The AML/CTF laws, rules and regulations and other relevant issuances are implemented using a risk-based approach in a way that responds to the need to bring the financially excluded into the regulated financial sector, while at the same time maintaining effective safeguards and effective controls against money laundering/terrorism financing risks.

(c) A strong compliance culture, good governance and observance of high ethical standards in the conduct of business are good foundations for an effective AML/CTF regime. It will be developed and sustained through capacity building and deterrence of violations through imposition of appropriate, proportionate and dissuasive sanctions.

(d) A sound risk management system to identify, assess, mitigate, monitor, and control risks associated with money laundering/terrorism financing is essential.

(e) Timely and effective domestic and international cooperation and established coordination mechanism are critical in the investigation and prosecution of money laundering/terrorism financing and associated unlawful activities.

(f) The implementation of AML laws, rules and regulations shall conform to international AML/CTF standards and best practices.

(j) The observance of the constitutional requirements on due process, and injunction against *ex post* facto laws and bills of attainder.

RULE 2 – DEFINITION OF TERMS

Section 1. Definitions.

For purposes of this IRR, the following terms are hereby defined as follows:

(a) "**Account**" refers to a bank account, electronic money account, investment account, insurance policy, membership account, and other similar contract or service agreement, business or professional relationships between a covered person and its customers where funds or any monetary instrument of the latter are held by the former.

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

(c) "**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 IRR, the government agency shall be referred hereafter as the "AMLC", while the governing body shall be referred hereafter as the "Council".

(d) "**Appropriate Government Agency**" (AGA) refers to the Philippine Amusement and Gaming Corporation (PAGCOR), Cagayan Economic Zone Authority (CEZA), Aurora Pacific Economic Zone and Freeport Authority (APECO), or other government agency, as may be determined by law, which may authorize casinos to engage in gaming operations.

(e) "**Asset**" refers to a monetary instrument, property, or both.

(f) "**Asset Preservation Order**" (APO) refers to a provisional remedy aimed at preserving monetary instruments or properties in any way related to an unlawful activity or money laundering offense defined herein, during the pendency of civil forfeiture proceedings.

(g) "**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.

(h) "**Bangko Sentral ng Pilipinas**" (BSP) refers to the central bank of the Republic of the Philippines established pursuant to the provisions of the 1987 Constitution and Republic Act No. 7653.

(i) "**Bank Inquiry**" (BI) refers to a provisional remedy that allows the AMLC to examine or inquire into particular bank accounts or investment with a bank or non-bank financial institution, notwithstanding the provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, as amended; Republic Act No. 8791; and other bank secrecy laws.

(j) "**Bearer Negotiable Instruments**" (BNIs) refers to monetary instruments in bearer form such as, traveler's checks; negotiable instruments, including checks, promissory notes and money orders, that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; and incomplete instruments, including checks, promissory notes and money orders, signed, but with the payee's name omitted.

(k) *"***Bearer Shares***"* refers to negotiable instruments that accord ownership in a juridical person to the person who possesses the bearer share certificate.

(l) "**Beneficial Owner**" refers to any natural person who:

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

(2) Has ultimate effective control over a juridical person or legal arrangement; or

(3) Owns, at least, twenty percent (20%) shares, contributions or equity interest in a juridical person or legal arrangement.

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

(m) "**Beneficial Ownership Verification**" (BOV) is the process of taking reasonable measures to identify and verify the beneficial owner, including the determination of the true nature of the beneficial owner's capacities and duties vis-à-vis his agent, nominee or trustee.

(n) "**Beneficiary**" refers to:

(1) *General*: any person for whose benefit an account was created or transaction was made.

(2) *For trust agreements*: any person for whose benefit the trust has been created.

(3) *For life insurance or investment-linked insurance policies*: any person who will be paid the policy proceeds.

(4) *For wire transfers*: refers to a person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

(n) "**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.

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

(p) "**Casino**" refers to a business authorized by the appropriate government agency to engage in gaming operations.

(q) "**Casino Cash Transaction**" refers to transactions involving the receipt of cash by a casino paid by or on behalf of a customer; or transactions involving the payout of cash by a casino to a customer or to any person in his behalf.

(r) "**Civil Forfeiture**" (CF) refers to the non-conviction-based proceedings aimed at forfeiting, in favor of the government, monetary instruments or properties related to an unlawful activity or money laundering offense defined herein.

(s) "**Close Relationship/Associate**" refers to persons who are widely and publicly known, socially or professionally, to maintain a particularly close relationship with the PEP, and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

(t) "**Correspondent Banking**" refers to the provision of banking services by one bank, called the correspondent bank, to another bank, called the respondent bank.

(u) "**Company Service Provider**" (CSP) refers to a person engaged in the business of providing the following services for customers, who need to perform or offer a service

or activity, but are not capable of doing or do not want to do so directly due to financial or operational reasons, or business judgment:

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

(2) 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;

(3) providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other juridical person or legal arrangement; and

(4) acting as (or arranging for another person to act as) a nominee shareholder for another person.

(v) "**Cover Payment**" refers to a wire transfer that combines a payment message sent directly by the originating/ordering financial institution to the beneficiary financial institution with the routing of the funding instruction, called the cover, from the originating/ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

(w) "**Covered Transaction**" refers to:

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

(2) A transaction with or involving jewelry dealers, dealers in precious metals and dealers in precious stones in cash or other equivalent monetary instrument exceeding One Million pesos (Php1,000,000.00).

(3) A casino cash transaction exceeding Five Million Pesos (PHP5,000,000.00) or its equivalent in other currency.

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

(y) "**Cross-Border Wire Transfer**" refers to any wire transfer where the originating and/or beneficiary financial institutions are located in different countries. It shall also refer to any chain of wire transfers in which, at least, one of the financial institutions involved is located in a different country.

(z) "**Customer/Client**" refers to any person who keeps or maintains 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 trusts, investment and pension funds, insurance policies, and remittance transactions;

(5) Persons whose assets are managed by an asset manager;

(5) trustors/grantors/settlors of a trust; and

(6) Insurance policy holders, whether actual or prospective.

(aa) "**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.

(bb) "**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.

(cc) "**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.

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

(ee) "**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.

(ff) "**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.

(gg) "**Domestic Wire Transfer**" refers to any wire transfer where the originating and beneficiary financial institutions are located in the same country. It shall refer to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country.

(hh) "**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.

(ii) "**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.

(jj) "**Financial Intelligence**" refers to the gathering and analysis of information about the transactions and financial activities of persons of interest, to understand their nature and capabilities, and predict their future actions. It may also refer to intelligence information, which is the result of the analysis of the information gathered.

(kk) "**Financial Intelligence Unit**" (FIU) refers to the national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to ML/TF and associated unlawful activities, and for the dissemination of the results of that analysis.

(ll) "**Financial Investigation**" refers to an inquiry into the financial affairs of persons related to ML/TF and associated unlawful activity, with a view to:

(1) identifying the extent of criminal networks and/or the scale of criminality;

(2) identifying and tracing the proceeds and instrumentalities of crime, terrorism funds or any other assets that are, or may become, subject to forfeiture proceedings; and

(3) developing and/or gathering of evidence which can be used in litigation of cases.

(mm) "**Freeze Order**" (FO) refers to a provisional remedy aimed at blocking or restraining monetary instruments or properties in any way related to an unlawful activity, as herein defined, from being transacted, withdrawn, deposited, transferred, removed, converted, concealed, or otherwise moved or disposed without affecting the ownership thereof.

(nn) "**Gaming Operations**" refers to games of chance and variations thereof offered by casinos, and approved by the AGA under their enabling laws and other applicable issuances. It shall exclude:

(1) Traditional bingo operations authorized by the AGA;

(2) Lotteries and sweepstakes of the Philippine Charity Sweepstakes Office; and

(3) Such other games of chance and variations as may be declared exempt by the AGA based on the result of their risk assessment, in consultation with AMLC.

(oo) **"Identification and Verification of Agents"** (IVA) refers to the process of establishing and recording the true and full identity and existence of an agent, nominee, trustee or other authorized representatives who is acting as an account holder or transactor, and other person who is acting in behalf of a beneficial owner or principal, including verifying the validity of the authority of the agent, nominee, trustee, or authorized representative.

(pp) "**Identification Data**" refers to both the identification information and identification document, as herein defined.

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

(1) For Filipino citizens: Those issued by any of the following official authorities:

(a) PhilID;

(b) Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities; and

(c) Other identification documents that can be verified using reliable, independent source documents, data or information.

(2) For foreign nationals:

(a) PhilID, for resident aliens;

(b) Passport;

(c) Alien Certificate of Registration; and

(d) Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities.

(3) For Filipino students:

(a) PhilID;

(b) School ID signed by the school principal or head of the educational institution; and

(c) Birth Certificate issued by the Philippine Statistics Authority; and

(4) For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity.

(rr) "**Identification Information/Personal Information**" refers to the demographic data and biometric information of a natural person, or information about a juridical person or legal arrangement, from which the identity of a person is apparent or can be reasonably and directly ascertained by the person holding the information, or when put together with other information would directly and certainly identify a person.

(ss) "**Immediate Family Member**" refers to individuals related to the PEP within the second degree of consanguinity or affinity.

(tt) "**Independent Legal/Accounting Professional**" refers to lawyers/accountants working in a private firm or as a sole practitioner who, by way of business or occupation, provides purely legal or accounting services to their clients.

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

(vv) "**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.

(ww) "**Instrumentality**" refers to any monetary instrument or property used to finance, operate, and/or maintain an unlawful activity.

This definition is in relation to "monetary instrument or property related to unlawful activity".

(xx) "**Insurance Commission**" (IC) refers to the Philippines' regulator of the insurance and pre-need industries.

(yy) "**Intermediary Financial Institution**" refers to a financial institution in a serial payment or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

(zz) "**Internet-Based Casino**" refers to casinos in which persons participate by the use of remote communication facilities such as, but not limited to, internet, telephone, television, radio or any other kind of electronic or other technology for facilitating communication.

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

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

(ccc) "**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.

(ddd) "**Materially-linked Accounts**" refer to:

(1) All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;

(2) All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;

(3) All "In Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

(4) All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

(5) All accounts of juridical persons or legal arrangements that are owned, controlled or ultimately effectively controlled by the natural person whose accounts, monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control; and

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

(eee) "**Monetary Instrument**" refers, 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.

(fff) "**Monetary Instrument or Property Related to an Unlawful Activity**" refers to:

(1) All proceeds of an unlawful activity;

(2) All instrumentalities of an unlawful activity, including all moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds, and other similar items for the financing, operations, and maintenance of any unlawful activity;

(3) All monetary instruments or property, including monetary, financial or economic means, devices, accounts, documents, papers, items, objects or things, used in or having any relation to any unlawful activity or money laundering, regardless of the current owner or possessor, and circumstances of ownership or acquisition; and

(4) For purposes of freeze order and bank inquiry order: related and materially-linked accounts.

(ggg) "**Money Laundering**" (ML) refers to the crime defined under Section 4 of the AMLA.

(hhh) "**Money Laundering/Terrorism Financing Prevention Program**" (MTPP) refers to a covered person's comprehensive, risk-based, and written internal policies, controls 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.

(iii) "**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.

(jjj) "**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.

(kkk) "**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.

(lll) "**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".

(mmm) "**Offender**" refers to any person who commits a money laundering offense.

(nnn) "**Ongoing 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.

(ooo) "**Originating/Ordering Financial Institution**" refers to the financial institution, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

(ppp) "**Originator**" refers to the account holder who allows the wire transfer from that account or where there is no account, the person that places an order with the originating/ordering financial institution to perform a wire transfer.

(qqq) "**Other Government Agency**" (OGA) refers to a government agency that is not an SA, AGA or LEA.

(rrr) "**Parallel Financial Investigation**" refers to conducting a financial investigation or investigation into the ML/TF aspect of a case alongside, or in the context of, the investigation into the associated unlawful activity.

(sss) "**Payable-through Accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

(ttt) "**Person/Entity**" refers to any natural or juridical person.

(uuu) "**Philippine Identification Card**" (PhilID) refers to the non-transferrable identification card issued 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.

(vvv) "**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.

(www) "**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.

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

(yyy) "**Precious Metals**" refers to gold, silver, platinum, palladium, rhodium, ruthenium, iridium, and osmium at a level of purity of five hundred (500) parts per one thousand (1,000), singly or in any combination, and alloys of precious metals, solders, and plating chemicals, such as rhodium and palladium plating solutions, potassium gold cyanide containing at least sixty-eight and three-tenths percent (68.3%) gold, potassium silver cyanide containing at least sixty-eight percent (68%) silver and silver cyanide in salt solution containing at least fifty-four percent (54%) silver.

(zzz) "**Precious Stones**" refers to all gems and stones used in jewelry making, such as gemstones, jewels, and those substances that have market-recognized gem level of quality, beauty, and rarity, such as diamond, corundum (including rubies and sapphires), beryl (including emeralds and aquamarines), chrysoberyl, spinel, topaz, zircon, tourmaline, garnet, crystalline and cryptocrystalline quartz, olivine peridot, tanzanite, jadeite jade, nephrite jade, spodumene, feldspar, turquoise, lapis lazuli, opal and pearl.

(aaaa) "**Probable Cause**" refers to such facts and circumstances which would lead a reasonably discreet, prudent, or cautious man to believe that:

(1) any monetary instrument or property sought to be frozen, inquired into or preserved is in any way related to any unlawful activity and/or money laundering offense; or

(2) ML/TF has been committed and that the respondent is probably guilty thereof.

(bbbb) "**Proceeds**" refers to an amount derived or realized from any unlawful activity, as herein defined.

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

(1) Personal property, including proceeds derived therefrom, or traceable to any unlawful activity, as herein defined, such as, but not limited to:

(a) Cash;

(b) Jewelry, precious metals and stones, and other similar items;

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

(d) Perishable goods; and

(e) Vehicles, vessels, aircraft, or any other similar conveyance.

(2) Personal property, used as instrumentalities in the commission of any unlawful activity, as herein defined, such as:

(a) Computers, servers, and other electronic information and communication systems; and

(b) Any conveyance, including any vehicle, vessel, and aircraft.

(3) Real estate, improvements constructed or crops growing thereon, or any interest therein, standing upon the record of the registry of deeds or local government unit in the name of the party against whom the freeze order or asset preservation order is issued, or not appearing at all upon such records, or not belonging to the party against whom the freeze order or asset preservation order is issued and held by any other person, or standing on the records of the registry of deeds or local government unit in the name of any other person, but are:

(a) derived from, or traceable to, any unlawful activity; or

(b) used as an instrumentality in the commission of any unlawful activity, as herein defined.

(dddd) "**Purely Legal/Accounting Service**" refers to:

(1) Rendition of purely litigation, notarial, legal counseling, and/or other services that can only be undertaken by a lawyer, as a professional; or

(2) Rendition of purely accounting, auditing and/or other services that can only be undertaken by a certified public accountant, as a professional.

(eeee) "**Relationship**" refers to business or professional relationship between the covered person and its customer.

(ffff) "**Request for Information**" (RFI) refers to a request for information by FIUs, LEAs and OGAs, whether domestic or foreign, for intelligence or investigative purposes only.

(gggg) "**Realty Transaction**" refers to a real estate transaction involving an amount in excess of Five Hundred Thousand Pesos (PHP500,000.00).

(hhhh) "**Realty Transaction Report**" (RTR) refers to a report, including copies of the relevant documents, on a realty transaction, as herein defined, filed by the Land Registration Authority and all its Registry of Deeds, before the AMLC.

(iiii) "**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.

(jjjj) "**Related Account**" refers to an account, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry, regardless of the layer of accounts that the funds had passed through or transactions that they had undergone.

(kkkk) "**Risk**" refers to risk of loss arising from ML/TF activities.

(llll) "**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.

(mmmm) "**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.

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

(oooo) "**Serial Payment**" refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the

originating/ordering financial institution to the beneficiary financial institution, directly or through one or more intermediary financial institutions.

(pppp) "**Shell Bank**" refers to a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

(qqqq) "**Ship-Based Casino**" refers to casinos, the operation of which is undertaken on board a vessel, ship, boat or any other water-based craft wholly or partly intended for gambling.

(rrrr) "**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.

(ssss) "**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.

(tttt) "**Straight-through Processing**" refers to payment transactions that are conducted electronically without the need for manual intervention.

(uuuu) "**Strategic Analysis**" refers to the high-level macro analysis of data to decipher the underlying patterns and trends that would enable the AMLC to draw conclusions and develop long-term strategies for the prevention of ML/TF, and to provide input for policy formulation.

(vvvv) "**Substantial Evidence**" refers to such level of evidence which a reasonable mind might accept as adequate to justify or support a conclusion that a specific violation was committed.

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

(xxxx) "**Suspicious Circumstance**" refers to any of the following circumstances, the existence of which makes a transaction suspicious:

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

(2) the client is not properly identified;

(3) the amount involved is not commensurate with the business or financial capacity of the client;

(4) taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;

(5) any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;

(6) the transaction is in any way related to ML/TF or related unlawful activity 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, such as the relevant transactions in related and materially-linked accounts, as herein defined.

(yyyy) "**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.

(zzzz) "**Suspicious Transaction**" refers to a transaction, regardless of amount, where any of the suspicious circumstances, as herein defined, is determined, based on suspicion or, if available, reasonable grounds, to be existing.

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

(bbbbb) "**Tactical Analysis**" refers to the analysis of data directed towards the short-term development of investigative priorities and deployment of resources, which include the analysis of time, space, offender, victim, and *modus operandi* for individual high-profile crimes, repeat incidents, and crime patterns, with a specific focus on crime series.

(ccccc) "**Terrorism Financing**" (TF) refers to the crime defined under Sections 4 of the TFPSA.

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

(eeeee) "**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 of a covered person.

(fffff) **"Trustee"** refers to a person in whom confidence is reposed as regards property for the benefit of another person called the trustor/grantor/settlor.

(ggggg) "**Trustor/Grantor/Settlor**" refers to a person who establishes a trust, or who transfers ownership of his assets to a trustee by means of a trust deed or similar arrangement.

(hhhhh) "**Unique Transaction Reference Number**" refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

(iiiii) "**Virtual Asset**" refers to a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.

(jjjjj) "**Virtual Asset Provider**" refers to any person who, as a business, conducts one or more of the following activities or operations for or on behalf of another person:

(a) Exchange between virtual assets and fiat currencies;

(b) Exchange between one or more forms of virtual assets;

(c) Transfer (the conduct of a transaction on behalf of another person that moves a virtual asset from one one virtual asset address or account to another) of virtual assets;

(d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

(e) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

(kkkkk) "**Wire Transfer**" refers to any transaction carried out on behalf of an originator, through an originating/ordering financial institution, by electronic means, with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

RULE 3 – UNLAWFUL ACTIVITIES

Section 1. Unlawful Activities.

Unlawful activities refer to any act or omission, or series or combination thereof, involving or having direct relation, to the following:

(a) "Kidnapping for Ransom" under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;

(b) 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";

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

(d) "Plunder" under Republic Act No. 7080, as amended;

(e) "Robbery" and "Extortion" under Articles 294, 295, 296, 299, 300, 301 and 302 of the Revised Penal Code, as amended;

(f) "Jueteng" and "Masiao" punished as illegal gambling under Presidential Decree No. 1602;

(g) "Piracy on the High Seas" under the Revised Penal Code, as amended, and Presidential Decree No. 532:

(h) “Qualified Theft” under Article 310 of the Revised Penal Code, as amended;

(i) “Swindling” under Article 315 and “Other Forms of Swindling” under Article 316 of the Revised Penal Code, as amended:

(j) “Smuggling” under Republic Act No. 455, and Republic Act No. 1937, as amended, otherwise known as the “Tariff and Customs Code of the Philippines”;

(k) Violations under Republic Act No. 8792, otherwise known as the “Electronic Commerce Act of 2000”;

(l) “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;

(m) “Terrorism” and “Conspiracy to Commit Terrorism”, as defined and penalized under Sections 3 and 4 of Republic Act No. 9372;

(n) “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”;

(o) “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;

(p) “Frauds and Illegal Exactions and Transactions” under Articles 213, 214, 215 and 216 of the Revised Penal Code, as amended;

(q) “Malversation of Public Funds and Property” under Articles 217 and 222 of the Revised Penal Code, as amended;

(r) “Forgeries” and “Counterfeiting” under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code, as amended;

(s) Violations of Sections 4 to 6 of Republic Act No. 9208, otherwise known as the “Anti-Trafficking in Persons Act of 2003, as amended”;

(t) 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”;

(u) Violations of Sections 86 to 106 of Chapter IV of Republic Act No. 8550, otherwise known as the “Philippine Fisheries Code of 1998”;

(v) Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the “Philippine Mining Act of 1995”;

(w) 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”;

(x) Violations of Section 7(b) of Republic Act No. 9072, otherwise known as the “National Caves and Cave Resources Management Protection Act”;

(y) Violation of Republic Act No. 6539, otherwise known as the "Anti-Carnapping Act of 2002, as amended";

(z) Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree "Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives";

(aa) Violation of Presidential Decree No. 1612, otherwise known as the "Anti-Fencing Law";

(bb) Violation of Section 6 of Republic Act No. 8042, otherwise known as the "Migrant Workers and Overseas Filipinos Act of 1995, as amended";

(cc) Violation of Republic Act No. 8293, otherwise known as the "Intellectual Property Code of the Philippines, as amended";

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

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

(ff) 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";

(gg) Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the "Securities Regulation Code of 2000";

(hh) Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

Section 2. Same Conduct Approach.

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.

Section 3. Amendment and Repeal of Laws Prescribing the Details of the Unlawful Activities.

2.1. Any unlawful activity which law has been amended, by way of renaming, renumbering or rephrasing the relevant provisions thereof, shall continue to be an unlawful activity under the AMLA. *Provided*, that the material elements of the unlawful activity under the amendatory law remains the same with the amended law; or the unlawful activity, as defined under the amendatory law includes or is necessarily included in the unlawful activity under the amended law.

2.2. Any law repealing, superseding or replacing the law covering any unlawful activity defined herein, shall be construed as the continuation of the repealed, superseded or replaced law, which is the basis of the unlawful activity cited under the AMLA. *Provided*, that the new law provides the same elements as the unlawful activity under the repealed, superseded or replaced law.

RULE 4 – COVERED PERSONS

Section 1. Covered Persons.

The following are the covered persons under the AMLA:

(a) The following financial institutions:

(1) Persons supervised and/or regulated by BSP, including their subsidiaries and affiliates, which are also covered persons, supervised and/or regulated by the BSP such as:

(a) Banks;
(b) Quasi-banks;
(c) Trust entities
(d) Pawnshops;
(e) Non-stock savings and loan associations;
(f) Other Non-bank financial institutions which under special laws are subject to BSP supervision and/or regulation;
(g) Electronic money issuers; and
(h) Foreign exchange dealers, money changers, and remittance and transfer companies.

(2) Persons supervised or regulated by IC, such as:

(a) Insurance companies;
(b) Pre-need companies;
(c) Insurance agents;
(d) Insurance brokers;
(e) Professional reinsurers;
(f) Reinsurance brokers;
(g) Holding companies;
(h) Holding company systems;
(i) Mutual benefit associations; and
(j) All other persons and their subsidiaries and affiliates supervised or regulated by the IC.

(3) Persons supervised or regulated by SEC, such as:

(a) Securities dealers, brokers, salesmen, investment houses, and other similar persons managing securities or rendering services, such as investment agents, advisors, or consultants;

(b) mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities; and

(c) 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 SEC.

(b) The following DNFBPs:

(1) Jewelry dealers.

(2) Dealers in precious metals, and dealers in precious stones.

(3) Company service providers, which, as a business, provide any of the following services to third parties:

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

(b) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons;

(c) providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other juridical person or legal arrangement; and

(d) acting as (or arranging for another person to act as) a nominee shareholder for another person.

(4) 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, securities or other assets;

(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.

(5) Casinos, including internet-based casinos and ship-based casinos, with respect to their casino cash transactions related to their gaming operations.

The "Casino Implementing Rules and Regulations of Republic Act No. 10927" shall govern the implementation of the AMLA with regard to casinos, unless, otherwise indicated therein by the AMLC and the AGAs.

Section 2. Primary Duties of Covered Persons.

2.1. Covered persons shall, comply with all the requirements under the AMLA and TFPSA, their respective IRR, and other AMLC issuances. They shall have the duty to cooperate with the AMLC in the, discharge of the latter's mandate, and execution of its lawful orders and issuances, to protect their businesses or professions from being used in ML/TF activities.

2.2. The covered persons' board of directors, partners or sole proprietors shall be ultimately responsible for the covered persons' compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

Section 3. Market Entry.

3.1. *Licensing or Registration with SAs.*

Covered persons shall secure a license or registration with the appropriate SAs, if any, or the appropriate government agency before they shall operate, as required by the laws covering their operations.

3.2. *Registration with AMLC.*

All covered persons shall register with the AMLC. In line with this requirement, and consistent with their respective authorities, SAs, or other licensing or business registration authorities, shall prescribe registration with the AMLC as a requirement for continued licensing and/or operations of covered persons, and, when necessary, transacting with other covered persons.

3.3. *Prohibition against Shell Banks.*

No shell bank shall be allowed to operate or be established in the Philippines.

3.4. *Prevention of Criminals from Participating in the Affairs of Covered Persons.*

The AMLC and the SAs shall take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function, in covered persons.

CHAPTER II
SUPERVISION AND ENFORCEMENT

RULE 5 – ANTI-MONEY LAUNDERING COUNCIL

Section 1. The Government Instrumentality.

1.1. Implementing Agency.

The AMLC is the independent government instrumentality mandated to implement the AMLA and TFPSA.

1.2. Operational Independence.

The AMLC shall safeguard the integrity and independence of its operations, including its independent authority to do the following:

(a) Carrying out its functions freely and without delay, including making decisions to analyze, request and/or share specific information without, interference by, or the need to seek permission of, other agency or office;

(b) Making arrangements or engaging independently with SAs, LEAs and OGAs, or foreign jurisdictions on the exchange of information;

(c) Determining the appropriate organizational structure and the functions of the different operating units of the agency to properly discharge its mandate; and

(d) Obtaining and using the resources, consistent with existing laws and regulations, needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence.

1.3. Confidentiality and Security of Records and Premises.

The AMLC shall, ensure the confidentiality of its records and the security of its systems, and limit access to its premises to authorized persons. Except the Commission on Audit, or by order of a competent court, no agency or office shall audit or examine the operations and premises of the AMLC, without the consent of the Council or its duly authorized representative. The AMLC shall establish an identification, monitoring and/or control system for non-AMLC personnel who will be allowed access to its premises.

1.4. Budget.

The annual budget appropriated by Congress for the AMLC in the General Appropriations Act shall be used to defray capital outlays, as well as maintenance and operational expenses of the AMLC.

Section 2. The Council.

2.1. *Composition.*

The powers and functions of the AMLC shall be exercised by a Council composed of the following persons:

(a) Chairperson - Governor of the BSP;

(b) Member - Chairperson of the SEC; and

(c) Member - Commissioner of the IC.

2.2. *Acting Capacity.*

In case of absence, incapacity, resignation, expiration of term, retirement, or death of any member, the officer duly designated or authorized to discharge the functions of the Governor of the BSP, the Chairperson of the SEC, and the Commissioner of the IC, shall act in their stead in the Council.

2.3. *Presiding Officer.*

The Chairperson shall serve as the presiding officer in all Council meetings and deliberations. In his absence, the officer duly designated or authorized to discharge the functions of the Governor of the BSP shall serve as the Acting Chairman of the Council.

2.4. *Unity in All Actions.*

The Council shall act unanimously in the discharge of its functions.

2.5. *Frequency and Mode of Meetings.*

The Council shall hold its meetings at such frequency and mode as it may deem appropriate. The date, time and venue of Council meetings shall be agreed in advance.

2.6. *Documentation of Meetings.*

The AMLC shall maintain and preserve a complete record of the proceedings and deliberations of the Council, including the recordings and transcripts of the stenographic notes, either in their original, digital or electronic form.

Section 3. The Secretariat.

3.1. *Establishment of the AMLC Secretariat.*

The Council shall establish and organize the AMLC Secretariat to assist in the discharge of its functions. The Council shall, in accordance with its authority, determine and provide for such operating units and other offices of the AMLC as may be necessary and appropriate for the proper and efficient conduct of the operations and the accomplishment of the objectives of the AMLC. The functions and duties of such operating units and other offices shall be determined by the Council. *Provided*, that the determination of the appropriate number and rank of its personnel shall be subject to the approval of the BSP's Monetary Board.

3.2. *Qualifications.*

In organizing the Secretariat, the Council shall appoint from those who have served, continuously or cumulatively, for, at least, five (5) years either in the BSP, the SEC or the IC.

3.3. *Employment Status.*

All members of the Secretariat shall be considered full-time, permanent employees of the BSP. They shall be entitled to such benefits and subject to such rules and regulations as are applicable to BSP employees of similar rank. *Provided*, that to protect the independence of the AMLC and prevent the disruption of its operations, no member of the Secretariat shall be transferred, reassigned or otherwise removed from the AMLC without the prior approval of the Council.

Section 4. The Executive Director.

4.1. *Term of Office.*

The AMLC Secretariat shall be headed by an Executive Director who shall be appointed by the Council for a term of five (5) years.

4.2. *Qualifications.*

The Executive Director shall, at the time of appointment, have the following qualifications:

(a) Member in good standing of the Philippine Bar;

(b) At least, thirty-five (35) years of age;

(c) Have served, continuously or cumulatively, for, at least, five (5) years either at the BSP, the SEC or the IC; and

(d) Of good moral character, unquestionable integrity, and known probity.

3.3. *Employment Status.*

The Executive Director shall be considered a full-time, permanent employee of the BSP. He shall be entitled to such benefits and subject to such rules and regulations, as well as prohibitions, as are applicable to officers of similar rank in the BSP.

3.4. *Officer-in-Charge.*

In case of absence, or temporary incapacity or disability of the Executive Director, any next-in-rank lawyer of the AMLC that is duly designated in accordance with existing administrative procedure, shall act in his stead as Officer-in-Charge.

RULE 6
POWERS AND FUNCTIONS OF THE AMLC

Section 1. Powers and Functions.

A. Central AML/CTF Authority.

1.1. *AML/CTF Supervisor and Enforcer.*

1.1.1. The AMLC shall formulate and implement such measures as may be necessary and justified under the AMLA and TFPSA to counteract ML/TF, including, but not limited to, the following:

(a) Spearheading the conduct of national risk assessment and evaluation of existing legal and operational frameworks, and formulation of national strategies to counteract ML/TF;

(b) Formulation of policy directions for the AML/CTF regime of the Philippines;

(c) Promulgation of implementing rules and regulations of the AMLA and TFPSA, and circulars, orders, guidelines, and other AML/CTF issuances;

(d) Issuance of legal opinions and interpretations of the AMLA and TFPSA, and their respective IRR;

(e) Conduct of onsite and offsite examination or other forms of compliance checking mechanism on covered persons to determine their level and quality of compliance with, the AMLA and TFPSA, their respective IRR, and other AMLC issuances; and

(f) Analysis and use of intelligence information to detect, prevent and counteract ML/TF and associated unlawful activities.

1.1.2. The Council shall ensure that the provisions of the AMLA and TFPSA, their respective IRR, and other AMLC issuances are faithfully executed, and complied with by all public and private stakeholders.

1.2. *Lead Agency on AML/CTF Matters.*

1.2.1. The AMLC shall enlist the assistance of any branch, department, bureau, office, agency or instrumentality of the government, including government-owned and controlled corporations, in undertaking any and all AML/CTF operations, such as:

(a) formulation of national strategies for a concerted and holistic government effort to combat ML/TF;

(b) conduct of parallel financial investigation and prosecution as part of domestic cooperation and coordination;

(c) execution of requests for mutual legal assistance and other forms of international cooperation;

(d) conduct of national risk assessment and mutual evaluation; and

(e) conduct of capacity-building programs and information campaign.

1.2.2. Enlistment of assistance may include the use of personnel, facilities and resources of the enlisted party for the more resolute prevention, detection and investigation of ML/TF offenses and prosecution of offenders.

1.2.3. The AMLC may enlist the SAs to assist in checking compliance of covered persons under their respective jurisdictions on the requirements of the AMLA and TFPSA, their respective IRR, and other AMLC issuances, through monitoring, examination, inspection, audit, investigation, or such other fact-finding mechanism. Subject to the parameters set by the Council, the findings of the SAs shall be submitted to the AMLC for evaluation for possible sanctions against the covered persons, and their responsible directors, officers and employees, as may be warranted under the circumstances.

1.2.4. The AMLC may enlist the relevant SAs, LEAs and OGAs to assist the AMLC in investigation and other domestic coordination and cooperation efforts to counteract ML/TF.

1.3. *Authority to Resolve Administrative Cases.*

1.3.1. The AMLC shall, after due notice and hearing, impose administrative sanctions for the violation of the AMLA and TFPSA, their respective IRR, other AMLC issuances.

1.3.2. The “Rules on the Imposition of Administrative Sanctions under Republic Act No. 9160, as Amended” shall govern the administrative proceedings before the AMLC.

1.4. *International Cooperation Advocate.*

1.4.1. The AMLC shall receive and take action in respect of any request from foreign States for assistance in their own AML/CTF operations as provided in the AMLA.

1.4.2. The AMLC shall formulate clear and efficient processes for the timely prioritization and execution of requests for mutual legal assistance and international cooperation concerning ML/TF and the associated unlawful activities.

1.4.3. The AMLC shall ensure that its responsible unit for mutual legal assistance is provided with adequate financial, human and technical resources. The AMLC shall have in place processes to ensure that the staff in the said unit maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and appropriately skilled.

1.5. *AML/CTF Educator.*

1.5.1. The AMLC shall develop educational programs, carry out capacity-building activities or offer training opportunities, and conduct awareness campaign on the pernicious effects, the methods and techniques used, and the viable means of preventing ML/TF and associated unlawful activities, and the effective ways of investigating, prosecuting and punishing offenders.

1.5.1. The AMLC shall develop an AML/CTF training system for public and private stakeholders, especially for the financial intelligence, investigation and legal personnel, on the fundamentals of ML/TF, the AMLA and TFPSA, and all requisite knowledge, skills, and abilities to be able to discharge their functions effectively.

1.5.2. The AMLC shall develop a mechanism for accreditation of subject matter experts to assist in the continuing training program of covered persons, and their responsible directors, officers and employees.

B. Financial Intelligence Unit.

1.6. *National Center for Receipt and Analysis of CTRs and STRs.*

1.6.1. The AMLC shall require and receive CTRs and STRs from covered persons, in accordance with Rule 22 hereof.

1.6.2. The AMLC shall formulate guidelines and develop protocols necessary to require covered persons to submit relevant information, consistent with existing laws, as part of CTRs and STRs.

1.6.3. The AMLC shall, as may be allowed by law, access all relevant financial, administrative and law enforcement information for a holistic financial intelligence analysis of CTRs and STRs.

1.6.4. The AMLC shall conduct tactical analysis, which uses available and obtainable information to identify specific targets, to follow the trail of particular activities or transactions, and to determine the relationship between monetary instruments and properties, and ML/TF and associated unlawful activities.

1.6.5. The AMLC shall conduct strategic analysis, which uses available and obtainable information, including data that may be provided by SAs, LEAs and OGAs, to identify ML/TF-related trends and patterns.

1.6.6. The AMLC shall develop a mechanism to use CTRs and STRs to identify, in a timely manner, whether natural or juridical person, or legal arrangement hold or control accounts, and to identify assets, without prior notification to the owner or holder.

1.6.7. The AMLC shall establish or adopt a mechanism for, and/or formulate guidelines on, exchange and dissemination, whether spontaneously or upon request, of information and the results of its analysis, to LEAs, OGAs, foreign jurisdictions, covered persons, and relevant private entities; and shall use dedicated, secure and protected channels for dissemination.

1.6.8. The AMLC shall protect the confidentiality of CTRs and STRs by:

(a) having policies and procedures in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information;

(b) ensuring that AMLC personnel have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information; and

(c) ensuring that there is limited access to its facilities and information, including Information and Communication Technology equipment.

1.7. *National Center for Receipt and Analysis of RTRs.*

1.7.1. The AMLC shall require and receive RTRs from the Land Registration Authority and all its Registries of Deeds within fifteen (15) days from the date of registration of the transaction, in a form to be prescribed by the AMLC.

1.7.2. The AMLC may also require the Land Registration Authority and all its Registries of Deeds to submit copies of relevant documents of all real estate transactions.

1.7.3. The provisions of Rule 6, Section 1.6 hereof shall apply to RTRs.

C. ML/TF Investigator.

1.8. *Identity Verifier.*

2.8.1. The AMLC shall issue orders addressed to the appropriate SA or the covered person to determine the true identity of the owner of any monetary instrument or property:

(a) subject of CTR or STR;

(b) subject of request for assistance from a foreign State or jurisdiction; or

(c) believed by the Council, on the basis of substantial evidence, to be, in whole or in part, wherever located, representing, involving, or related to, directly or indirectly, in any manner or by any means, the proceeds of any unlawful activity.

1.8.2. SAs and covered persons shall have the following duties in relation to AMLC requests or orders for the production of records of identification information and IDs:

(a) Act on the requests or orders immediately upon receipt thereof;

(b) Submit within five (5) working days from receipt of the request or order from the AMLC certified true copies of the records of identification information and documents pertaining to account, transaction and/or person subject of the order; and

(c) Keep the confidentiality of the request or order, and ensure that the owner of any monetary instrument or property or other unauthorized personnel shall not be informed about the request or order, to prevent tipping-off.

1.9. *Financial Investigator.*

1.9.1. The AMLC shall investigate the following:

(a) Suspicious transactions and covered transactions deemed suspicious after investigation by the AMLC;

(b) ML/TF activities;

(c) Any property or funds that are in any way related to TF or acts of terrorism;

(d) Properties or funds of any person in relation to whom there is probable cause to believe that such person or persons are committing or attempting to commit or conspiring to commit, or participating in or facilitating terrorism and TF; and

(e) Other violations of the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

1.9.2. The AMLC shall conduct an *ex parte* inquiry or examination, in accordance with Rule 11 hereof, when investigating particular transactions in deposit or investment accounts with any banking institution.

1.9.3. The AMLC shall use its investigative powers, and other existing mechanism or arrangements, to identify, in a timely manner, whether natural or juridical person, or legal arrangement hold or control accounts, and to identify assets without prior notification to the owner or holder.

1.9.4. In the exercise of its investigative functions, the AMLC may:

(a) direct covered persons to produce information, documents and objects necessary to determine the true identity of persons subject of investigation;

(b) request responsible officers and employees of covered persons and relevant government agencies to give statements pertinent to the transaction, person or violation being investigated;

(c) request information, documents and objects from domestic government agencies; foreign states, including its FIUs, LEAs, and financial regulators; or the United Nations and other international organizations or entities. *Provided*, that request for transaction documents pertaining to specific deposits and investments in banks shall be subject to the provisions on Bank Inquiry under Rule 11 hereof;

(d) use all appropriate investigative techniques, allowed under existing laws, to obtain access to all information, documents and objects for investigative and prosecutorial purposes, including the formation of joint investigative teams to conduct cooperative investigations; and

(e) adopt measures to ensure the confidentiality of requests and timeliness of the response of covered persons.

D. Government Representative on ML/TF Cases.

1.10. *Initiator of Freeze Order Proceedings.*

1.10.1. The AMLC shall file with the Court of Appeals, *ex parte*, through the Office of the Solicitor General, a petition for the freezing of any monetary instrument or property that is in any way related to an unlawful activity, in accordance with Rule 10 hereof.

1.10.2. Notwithstanding the foregoing, the AMLC shall directly issue, in accordance with the TFPSA, an *ex parte* freeze order:

(a) against properties or funds that are in any way related to terrorism or TF;

(b) against properties or funds of any person, group of persons, terrorist organization, or association or group of persons, in relation to whom there is probable cause to believe that they are committing or attempting or conspiring to commit, or participating in or facilitating the commission of terrorism or TF; and

(c) with respect to property or funds of a designated organization, association, group or any individual to comply with binding terrorism-related Resolutions, including Resolution No. 1373, of the UN Security Council pursuant to Article 41 of the Charter of the UN.

1.11. *Initiator of Civil Forfeiture Proceedings.*

The AMLC shall institute civil forfeiture proceedings and all other remedial proceedings, through the Office of the Solicitor General, to confiscate all monetary instruments or properties related to ML/TF or associated unlawful activity, in accordance with Rule 12 hereof.

1.12. *Complainant in ML/TF cases.*

The AMLC shall file complaints with the Department of Justice (DOJ) or the Office of the Ombudsman for the prosecution of ML/TF and other criminal violations under the AMLA and TFPSA.

Section 2. Functions of the Executive Director.

The Executive Director shall be the chief executive officer of the AMLC, and shall perform the following functions as hereby delegated by the Council:

(a) to act, in such capacity and in accordance with the specific instructions from the Council, as the principal representative of the Council and of the AMLC, in all dealings with other agencies of the government and all other persons or entities, public or private, whether domestic or international;

(b) to prepare the agenda for the meetings of the Council, and submit for consideration of the Council policies and measures necessary to carry out the purposes and provisions of the AMLA and TFPSA;

(c) to supervise the execution and administration of policies and measures approved by the Council;

(d) to direct and supervise the operations and internal administration of the AMLC. The Executive Director may delegate certain of his administrative responsibilities to other officers or may assign specific tasks or responsibilities to any unit of the AMLC whenever he may deem fit or subject to such rules and regulations as the Council may prescribe;

(e) to sign administrative issuances "For the AMLC" on policies and measures already approved, and subject to conditions imposed, by the Council;

(e) to exercise functions that may be delegated by the Council under such guidelines it may determine, and such other functions that are incidental and necessary thereto.

RULE 7 – SUPERVISION AND COMPLIANCE CHECKING

Section 1. General Supervision.

1.1. The AMLC shall exercise general AML/CTF supervision over all covered persons to ensure faithful compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

1.2. The provisions applicable to SAs under Rule 7 hereof shall apply to AMLC's AML/CTF supervision over covered persons.

Section 2. Supervising Authorities.

2.1. Authority to Assist the AMLC in AML/CTF Supervision.

SAs shall assist the AMLC in supervising the implementation of the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

2.2. Functions of SAs on AML/CTF Compliance

In assisting the AMLC in the discharge of its mandate to implement the AMLA and TFPSA, their respective IRR, and other AMLC issuances, the SAs shall perform the following with regard to their respective jurisdiction:

(a) Conduct sectoral risk assessment to understand the risks across the different sectors or sub-sectors;

(b) Issue AML/CTF guidelines to guide covered persons on how to comply with their AML/CTF duties and responsibilities, and/or recommend to the AMLC regulations unique to a particular covered person, industry or profession;

(c) Supervise, assess and monitor compliance with AML/CTF requirements, through the conduct of AML/CTF inspection, examination, audit, or such other mechanism the SAs deem appropriate;

(d) Take necessary measures to prevent criminals or their associates from being professionally accredited; or holding or being the beneficial owner of a significant or controlling interest; or holding a management function in a covered person;

(e) Require the submission of necessary information and documentation on AML/CTF compliance;

(f) Take enforcement actions and other necessary measures to correct AML/CTF deficiencies;

(g) Escalate AML/CTF findings to the AMLC for possible administrative sanctions;

(h) Assess, monitor and conduct outreach programs on NPOs with regard to TF matters; and

(i) Take other measures necessary and justified in assisting the AMLC.

Section 3. Sectoral Risk Assessment.

SAs shall conduct sectoral or sub-sectoral risk assessment to facilitate the preparation for the national risk assessment, or as it may deem necessary to determine, understand, mitigate, and manage the risks on their respective jurisdiction.

Section 4. AML/CTF Guidelines.

4.1. *Issuance.*

The SAs shall, in coordination with the AMLC, issue and/or update their respective AML/CTF guidelines to complement the provisions of this IRR, in relation to the specific industry, product or operation of covered persons under their respective jurisdiction.

4.2. *Contents.*

The AML/CTF guidelines of SAs shall include, but not limited to, the following:

(a) Details, policies, and procedures in implementing the provisions on CDD, including instances where delayed verification and no face-to-face contact may be implemented, considering risk-based approach, financial inclusion, and sound risk management policies and procedures;

(b) Red flag indicators that engender a reasonable belief that an ML/TF offense or associated unlawful activity is about to be, is being, or has been committed;

(c) System/procedure of flagging and monitoring transactions that qualify as suspicious transactions or covered transactions;

(d) Guidelines on setting up of risk management systems, including policies on identification, assessment, management and mitigation of risks that may arise from the development of new products and new business practices, as well as new delivery mechanisms; and the use of new or developing technologies for both new and pre-existing products; and

(e) Rules on AML/CTF compliance checking, including access to pertinent records and information, and use of risk rating system.

4.3. *International Standards and Best Practices.*

SAs shall consider internationally-accepted standards and best practices in formulating their AML/CTF guidelines. *Provided*, that they are consistent with the provisions of the AMLA, TFPSA, their respective IRR, and other AMLC issuances.

Section 5. Risk-based AML/CTF Supervision.

5.1. *Supervision and Monitoring in General.*

The SAs shall, in accordance with law and its procedures, check compliance by covered persons with the provisions of the AMLA, TFPSA, their respective IRR, and other AMLC issuances using risk-based approach. SAs shall subject covered persons to:

(a) Supervision having regard to the ML/TF risks in their respective sector and in line with applicable AML/CTF standards, including the application of consolidated group supervision for AML/CTF purposes.

(b) Monitoring and ensuring compliance with national AML/CTF requirements.

5.2. *Supervision and Monitoring of DNFBPs.*

Supervision of DNFBPs shall be performed on a risk-sensitive basis, including:

(a) determining the frequency and intensity of AML/CTF supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and

(b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CTF internal controls, policies and procedures of DNFBPs.

5.3. *Frequency and Intensity of Compliance Checking*

The frequency and intensity of on-site and off-site AML/CTF monitoring, inspection, examination, or audit of covered persons or groups shall be determined based on:

(a) the risks and the policies, internal controls and procedures associated with the covered person or group, as identified by the SAs' assessment of the covered person's or group's risk profile;

(b) the risks present in the country; and

(c) the characteristics of the covered persons or groups, in particular the diversity and number of covered persons and the degree of discretion allowed to them under the risk-based approach.

5.4. *Review of Risk Profiles of Covered Persons or Groups*

The SAs shall review the assessment of the risk profile, including the risks of non-compliance, of a covered person or group periodically, and when there are major events or developments in the management and operations of the covered person or group.

5.5. *Escalation of AML/CTF Findings to the AMLC*

Subject to the parameters set by the AMLC, and agreed to by the SAs, considering the risks involved, the findings of the SAs shall be submitted to the AMLC for evaluation for possible administrative proceedings against the covered persons, and their responsible directors, officers and employees.

RULE 8 – INVESTIGATION AND LAW ENFORCEMENT

Section 1. Primary Investigator and Law Enforcer.

1.1. *AMLC Investigation.*

The AMLC shall investigate ML/TF offenses and other violations of the AMLA and TFPSA.

1.2. *Duty of Covered Persons to Cooperate in AMLC Investigations.*

Covered persons shall have the following duties in relation to AMLC investigations:

(a) Give the authorized personnel of the AMLC, full access to all information, documents or objects pertaining to the account, transaction and/or person subject of the investigation immediately upon receipt of the request or order;

(b) Submit within five (5) working days from receipt of the request or order from the AMLC, certified true copies of the documents pertaining to account, transaction and/or person subject of the investigation; and

(c) Keep the confidentiality of the investigation and ensure that the owner of any monetary instrument or property, or other unauthorized personnel, shall not be informed about the investigation, to prevent tipping off.

Section 2. Law Enforcement and Other Government Agencies.

2.1. *Authority to Assist the AMLC in Law Enforcement.*

The SAs, LEAs and OGAs investigating the unlawful activities defined herein shall assist the AMLC in enforcing the AMLA and TFPSA, their respective IRR, and other AMLC issuances, particularly on the aspect of investigation and prosecution.

2.2. *Roles of Government Agencies in AML/CTF Enforcement.*

In assisting the AMLC in the discharge of its mandate to implement the AMLA and TFPSA, their respective IRR, and other AMLC issuances, the SAs, LEAs and OGAs shall perform the following with regard to their respective jurisdiction:

(a) Ensure that ML/TF and associated unlawful activities are properly investigated, within the framework of national AML/CTF policies and the laws they are implementing.

(b) Pursue the investigation of any ML/TF offenses, whenever applicable, during a parallel financial investigation with the AMLC, or refer the case to the AMLC for financial investigation, regardless of where the unlawful activity occurred. *Provided*, that when the cases are referred to the AMLC, the LEAs and OGAs shall provide the necessary support in obtaining evidence for the AMLC to prosecute the financial aspects of the crime.

(c) Formulate their respective AML/CTF policies and procedures, in accordance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

(d) Establish a mechanism, or designate a unit in their respective agencies dedicated, in addressing AML/CTF matters, including cooperation and coordination with the AMLC.

2.3. *Investigative Powers of Specific Government Agencies.*

2.3.1 The relevant SAs, LEAs and OGAs conducting investigations of ML/TF and/or associated unlawful activities shall, in accordance with their respective charters or laws, obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This shall include powers to use compulsory measures for:

(a) the production of records held by financial institutions, DNFBPs and other natural or legal persons;

(b) the search of persons and premises;

(c) taking witness statements; and

(d) seizing and obtaining evidence.

2.3.2 The relevant SAs, LEAs and OGAs shall, in accordance with their respective charters or laws, use a wide range of investigative techniques for the investigation of ML/TF and/or associated unlawful activities.

2.3.3 The relevant SAs, LEAs and OGAs shall, in accordance with their respective charters or laws, adopt mechanisms:

(a) to identify, in a timely manner, whether natural or legal persons hold or control accounts; and

(b) to ensure that they have processes to identify assets without prior notification to the owner.

2.3.4 The relevant SAs, LEAs and OGAs conducting investigations of ML/TF and/or associated unlawful activities shall, in accordance with their respective charters or laws and existing agreement, be able to ask for all relevant information from the AMLC.

2.3. *Pursuing Forfeiture of Assets Related to Unlawful Activity.*

The LEAs and OGAs, in relation to their investigative authority, and in accordance with their respective charter or the relevant provisions of the Rules of Court, shall expeditiously identify, trace, attach, freeze and/or seize all monetary instrument or property related to unlawful activity defined herein, for purposes of forfeiture.

2.4. *Immediate Implementation of Freeze and Asset Preservation Orders.*

LEAs and OGAs shall immediately implement all freeze orders and asset preservation orders issued by the Court of Appeals and Regional Trial Courts, respectively, with regard to the monetary instruments or properties in their custody. They shall, likewise, comply with the required detailed returns for the said court orders, in accordance with Rule 10, Sections 4.4 and 4.5.

CHAPTER III
MONEY LAUNDERING, TERRORISM FINANCING AND ASSET FORFEITURE

RULE 9 – MONEY LAUNDERING AND TERRORISM FINANCING

Section 1. Money Laundering.

Money laundering is committed by:

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

(1) transacts said monetary instrument or property;

(2) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;

(3) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;

(4) attempts or conspires to commit ML offenses referred to in (1), (2), or (3) above;

(5) aids, abets, assists in, or counsels the commission of the ML offenses referred to in (1), (2), or (3) above; and

(6) performs or fails to perform any act as a result of which he facilitates the offense of ML referred to in items (1), (2), or (3) above.

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

Section 2. Predicate Offenses to Money Laundering.

All unlawful activities, as defined herein, are the predicate offenses to ML committed under Rule 9, Section 1(a) hereof.

Section 3. Jurisdiction over Money Laundering Cases.

3.1. *Regional Trial Court.*

The regional trial courts shall have jurisdiction to try ML cases committed by private individuals, and public officers not covered by the jurisdiction of the Sandiganbayan.

3.2. *Sandiganbayan.*

The Sandiganbayan shall have jurisdiction to try ML cases committed by public officers under its jurisdiction, and private persons who are in conspiracy with such public officers.

Section 4. Prosecution of Money Laundering Cases.

4.1. *Independent Proceedings.*

The prosecutions of ML and the associated unlawful activity shall proceed independently. Any person may be charged with and convicted of both ML and the associated unlawful activity.

4.2. *Separate and Distinct Elements.*

The elements of ML are separate and distinct from the elements of the associated unlawful activity. The elements of the unlawful activity, including the identity of the perpetrators and the details of the commission of the unlawful activity, need not be established by proof beyond reasonable doubt in the case for ML.

4.3. *Knowledge.*

The element of knowledge may be established by direct or circumstantial evidence. The deliberate non-performance of the preventive measures under the AMLA, this IRR, AMLC issuances, and SA's guidelines by a covered person's responsible directors, officers and employees shall be considered in determining knowledge of the commission of ML offenses.

4.4. *Rules of Procedure.*

The Rules of Court shall govern all proceedings concerning the prosecution of ML. The prosecution of ML and other violations of the AMLA shall be handled by the Department of Justice, through its public prosecutors, the Office of the Ombudsman, through the Office of the Special Prosecutor, pursuant to the Rules on Criminal Procedure.

4.5. *No ML Case During Election Period.*

No case for ML may be filed against a candidate for an electoral office during an election period.

Section 5. Terrorism Financing.

The provisions of the TFPSA and its IRR shall govern matters relating to TF, including the implementation of the relevant targeted financial sanctions.

RULE 10 – FREEZE ORDER

Section 1. General Rules on Freeze Orders.

The following requirements shall be observed in the issuance of freeze orders:

(a) No prior criminal charge, pendency of a case, or conviction for an unlawful activity or ML offense is necessary for the commencement or the resolution of a petition for freeze order.

(b) No asset shall be frozen to the prejudice of a candidate for an electoral office during an election period.

(c) No court shall issue a temporary restraining order or a writ of injunction against any freeze order, except the Supreme Court.

Section 2. Court-issued Freeze Order.

2.1. *Petition for Issuance of Freeze Order.*

By authority of the Council, the AMLC Secretariat shall file before the Court of Appeals, through the Office of the Solicitor General, an *Ex Parte* Petition for Issuance of Freeze Order.

2.2. *Related Accounts.*

Considering the intricate and diverse web of interlocking accounts that a person may create in different covered persons, and the high probability that these accounts are utilized to divert, move, conceal, and disguise the monetary instrument or property subject of the freeze order, the AMLC may include in its petition the freezing of related and materially-linked accounts.

2.3. *Rule of Procedure.*

Proceedings for the issuance of freeze order shall be governed by the "Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing of Monetary Instrument, Property, or Proceeds Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense under Republic Act No. 9160, as amended (A.M. No. 05-11-04-SC)" and other applicable rules that may be promulgated by the Supreme Court.

2.4. *Period to Resolve Petition.*

The Court of Appeals shall resolve the petition to freeze within twenty-four (24) hours from filing thereof.

2.5. *Issuance.*

Upon verified *ex parte* petition by the AMLC and after determination that probable cause exists that any monetary instrument or property is in any way related to an unlawful activity, the Court of Appeals may issue a freeze order, which shall be effective immediately, for a period of twenty (20) days, directing the concerned covered persons and government agencies to desist from allowing any transaction, withdrawal, deposit, transfer, removal, conversion, other movement, concealment, or other disposition of the subject monetary instrument or property.

2.6. *Coverage.*

The freeze order shall be limited only to the amount of cash or monetary instrument, or value of property that the Court of Appeals finds there is probable cause to be considered as proceeds of a predicate offense or otherwise related to an unlawful activity. The freeze order shall not apply to amounts in the same account in excess of the amount or value of the proceeds of the predicate offense or otherwise related to an unlawful activity.

2.7. *Summary Hearing and Extension.*

Before the expiration of the twenty (20)-day freeze order, the Court of Appeals shall conduct a summary hearing, with notice to the parties, to determine whether or not to modify or lift the freeze order, or to extend its effectivity. Pending resolution by the Court of Appeals, the freeze order shall remain effective.

2.8. *Effectivity of Freeze Order.*

The freeze order shall take effect immediately and shall remain effective for a total period not exceeding six (6) months. This is without prejudice to an asset preservation order that the regional trial court having jurisdiction over the appropriate AMLC case or civil forfeiture case may issue on the same account depending upon the circumstances of the case, where the Court of Appeals will remand the case and its records.

2.9. *Motion to Lift.*

(a) A person whose monetary instrument or property has been frozen may file a motion to lift the freeze order.

(b) If a freeze order is imposed on an account, including bank account, of a covered person that it uses for payment of salary, rent, suppliers, and/or taxes in the ordinary course of a legitimate business, the covered person may apply with the court which issued the freeze order to lift the same by submitting a bond or other acceptable securities of equal value to the amount or value subject of the freeze order. The bond or security when approved by the court shall secure the payment or enforcement of any order or judgment that the AMLC may recover in the appropriate action relating to the freeze order.

(c) The court must resolve the motion before the expiration of the freeze order.

2.10. *Lifting the Effects of the Freeze Order.*

(a) The freeze order shall be deemed *ipso facto* lifted after its expiration, unless an ML complaint against the person whose monetary instrument or property was frozen, or a petition for CF against the frozen monetary instrument or property, has been filed, in which

case the freeze order shall remain effective until the ML case is terminated or an asset preservation order is issued, respectively.

(b) Before the expiration of the freeze order, the covered person shall secure a written confirmation from the AMLC to ascertain if a petition for civil forfeiture or an ML complaint has been filed.

Section 3. AMLC-issued Freeze Order.

Freeze orders issued by the AMLC shall be governed by the TFPSA and its IRR.

Section 4. Duties of Covered Persons and Concerned Government Agencies.

4.1. *Implement Freeze Order.*

(a) Upon receipt of the notice of the freeze order, the covered person and government agency concerned shall immediately freeze the monetary instrument or property subject thereof, and shall immediately desist from and not allow any transaction, withdrawal, transfer, removal, conversion, other movement or concealment thereof.

(b) Interests earned during the effectivity of the freeze order shall be earned to the benefit of the frozen monetary instrument or property, and shall be considered as fruits of the said assets in cases the court grants the petition for civil forfeiture.

(c) Government agencies concerned, shall annotate the freeze order on the title of the property, as may be allowed under existing laws, or such other mechanism that would prevent any transaction, withdrawal, transfer, removal, conversion, other movement or concealment of the property subject of the freeze order.

4.2. *Freeze and Report Related Accounts.*

(a) Upon receipt of the freeze order that directs the freezing of related accounts, and upon verification by the covered person that there are accounts related to the monetary instrument or property subject of the freeze order, the covered person shall immediately freeze these related accounts wherever these may be found.

(b) If the related accounts cannot be determined within twenty-four (24) hours from receipt of the freeze order due to the volume and/or complexity of the transactions, or any other justifiable factors, the covered person shall effect the freezing of the related accounts within a reasonable period and shall submit a supplemental return thereof to the Court of Appeals and the AMLC within twenty-four (24) hours from the freezing of said related accounts.

(c) Relevant transactions of related accounts shall be reported to the AMLC as suspicious transactions.

4.3. *Furnish Copy of Freeze Order to Owner or Holder.*

(a) The covered person and government agency concerned shall immediately furnish a copy of the freeze order upon the owner or holder of the monetary instrument or property or related accounts subject thereof.

(b) The covered person and government agency concerned shall, likewise, immediately notify the owner or holder of a frozen related account on why the monetary instrument or property was considered as such, and furnish a copy of the freeze order, which was used as the basis for the freeze.

4.4. *Submit Detailed Return.*

(a) Within twenty-four (24) hours from receipt of the freeze order or freezing of the related account, the covered person and government agency concerned shall submit, by personal delivery, to the Court of Appeals and to the AMLC, a written detailed return on the freeze order.

(b) The covered person shall also submit to the AMLC, through the internet, an electronic detailed return in a format to be prescribed by the latter.

4.5. *Contents of the Detailed Return.*

The detailed return on the freeze order shall specify all the pertinent and relevant information, which shall include the following:

(a) *For covered persons and government agencies, whichever are applicable*:

(1) The names of the account holders, personal property owners or possessors, or real property owners or occupants;

(2) The value of the monetary instrument, property, or proceeds as of the time the assets were ordered frozen;

(3) All relevant information as to the status and nature of the monetary instrument, property, or proceeds;

(4) The date and time when the freeze order was served; and

(5) The basis for the identification as related accounts.

(b) *For covered persons*: The account numbers and/or description of the monetary instrument, property, or proceeds involved;

(c) *For concerned government agencies*:

(1) Certificates of title numbers of registered real property and the volumes and pages of the registration books of the Register of Deeds where the same are registered;

(2) Registration in the Primary Entry Book and corresponding Registration Book in the Register of Deeds for unregistered real property;

(3) Registration with the Register of Deeds of the enabling or master deed for a condominium project, declaration of restrictions relating to such condominium project, certificate of title conveying a condominium and notice of assessment upon any condominium;

(4) Tax declarations for improvements built on land owned by a different party, together with the annotation of the contract of lease on the title of the owner of the land as registered in the Register of Deeds;

(5) Certificates of registration for motor vehicles and heavy equipment indicating the engine numbers, chassis numbers and plate numbers;

(6) Certificates of numbers for seacraft;

(7) Registration certificates for aircraft; or

(8) Commercial invoices or notarial identification for personal property capable of manual delivery.

RULE 11 – BANK INQUIRY

Section 1. Bank Inquiry Order by the Court.

1.1. *Application for Issuance of Bank Inquiry Order.*

By authority of the Council, the AMLC Secretariat shall file before the Court of Appeals, through the Office of the Solicitor General, an *Ex Parte* Application for the Issuance of Bank Inquiry Order to examine or inquire into any particular deposit or investment account that is related an unlawful activity or ML offense.

1.2. *Inquiry Into or Examination of Related Accounts.*

A court order *ex parte* must be obtained before the AMLC can inquire into the related accounts. The procedure for the *ex parte* application for an order of inquiry into the principal account shall be the same for that of the related accounts.

1.3. *No Prior Criminal Charge, Pendency of a Case, or Conviction Necessary.*

No prior criminal charge, pendency of a case, or conviction for an unlawful activity or ML offense is necessary for the filing or the resolution of an application for issuance of bank inquiry order.

1.4. *Compliance with Article III, Sections 2 and 3 of the Constitution.*

The authority to inquire into or examine the main account and the related accounts shall comply with the requirements of Article III, Sections 2 and 3 of the 1987 Constitution.

1.5. *Period to Resolve Application.*

The Court of Appeals shall resolve the application within twenty-four (24) hours from filing thereof.

1.6. *Bank Inquiry Order.*

Notwithstanding the provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, as amended; Republic Act No. 8791, and other laws, the AMLC may inquire into or examine any

particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution, upon order by the Court of Appeals based on an *ex parte* application in cases of violation of the AMLA when it has been established that probable cause exists that the deposits or investments involved, including related accounts, are in any way related to an unlawful activity or ML offense.

Section 2. Bank Inquiry Order by the AMLC.

2.1. The AMLC shall issue an *ex parte* order authorizing the AMLC Secretariat to inquire into or examine any particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution and their subsidiaries and affiliates when it has been established that probable cause exists that the deposits or investments involved, including related accounts, are in any way related to any of the following unlawful activities:

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

(b) 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;

(c) Hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended;

(d) Felonies or offenses of a nature similar to those mentioned in Rule 11, Sections 2.1 (a), (b) and (c), which are punishable under the penal laws of other countries;

(e) Terrorism and conspiracy to commit terrorism as defined and penalized under Republic Act No. 9372; and

(f) Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of the TFPSA.

2.2. The relevant requirements for Bank Inquiry Order by the Court shall apply to Bank Inquiry Order by the AMLC, including the procedure for inquiry into related accounts.

Section 3. Duties of the Covered Persons.

Covered persons shall have the following duties in relation to bank inquiry orders:

(a) The concerned covered persons shall immediately, upon receipt of the court order or AMLC Resolution, give the AMLC and/or its Secretariat full access to all information, documents or objects pertaining to the deposit, investment, account and/or transaction.

(b) Certified true copies of the documents pertaining to deposit, investment, account and/or transaction subject of the bank inquiry shall be submitted to the AMLC Secretariat, within five (5) working days from receipt of the court order or notice of AMLC Resolution.

(c) Keep the confidentiality of the inquiry, and ensure that the owner of any monetary instrument or property or other unauthorized personnel shall not be informed about the inquiry, to prevent tipping-off.

Section 4. Bank Examination by the BSP.

4.1. In the course of a periodic or special examination of covered persons under its supervision and/or regulation, the BSP may inquire into or examine bank accounts, including customer identification, account opening, and transaction documents, for the purpose of checking compliance with the requirements of the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

4.2. The AML/CTF findings that fall within the parameters set by the AMLC shall be referred by the BSP to the AMLC for evaluation and filing of an administrative case, if warranted, against the covered person and its responsible directors, officers and employees.

RULE 12 – ASSET FORFEITURE

Section 1. General Rules on Asset Forfeiture.

The following rules shall be observed in asset forfeiture proceedings:

(a) No prior criminal charge, pendency of a case, or conviction for an unlawful activity or ML offense is necessary for the commencement or the resolution of a petition for civil forfeiture.

(b) No asset shall be attached or forfeited to the prejudice of a candidate for an electoral office during an election period.

Section 1. Civil Forfeiture.

1.1. *Petition for Civil Forfeiture.*

Upon determination that probable cause exists that any monetary instrument or property is in any way related to an unlawful activity or ML offense, the AMLC shall file with the regional trial court, through the Office of the Solicitor General, a verified petition for civil forfeiture.

1.2. *Equal Value Assets.*

The petition for civil forfeiture shall include other monetary instrument or property of equal value in cases where the monetary instrument or property that should be subject of forfeiture:

(a) cannot be located despite due diligence;

(b) has been substantially altered, destroyed, diminished in value or otherwise rendered worthless by any act or omission;

(c) has been concealed, removed, converted, or otherwise transferred;

(d) is located outside the Philippines or has been placed or brought outside the jurisdiction of the court; or

(e) has been commingled with other monetary instrument or property belonging to either the offender himself or a third person or entity, thereby rendering the same difficult to identify or be segregated for purposes of forfeiture.

1.3. *Rule of Procedure.*

Civil forfeiture proceedings shall be governed by the "Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing of Monetary Instrument, Property, or Proceeds Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense under Republic Act No. 9160, as Amended" (A.M. No. 05-11-04-SC).

1.4. *Asset Preservation Order.*

Upon verified petition by the AMLC, with prayer for issuance of asset preservation order, and after determination that probable cause exists that any monetary instrument or property is in any way related to an unlawful activity, the Regional Trial Court may issue an asset preservation order, in accordance with the "*Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing of Monetary Instrument, Property, or Proceeds Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense under Republic Act No. 9160, as Amended*" (A.M. No. 05-11-04-SC), which shall be effective immediately, forbidding any transaction, withdrawal, deposit, transfer, removal, conversion, concealment or other disposition of the subject monetary instrument or property.

1.5. *Motion to Discharge.*

(a) A person whose monetary instrument or property has been preserved may file a motion to discharge the asset preservation order.

(b) If an asset preservation order is imposed on an account of a covered person that it uses for payment of salary, rent, suppliers, and/or taxes in the ordinary course of a legitimate business, the covered person may apply with the court which issued the asset preservation order to discharge the same by submitting a bond or other acceptable securities of equal value to the amount or value subject of the asset preservation order. The bond or security when approved by the court shall secure the payment or enforcement of any order or judgment that the AMLC may recover in the appropriate action relating to the asset preservation order.

Section 2. Asset Forfeiture in ML Cases.

Where there is conviction for ML, the court shall issue a judgment of forfeiture in favor of the Government of the Philippines with respect to the monetary instrument or property found to be proceeds of or related to an unlawful activity.

Section 3. Claim on Forfeited Assets.

3.1. Where the court has issued an order of forfeiture of the monetary instrument or property in a criminal prosecution for any ML offense, the offender or any other person claiming an interest therein may apply, by verified petition, for a declaration that the same legitimately belongs to him and for segregation or exclusion of the monetary instrument or property corresponding thereto.

3.2. The verified petition shall be filed with the court which rendered the judgment of forfeiture, within fifteen (15) days from the date of the finality of the order of forfeiture, in default of which the said order shall become executory.

3.3. This provision shall also apply in civil forfeiture.

Section 4. Payment in Lieu of Forfeiture.

4.1. Where the court has issued an order of forfeiture of the monetary instrument or property subject of an ML offense, and said order cannot be enforced because:

(a) any particular monetary instrument or property cannot, with due diligence, be located;

(b) it has been substantially altered, destroyed, diminished in value or otherwise rendered worthless by any act or omission, directly or indirectly, attributable to the offender;

(c) it has been concealed, removed, converted, or otherwise transferred to prevent the same from being found or to avoid forfeiture thereof;

(d) it is located outside the Philippines or has been placed or brought outside the jurisdiction of the court; or

(e) it has been commingled with other monetary instruments or property belonging to either the offender himself or a third person or entity, thereby rendering the same difficult to identify or be segregated for purposes of forfeiture,

the court may, instead of enforcing the order of forfeiture of the monetary instrument or property or part thereof or interest therein, accordingly order the convicted offender to pay an amount equal to the value of said monetary instrument or property.

4.2. This provision shall apply in both civil and criminal forfeiture.

CHAPTER IV
NATIONAL RISK ASSESSMENT AND MANAGEMENT

RULE 13 – NATIONAL RISK ASSESSMENT

Section 1. Conduct of National Risk Assessment.

The AMLC, unless otherwise provided by law or the Office of the President, in coordination with all relevant SAs, LEAs and OGAs, covered persons, and other stakeholders, shall conduct a National Risk Assessment (NRA) to identify and assess the ML/TF risks of the Philippines.

Section 2. Frequency of Updating.

The NRA shall be updated, at least, once every three (3) years, or as often as the Council may deem necessary, depending on the level of risks found in the previous NRA or other relevant developments that may impact the Philippines AML/CTF regime.

Section 3. Publication and Dissemination.

The results of the NRA and all relevant AML/CTF risk assessments and strategies shall be published, posted in the website of the AMLC, and disseminated to relevant LEAs and OGAs. SAs shall assist the AMLC in disseminating the results of the NRA to covered persons.

RULE 14 – NATIONAL RISK MANAGEMENT

Section 1. Risk-based Approach to Risk Management.

Based on their understanding of their risks, the AMLC, SAs, LEAs and OGAs shall apply a risk-based approach to allocating resources and implementing measures to prevent or mitigate ML/TF.

Section 2. Policy on Exemptions to AML/CTF Requirements.

The SAs, upon approval of the AMLC, may allow certain exemptions to CDD and record-keeping requirements. *Provided*, that:

(a) there is proven low risk of ML/TF, the exemption occurs in strictly limited and justified circumstances, and it relates to a particular type of covered person or activity; or

(b) a financial activity, except money or value transfer services, is carried out by a natural or juridical person on an occasional or very limited basis, such that there is a low risk of ML/TF.

Section 3. Management of High-level Risks.

Where the AMLC or the SAs identify higher risks, they shall require covered persons to:

(a) take enhanced measures to manage and mitigate the risk; or

(b) ensure that these information are incorporated into their institutional risk assessment.

Section 4. Management of Low-level Risks.

The AMLC and the SAs may allow covered persons to take RDD measures; *Provided*, that lower risks have been identified, and this is consistent with the results of the NRA.

CHAPTER V
RISK ASSESSMENT AND MANAGEMENT BY COVERED PERSONS

RULE 15 – INSTITUTIONAL RISK ASSESSMENT AND MANAGEMENT

Section 1. Institutional Risk Assessment.

1.1. Covered persons shall take appropriate steps to identify, assess, and understand their ML/TF risks.

1.2. Covered persons shall perform the following activities when conducting institutional risk assessment:

(a) Document the risk assessments;

(b) Consider all the relevant risk factors before determining the level of overall risk and the appropriate mitigation measures to be applied;

(c) Keep these assessments up to date; and

(d) Establish appropriate mechanisms to provide the risk assessment results and any information related thereto to the AMLC and the SAs.

1.3. Covered person shall assess relevant risk factors, taking into consideration the results of the NRA, such as but not limited the following:

(a) Customers;

(b) Countries or geographic areas;

(c) Products and services; and

(d) Transactions and delivery channels.

1.4. Institutional risk assessment shall be conducted, at least, once every two (2) years, or as often as the board or senior management, SAs, or the Council may direct, depending of the level of risks found in the previous institutional risk assessment or other relevant AML/CTF developments that may impact the operations of covered persons.

Section 2. Institutional Risk Management.

2.1. The board of directors, partners or sole proprietor of the covered person shall exercise active control and supervision in the formulation and implementation of institutional risk management. They shall be ultimately responsible for the covered person's compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

2.2 Covered persons shall:

(a) develop sound risk management policies, controls and procedures, which are approved by the board of directors, partners or sole proprietor, to enable them to manage and mitigate the risks that have been identified in the NRA, or by the AMLC, SAs or the covered person itself;

(b) monitor the implementation of those controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

2.3. Covered persons may adopt RDD to manage and mitigate risks if lower risks have been identified. *Provided*, that the requirements of Rules 13 to 16 hereof are met. RDD is not allowed whenever there is a suspicion of ML/TF.

RULE 16 – MONEY LAUNDERING/TERRORISM FINANCING PREVENTION PROGRAM

Section 1. General MTPP Requirements.

Covered persons shall formulate and implement a comprehensive and risk-based MTPP that is compliant with the AMLA and TFPSA, their respective IRR, and other AMLC issuances, and the AML/CTF guidelines of SAs; and commensurate to the size and risk profile of the covered person. The covered person shall consider the results of the NRA and its own risk assessment in the development and/or updating of its MTPP. The MTPP shall be in writing and shall include, at the minimum, internal policies, controls and procedures on the following:

(a) Risk management;

(b) Compliance management setup, including the designation of a compliance officer at the management level or creation of compliance unit;

(c) Screening procedures to ensure high standards when hiring employees;

(d) Continuing education and training program;

(e) Independent audit function;

(f) Details of implementation of CDD, record-keeping and reporting requirements;

(g) Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC;

(h) Adequate safeguards on the confidentiality and use of information exchange, including safeguards to prevent tipping-off; and

(i) Cooperation with the AMLC and SAs.

Section 2. Compliance Management Structure.

2.1. Covered persons shall designate a compliance officer or create a compliance unit, who shall be responsible for the covered person's day-to-day compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances. In case the resources of the covered persons hamper the establishments of the compliance unit, the internal auditor, general manager or proprietor, as the case maybe, shall be the compliance officer.

2.2. The compliance officer or the head of the compliance unit shall be of senior management level. It shall have the support and a direct line of communication to the covered persons' Board of Directors, partners, or sole proprietor.

2.3. Covered persons with complex operations or multiple business locations, shall, taking into consideration the different risk factors, make and document its decision on the necessity of, creating a compliance unit, or appointing separate compliance officer for each of the covered persons' business locations.

2.4. Covered persons shall, as far as practicable, designate a separate records officer or create a records unit, who shall be responsible for the record-keeping requirements under the AMLA and this IRR. In case of sole proprietorships with no support employee or third party support staff, the proprietor shall be the records officer.

Section 3. Screening and Hiring of Employees.

3.1. Covered persons shall establish adequate screening procedures to ensure high standards when hiring employees.

3.2. Covered persons shall exercise due diligence in verifying that its employees were not involved in any ML/TF and associated unlawful activities, or were not found guilty of any serious, major or grave administrative offenses by the AMLC and/or the SAs, or convicted in any criminal case involving moral turpitude.

Section 4. Continuing Education and Training Program.

4.1. Covered persons shall develop, or create opportunities for, continuing education and training programs for its directors, officers and employees to promote AML/CTF awareness and strong compliance culture.

4.2. The education and training programs shall include relevant topics, such as:

(a) Overview on ML/TF, and the AMLA and TFPSA;

(b) Roles of directors, officers and employees in ML/TF prevention;

(c) Risk management;

(d) Preventive measures;

(e) Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC;

(f) Cooperation with the AMLC and the SAs; and

(g) International standards and best practices.

4.3. Attendance by covered persons' directors, officers and employees in all education and training programs, whether internally or externally organized, shall be documented. Copies of training certificates, attendance and materials, and shall be made available to the AMLC and the SAs, upon request.

4.4. Covered persons shall provide refresher programs, at least, every three (3) years. In cases where there are new developments brought about by new legislations, rules and regulations, and other AMLC issuances, covered persons shall immediately cascade these information to its responsible directors, officers and employees; *Provided*, that the cascading of the information is documented.

Section 5. Internal Audit.

5.1. Covered persons shall have an independent audit function commensurate with its size and risk profile.

5.2. Covered persons shall appoint an internal auditor or establish an internal audit unit that is independent from the personnel or unit to be audited. The internal auditor or internal audit unit shall be responsible for the periodic and comprehensive evaluation of the AML/CTF risk management framework.

5.3. The internal auditor or internal audit unit shall have the support and a direct line of reporting to the covered persons' Board of Directors, partners, or sole proprietor.

5.4. Covered persons shall develop their respective internal audit program, which shall include the audit scope. The audit scope shall include the review or evaluation of specific areas, such as but not limited to:

(a) Risk management framework;

(b) Compliance with the AMLA and TFPSA, their respective IRR, and other issuances by the AMLC and other SAs.

(c) Adequacy and effectiveness of the MTPP

5.5. Internal audits shall be conducted on a regular basis, commensurate with the size and risk profile of the covered person.

5.6. The results of the internal audit shall be timely and directly reported to the covered persons' Board of Directors, partners, or sole proprietor, copy furnished the compliance officer. The covered person shall establish a mechanism to promptly address and monitor noted weaknesses or findings in the internal audit report. Internal audit reports shall be made available to the AMLC and the SAs, upon request.

Section 6. Approval and Implementation.

6.1. The board of directors, partners or sole proprietors of the covered person shall approve, and exercise active oversight in the implementation of the MTPP. The compliance officer shall be the lead implementor of the MTPP.

6.2. Covered persons shall make the MTPP readily available in user-friendly form, and disseminated to all officers and staff who are responsible in implementing the same. Covered persons shall ensure that there is an audit trail evidencing the dissemination of the MTPP to all concerned officers and staff.

6.3. Where covered persons operate at multiple locations in the Philippines, it shall adopt an institution-wide MTPP to be implemented in a consolidated manner.

Section 7. Group-wide MTPP.

Financial and DNFBP groups shall implement group-wide MTPP, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial and professional group. These shall include the measures set out in Rule 16, Section 1.1, and also:

(a) policies and procedures for sharing information required for the purposes of CDD and risk management;

(b) the provision, at group-level compliance, audit, and/or AML/CTF functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CTF purposes. This should include information and analysis of transactions or activities which appear unusual, if such analysis was done. Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and

(c) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Section 8. Foreign Branches and Subsidiaries.

8.1. Covered persons shall ensure that their foreign branches and majority-owned subsidiaries apply the AML/CTF measures consistent with the AMLA and TFPSA, their respective IRR, and other AMLC issuances, where the minimum AML/CTF requirements of the host country are less strict, to the extent that the laws and regulations of the host country permit.

8.2. If the host country does not permit the proper implementation of the measures under the AMLA and TFPSA, their respective IRR, and other AMLC issuances, covered persons shall apply appropriate additional measures to manage the ML/TF risks, and inform their respective SAs and the AMLC.

Section 9. Inspection/Review of MTPP.

Covered persons shall, upon request, make available its MTPP to the AMLC and SAs, for inspection/review.

Section 10. Updating.

The MTPP shall be updated, at least, once every two (2) years or whenever necessary to reflect changes in AML/CTF obligations, ML/TF trends, detection techniques, and typologies.

CHAPTER VI
PREVENTIVE MEASURES

RULE 17 – PROHIBITED ACCOUNTS

Section 1. Anonymous Accounts and Accounts under Fictitious Names.

1.1. Covered persons shall maintain customers' account only in the true and full name of the account owner or holder.

1.2. Anonymous accounts, accounts under fictitious names, and all other similar accounts shall be absolutely prohibited.

Section 2. Numbered Accounts.

2.1. Numbered accounts, except non-checking numbered accounts, shall not be allowed.

2.2. CTRs and STRs involving non-checking numbered accounts shall contain the true name of the account holder.

Section 3. Annual Testing to Determine True Identity of Accounts.

The SAs may conduct annual testing for the sole purpose of determining the existence and true identity of the foregoing accounts, if any.

RULE 18 – CUSTOMER DUE DILIGENCE

Section 1. Purpose and Applicability of CDD.

1.1. *Purpose of CDD.*

Covered persons shall conduct CDD for the following purposes:

(a) To identify the customer, and its agents and beneficial owners;

(b) To determine the risk posed by each customer;

(c) To establish, maintain, close or terminate the account or business relationship; and

(d) To assess the level of monitoring to be applied.

1.2. *When is CDD Required.*

Covered persons shall undertake CDD measures when:

(a) establishing business or professional relationship;

(b) carrying out occasional transactions above (Php 100,000.00) or any other threshold as may be be determined by the relevant SAs, with notice to the Council, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

(c) carrying out occasional wire transfers in the circumstances under Rule 19, Section 6 hereof;

(d) there is a suspicion of ML/TF, regardless of any exemptions or thresholds that are referred to elsewhere under this IRR; or

(e) the covered person has doubts about the veracity or adequacy of previously obtained identification information and/or data.

1.3. *Existing Customers.*

Covered persons shall apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of information and document obtained.

Section 2. Customer Due Diligence Measures.

2.1. Covered persons shall conduct the appropriate CDD measures, which include the following procedures:

(a) Customer Identification Process;

(b) Customer Verification Process;

(c) Identification and Verification of Agents;

(d) Beneficial Ownership Verification;

(e) Determination of the Purpose of Relationship; and

(f) Ongoing Monitoring Process;

2.2. *Timing of CDD Measures.*

The foregoing CDD measures may be conducted simultaneously, consecutively, or at such timing and frequency as the covered person may determine to be appropriate, depending on the risks involved, unless otherwise provided in this IRR.

2.3. *Average Due Diligence.*

The requirements set forth in this IRR are for Average Due Diligence (ADD), unless otherwise stated or allowed to be RDD or EDD.

2.4. *Customer Acceptance Policies.*

Covered persons shall have clear, written and graduated customer acceptance policies and procedures that will seek to prevent suspicious individuals or entities from transacting with, or establishing or maintaining business relationship with them. Covered persons shall develop guidelines to assist their responsible officers in assessing whether a customer's profile warrants acceptance or refusal of service to protect the security and integrity of the business.

Section 3. Customer Identification Process.

3.1. General Requirement for CIP.

Covered persons shall identify and record the true identity of their customers, whether permanent or occasional, and whether natural or juridical person, or legal arrangement.

3.2. First Time Transactions

Customers who engage in a transaction with a covered person for the first time shall be required to present the original and submit a clear copy of, at least, one (1) ID as herein defined. In case the ID presented does not bear any photo of the customer, or the photo-bearing ID or a copy thereof does not clearly show the face of the customer, a covered person may utilize ICT or any other technology to take the photo of the customer.

3.3 System for Collection and Recording of Data

Covered persons shall implement appropriate systems of collecting and recording identification information and ID, such as:

(a) Photocopying/scanning of the ID presented;

(b) Using ICT to capture and record the demographic data and/or biometric information of customers; and/or

(c) Manual recording of identification information.

3.4 Required Identification Data from Natural Persons.

For customers who are natural persons, covered persons shall gather the following identification information and ID before or during account opening or onboarding:

(a) Identification Information:

(1) Full name;

(2) Date of birth;

(3) Place of birth;

(4) Sex;

(5) Citizenship or nationality;

(6) Address;

(7) Contact number or information, if any;

(8) Specimen signatures or biometric information;

(b) Identification Documents:

(1) PhilID; or

(2) Other identification document, as herein defined.

3.5 Required Identification Data from Juridical Persons.

For customers that are juridical persons, covered persons shall gather the following identification information and IDs before or during account opening or onboarding:

(a) Identification Information:

(1) Full name;

(2) Name of authorized representative/transactor/signer;

(3) Current office address;

(4) Contact number or information, if any;

(5) Nature of business; and

(6) Specimen signatures or biometric information of the authorized representative/transactor/signer.

(b) Identification Documents:

(1) Certificates of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation or Partnership issued by the SEC for corporations and partnerships, respectively, and by the BSP for money changers/foreign exchange dealers and remittance agents, and by the AMLC for covered persons.

(2) Articles of Incorporation/Partnership;

(3) Registration Data Sheet/Latest General Information Sheet;

(4) Secretary's Certificate citing the pertinent portion of the Board or Partners' Resolution authorizing the signatory to sign on behalf of the entity; and

(5) For entities registered outside of the Philippines, similar documents and/or information duly authenticated by a senior officer of the covered person assigned in the country of registration; in the absence of said officer, the documents shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

3.6 Required Identification Data from Legal Arrangements.

For customers that are legal arrangements, Rule 24 shall apply, in addition to the requirements for juridical persons, as applicable.

3.7 Sufficiency of PSN or PhilID in Proving Identity.

Notwithstanding the foregoing, covered persons shall deem the provision and submission of the PSN or PhilID as official and sufficient proof of identity, subject to the authentication requirements under the PhilSys Act and its IRR.

Section 4. Customer Verification Process.

4.1. *General Requirement for CVP.*

Covered persons shall implement and maintain a system of verifying the true identity of their clients, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data, or information.

4.2. *CVP for Juridical Persons and Legal Arrangements.*

For customers that are juridical persons or legal arrangements, covered persons shall maintain a system of understanding the nature of the customer's business or profession, and ownership and control structure, as well as the authority and identification of all persons purporting to act on their behalf. They shall verify the customer's identity through the following information :

(a) name, legal form and proof of existence;

(b) the powers and other legal requirements or contracts that regulate and bind the juridical person or legal arrangement, as well as the names of the relevant persons having a senior management position or perform significant responsibilities in the juridical person or legal arrangement; and

(c) the address of the registered office and, if different, a principal place of business.

4.3. *Timing of CVP.*

Covered persons shall verify the identity of the customer before or during the course of establishing a business or professional relationship, or conducting transactions for occasional customers. They may complete the verification process after the establishment of the business or professional relationship; *Provided*, that:

(a) completion occurs as soon as reasonably practicable;

(b) deferred CVP is essential so as not to interrupt the normal conduct of business; and

(c) the ML/TF risks are effectively managed, taking into consideration risk and materiality.

4.4. *Transacting or Using the Relationship Prior to CVP.*

Covered persons shall adopt risk management procedures concerning the conditions under which a customer may utilize the business or professional relationship prior to verification.

4.5. *Modes of CVP.*

Covered persons shall independently verify the collected data during CIP, through any of the following:

(a) face-to-face contact;

(b) use of ICT;

(c) by confirming the authenticity of the identification documents to the issuing office;

(d) reliance on third parties and service providers; or

(e) such other methods of validation based on reliable and independent sources, documents, data, or information.

Section 5. Identification and Verification of Agents.

5.1. *General Requirement for IVA.*

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

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

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

Section 6. Beneficial Ownership Verification.

6.1. *General Requirement for BOV.*

Covered persons shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable sources, such that the covered person is satisfied that it knows who the beneficial owner is.

6.2. *Document Evidencing Relationship.*

Covered persons shall determine the true nature of the beneficial owner's capacities and duties vis-à-vis his agent by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of CDD to be applied to both.

6.3. *Timing of BOV.*

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

(a) this occurs as soon as reasonably practicable;

(b) this is essential not to interrupt the normal conduct of business; and

(c) the ML/TF risks are effectively managed.

6.4. *BOV for Juridical Persons.*

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

(a) the identity of the natural persons, if any, who ultimately have controlling ownership interest in a juridical person;

(b) to the extent that there is a doubt under item (a) above, as to whether the persons with the controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural persons, if any, exercising control over the juridical person through other means; and

(c) where no natural person is identified under items (a) and (b) above, the identity of the relevant natural persons who hold senior management positions.

6.5. *BOV for Legal Arrangements.*

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

(a) *For trust agreements*: the identity of the trustors/grantors/settlors, the trustees, the beneficiaries or class of beneficiaries, the protector, if any, and any other natural person exercising ultimate effective control over the trust agreement.

(b) *For beneficiaries of trust agreements that are designated by characteristics or by class*: sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

(c) *For other types of legal arrangements*: the identity of persons in equivalent or similar positions.

6.6. *Guidelines on Beneficial Ownership.*

The AMLC shall formulate guidelines on the detailed implementation of the requirements on BOV.

Section 7. Determination of the Purpose of Relationship.

Covered persons shall understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business or professional relationship with their customers.

Section 8. Ongoing Monitoring Process.

8.1. *General Requirement for OMP.*

Covered persons shall, on the basis of materiality and risk, conduct ongoing monitoring by establishing a system that will enable them to understand the normal and reasonable account or business activity of customers, and scrutinize transactions undertaken throughout the course of the business or professional relationship to ensure that the customers' accounts, including transactions being conducted, are consistent with the covered person's knowledge of its customer, their business and risk profile, including where necessary, the source of funds.

8.2. *EDD After Conduct of OMP .*

Covered persons shall apply EDD on the customer if it acquires information in the course of its customer account or transaction monitoring that:

(a) Raises doubt as to the accuracy of any information or document provided or the ownership of the juridical person or legal arrangement;

(b) Justifies reclassification of the customer from low or normal risk to high risk, pursuant to this IRR;

(c) Indicates that any of the suspicious circumstances, as herein defined, exists.

8.3. *Review and Updating of Records.*

Covered persons shall, based on materiality and risk, ensure that information and documents collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers. Updating of records shall be mandatory when enhanced OMP is warranted.

Section 9. Risk-based Approach in Conducting CDD.

9.1. *Risk-based CDD.*

In conducting CDD, a risk-based approach shall be undertaken. Covered persons shall assess their customers to determine who are likely to pose low, normal, or high risk.

9.2 *Risk Profiling of Customers.*

Covered persons shall develop a clear set of criteria for customer risk profiling and assessment. Criteria shall include, at least, three (3) of the following; *Provided*, that the covered person is satisfied that customer's risk profile is sufficiently established:

(a) the nature of the service or product to be availed of by the customers;

(b) the purpose of the account or transaction;

(c) the source of fund and source of wealth;

(d) the nature of business and/or employment;

(e) country of origin and residence of operations, or the fact that a customer came from a high-risk jurisdiction or geographical area;

(f) 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 the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List;

(g) the existence of suspicious transaction indicators; and

(h) such other factors as the covered persons may deem reasonable or necessary to consider in assessing the risk of a customer, including the amount of funds to be transacted by a customer or the size of transactions undertaken, regularity or duration of the transaction, and/or are included in the negative list.

9.3. *Risk Profiling of Juridical Persons.*

In assessing the risk profile of juridical persons, the covered person shall also consider the financial profile and other relevant information of the active authorized signatories.

9.4. *Documentation of Risk Profiling Results.*

The covered person shall document the risk profiling results, as well as how a customer was profiled and the standard of CDD applied.

9.5. *Standards for RDD, ADD and EDD.*

Covered persons shall set the standards in applying RDD, ADD, and EDD, including a set of conditions for continuance or discontinuance of service, or business relationship.

Section 10. Enhanced Due Diligence.

10.1. Covered persons shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions, which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Where the risks are higher, covered persons shall conduct EDD.

10.2. When conducting EDD, covered persons shall perform the following:

(a) Gather documents to support the:

(1) Sources of wealth and fund;

(2) Nature of occupation and/or business;

(3) Reason for intended or 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.

(b) Conduct additional validation procedures, such as:

(1) verifying volume of assets, information available through public databases, internet and other records;

(2) verifying the declared residence address and conducting face-to-face contact with the customers, and their agents and beneficial owners; and

(3) other modes of validation, which the covered person deems reliable and practical.

(c) Secure the approval of senior management to commence or continue transacting with the customer;

(d) Conduct enhanced ongoing monitoring, including more frequent or regular updating of identification information and identification documents;

(e) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and

(f) Such other measures as the covered persons may deem reasonable or necessary.

Section 11. Reduced Due Diligence.

11.1. Where lower risks of ML/TF have been identified, through an adequate analysis of risk by the covered persons, RDD procedures may be applied. The RDD procedures shall be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.

11.2. In strictly limited circumstances and where there is proven low risk of ML/TF, the SAs may issue guidelines allowing certain exemptions on CDD measures, taking into account the nature of the product, type of business and the risks involved; *Provided*, that ML/TF risks are effectively managed.

Section 12. Failure to Satisfactorily Complete CDD.

Covered persons who are unable to comply with the relevant CDD measures shall:

(a) refuse to open an account, commence business relations or perform the transaction; or shall terminate the business relationship; and

(b) File an STR in relation to the customer, if circumstances warrant.

Section 13. CDD and Tipping-off.

In cases where covered persons form a suspicion of ML/TF and associated unlawful activities, and they reasonably believe that performing the CDD process will tip-off the customer, they need not pursue the CDD process, but should file an STR, closely monitor the account, and review the business relationship.

RULE 19 – PREVENTIVE MEASURES FOR SPECIFIC TRANSACTIONS AND ACTIVITIES

Section 1. Politically-Exposed Persons.

1.1. Covered persons shall establish and record the true and full identity of PEPs, as well as their immediate family members and close relationships /associates.

1.2. Domestic and International Organization PEPs.

In addition to performing the applicable CDD measures under Rule 18 hereof, covered persons shall:

(a) Take reasonable measures to determine whether a customer, and his agent and beneficial owner are PEPs; and

(b) In cases when there is a higher risk business relationship, adopt the following measures:

(1) Obtain senior management approval before establishing or, for existing customers, continuing, such business relationships;

(2) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(3) Conduct enhanced ongoing monitoring on that relationship.

1.3. Foreign PEPs.

In addition to performing the applicable CDD measures under Rule 18 hereof, covered persons shall:

(a) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;

(b) Obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;

(c) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) Conduct enhanced ongoing monitoring on that relationship.

Section 2. Life Insurance and Other Investment-related Insurance Policies.

2.1. In addition to the CDD required for the customers and beneficial owner, covered persons shall conduct the following CDD measures on the beneficiary of life insurance and other investment-related insurance policies, as soon as the beneficiary is identified or designated:

(a) For a beneficiary that is identified as specifically named natural or juridical person, or legal arrangements: taking the name of the person.

(b) For a beneficiary that is designated by characteristics, by class, or by other means: obtaining sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish the identity of the beneficiary at the time of payout.

(c) For both the above cases: the verification of the identity of the beneficiary should occur at the time of payout.

2.2. Covered persons shall include the beneficiary of life insurance policy as a relevant risk factor in determining whether EDD is applicable. If the covered person determines that a beneficiary who is a juridical person or legal arrangement presents a higher risk, it shall take enhanced measures, which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

2.3. In relation to life insurance policies, covered persons shall take reasonable measures to determine whether the beneficiaries and the beneficial owner of the beneficiary, are PEPs. This should occur, at the latest, at the time of the payout. Where higher risks are identified, covered persons shall inform senior management before the payout of the policy proceeds, to conduct

enhanced scrutiny on the whole business relationship with the policyholder, and to consider filing an STR.

Section 3. Correspondent Banking.

3.1. Covered persons shall adopt policies and procedures to prevent correspondent banking activities from being utilized for ML/TF activities, and designate an officer responsible in ensuring compliance with these policies and procedures.

3.2. A covered person may rely on the CDD measures undertaken by the respondent bank pursuant to the AML/CTF guidelines of the BSP.

3.3. In relation to cross-border correspondent banking and other similar relationships, covered persons are required to:

(a) Gather sufficient information about the respondent institution to understand fully the nature of the respondent's business, and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action;

(b) Assess the respondent institution's AML/CTF controls;

(c) Obtain approval from senior management before establishing new correspondent relationships; and

(d) Clearly understand the respective AML/CTF responsibilities of each institution.

3.4. With respect to payable-through accounts, covered persons are required to satisfy themselves that the respondent bank:

(a) Has performed CDD on its customers that have direct access to the accounts of the correspondent bank; and

(b) Is able to provide relevant CDD information upon request to the correspondent bank.

3.5. Covered persons shall not enter into, or continue, correspondent banking relationships with shell banks and shall have measures to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

Section 4. Money or Value Transfers Services.

4.1. Covered persons which provide money or value transfer services shall register with the BSP for purposes of supervision and checking compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances. They shall also register with the AMLC for purposes of filing CTRs and STRs.

4.2. Covered persons that provide money or value transfer services without the required license or registration shall be subject to enforcement actions of the BSP or administrative sanctions of the AMLC, whichever is appropriate.

4.3. Covered persons that provide money or value transfer services shall maintain a current list of its agents accessible by the AMLC and the BSP, and available upon request.

4.4. Covered persons which provide money or value transfer services that use agents shall include them in their AML/CTF programs and monitor them for compliance with these programs.

Section 5. New Technologies.

5.1. The AMLC, in coordination with the relevant SAs, LEAs, OGAs, and covered persons, should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

5.2. The AMLC and the relevant SAs shall adopt mechanisms to manage and mitigate risks emerging from virtual assets by ensuring that virtual asset providers are:

(a) regulated for AML/CTF purposes;

(b) licensed or registered; and

(c) subject to effective systems for monitoring and ensuring compliance with the relevant preventive measures.

5.3. Covered persons shall undertake risk assessments prior to the launch or use of such products, practices and technologies; and take appropriate measures to manage and mitigate the risks.

Section 6. Wire Transfers.

6.1. *Originating/Ordering Financial Institutions.*

6.1.1. Originating/ordering financial institutions shall not accept instructions for wire transfer from a non-customer originator, for occasional transactions exceeding the set threshold, unless it has conducted the necessary CDD measures to establish the true and full identity and existence of said originator.

6.1.2. Financial institutions shall ensure that all cross-border wire transfers in the amount or threshold to be determined by the BSP or its equivalent in foreign currency are always accompanied by the following:

(a) Required and accurate originator information:

(1) the name of the originator;

(2) the account number of the originator, where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number, which permits traceability of the transaction; and

(3) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) Required beneficiary information:

(1) the name of the beneficiary; and

(2) the beneficiary account number, where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number, which permits traceability of the transaction.

6.1.3. Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the financial institution shall include the originator's account number or unique transaction reference number.

6.1.4. If a *de minimis* threshold, as determined by the BSP, or its equivalent in foreign currency, is applied for the requirements under Rule 19, Section 6.1.2 hereof, originating/ordering financial institutions shall ensure that all cross-border wire transfers below the applicable *de minimis* threshold are always accompanied by the following:

(a) Required originator information:

(1) the name of the originator; and

(2) the originator account number, where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number, which permits traceability of the transaction.

(b) Required beneficiary information:

(1) the name of the beneficiary; and

(2) the beneficiary account number, where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number, which permits traceability of the transaction.

6.1.5. The information mentioned in Rule 19, Section 6.1.4 hereof need not be verified for accuracy. However, the financial institution shall verify the information pertaining to its customer where there is a suspicion of ML/TF.

6.1.6. For domestic wire transfers, the originating/ordering financial institution shall ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means.

6.1.7. Where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other means, the originating/ordering financial institution need only be required to include the account number or a unique transaction reference number; *Provided*, that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The originating/ordering financial institution shall make the information available within five (5) working days from receipt of the request either from the beneficiary financial institution or from appropriate authorities.

6.1.8. The ordering financial institution shall maintain all originator and beneficiary information collected, in accordance with Rule 19 hereof.

6.1.9. The ordering financial institution shall not be allowed to execute the wire transfer if it does not comply with all the requirements under Rule 19, Section 6.1.1 to 6.1.8 hereof.

6.2. *Intermediary Financial Institutions*

6.2.1. For cross-border wire transfers, an intermediary financial institution shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

6.2.2. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution should be required to keep a record, for at least five (5) years, of all the information received from the originating/ordering financial institution or another intermediary financial institution.

6.2.3. Intermediary financial institutions shall take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

6.2.4. Intermediary financial institutions shall have risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

6.3. *Beneficiary Financial Institutions*

6.3.1. A beneficiary financial institution shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Rule 19 hereof. Should the originator and beneficiary be the same person, the beneficiary financial institution may rely on the CDD conducted by the originating institution, treating the originating institution as third party.

6.3.2. Beneficiary financial institutions shall take reasonable measures, which may include post-event monitoring, or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

6.3.3. Beneficiary financial institutions shall have risk-based policies and procedures for determining:

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

6.4. *Money or Value Transfer Service Providers.*

6.4.1. MVTS providers shall comply with all of the relevant requirements of Rule 19, Section 6 hereof in all countries in which they operate, directly or through their agents.

6.4.2. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider shall:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the concerned FIU.

6.5 *Implementation of Targeted Financial Sanctions.*

Covered persons shall secure the consent of all their customers to be bound by obligations set out in the relevant United Nations Security Council Resolutions relating to the prevention and suppression of proliferation financing of weapons of mass destruction, including the freezing and unfreezing actions as well as prohibitions from conducting transactions with designated persons and entities.

Section 7. Shell Bank, Shell Company and Bearer Share Entity.

7.1. A covered person shall always apply EDD on both the entity and its beneficial owners when dealing with a shell company.

7.2. Covered persons shall refuse to deal, enter into, or continue, correspondent banking relationship with shell banks. They shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks.

7.3. A covered person dealing with bearer share entities shall be required to conduct EDD diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account. These entities shall be subject to ongoing monitoring procedure at all times and the list of stockholders and/or beneficial owners shall be updated within thirty (30) days after every transfer of ownership and the appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

Section 8. High-Risk Jurisdiction or Geographical Location.

8.1. Covered persons shall apply EDD, proportionate to the risks, to accounts, transactions, and business and professional relationships with customers who are nationals or citizens from foreign jurisdiction or geographical location that presents greater risk for ML/TF or its associated unlawful activities, or is recognized as having inadequate internationally accepted AML/CTF standards, as determined by the relevant domestic or international bodies.

8.2. The AMLC and the SAs shall apply proportionate countermeasures to address risks posed by customers from high-risk jurisdiction or geographical location.

8.3. The AMLC and the SAs shall establish measures to ensure that covered persons are advised of concerns about weaknesses in the AML/CTF systems of other countries.

RULE 20 – RECORD-KEEPING

Section 1. Record-Keeping.

Covered persons shall maintain and safely store for five (5) years from the dates of transactions all customer records and transaction documents.

Section 2. Closed Accounts and Terminated Relationships.

Covered persons shall keep all records obtained through CDD, account files and business correspondence, and the results of any analysis undertaken, for, at least, five (5) years following the closure of account, termination of the business or professional relationship or after the date of the occasional transaction.

Section 3. Retention of Records Where there is a Case.

If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5)-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

Section 4. Form of Records.

4.1. Complimented by the requirements under the 2018 Guidelines on Digitization of Customer Records, covered persons shall retain all transaction records either in:

(a) their original forms; or

(b) such other forms sufficient to permit reconstruction of individual transactions so as to provide admissible evidence in court.

4.2. Covered persons shall keep the electronic copies of all CTRs and STRs for, at least, five (5) years from the dates of submission to the AMLC.

4.3. For low risk customers, covered persons shall maintain and store, in whatever form, a record of information data and transactions, sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Section 5. Availability of Records

5.1. Covered persons shall ensure that all CDD information and transaction records are available swiftly to domestic competent authorities in the exercise of their official functions or upon order by a competent authority.

5.2. Covered persons shall take measures to ensure that customer records are submitted in the manner, quality and period as would assist the AMLC in its prompt financial investigations and institution of legal actions. For this purpose, covered persons shall implement the guidelines on the digitization of customer records issued by the AMLC.

RULE 21 – RELIANCE ON THIRD PARTIES AND SERVICE PROVIDERS

Section 1. Third Party Reliance.

1.1. A covered person may rely on a third party in conducting CDD under item a, b, d, e of Section 2.1 under Rule 18 and record-keeping measures. The third party shall be:

(a) A covered person; or

(b) A financial institution or DNFBP operating outside the Philippines that is covered by equivalent CDD and record-keeping measures. When determining in which countries the third party that meets the conditions can be based, covered persons shall have regard to information available on the level of country risk.

1.2. Notwithstanding the foregoing, the ultimate responsibility for CDD and record-keeping remains with the covered person relying on the third party, which shall be required to:

(a) obtain immediately the necessary information received and gathered during the conduct of the different CDD measures;

(b) take steps to satisfy itself that copies of record of identification information and IDs shall be made available from the third party upon request without delay; and

(c) satisfy itself that the third party is a covered person, and has measures in place for compliance with, CDD and record-keeping requirements.

1.3. In cases of high-risk customers, the covered person relying on the third person shall also conduct EDD procedure.

1.4. Covered persons may rely on a third party that is part of the same financial, business or professional group under the following circumstances:

(a) the group applies CDD and record-keeping requirements, in line with the AMLA and TFPSA, their respective IRR, and other AMLC issuances; and the MTPP, in accordance with Rule 16 hereof;

(b) the implementation of CDD and record-keeping requirements, and the MTPP is supervised at a group level by an SA; and

(c) any higher country risk is adequately mitigated by the group's AML/CTF policies.

RULE 22 – TRANSACTION REPORTING

Section 1. CTR and STR.

1.1. Filing of CTRs and STRs.

Covered persons shall file all CTRs and STRs, in accordance with the registration and reporting guidelines of the AMLC.

1.2. Covered Transaction also a Suspicious Transaction.

Should a transaction be determined to be both a covered and a suspicious transaction, the same shall be reported as a suspicious transaction. In this regard, it shall l be reported first as a CTR, subject to updating if it is finally confirmed to be reportable as STR.

1.3. Exemption from Reporting.

Lawyers and accountants who are: (a) authorized to practice their profession in the Philippines; and (b) engaged as independent legal or accounting professionals, in relation to information concerning their clients, or where disclosure of information would compromise client confidences or the attorney-client relationship are not required to file CTRs.

Lawyers and accountants, however, are not precluded from submitting STRs to the AMLC with regard to any transaction of their clients that is in any way related to ML/TF or related unlawful activity that is about to be committed, is being or has been committed.

Section 2. Timing of Reporting.

2.1. CTRs shall be filed within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

2.2. STRs shall be filed within the period prescribed under the registration and reporting guidelines of the AMLC.

Section 3. Quality and Form of Reports.

3.1. Covered persons shall ensure the completeness, accuracy, and timeliness of CTRs and STRs.

3.2. CTRs and STRs shall be filed in such form as may be prescribed by the AMLC and shall be submitted in a secured manner to the AMLC in electronic form.

Section 4. Registration with the AMLC.

All covered persons shall register with the AMLC's electronic reporting system accordance with the registration and reporting guidelines.

Section 5. AML/CTF Monitoring System.

5.1. All covered persons shall adopt an AML/CTF monitoring system that is appropriate for their risk-profile and business complexity and in accordance with these Rules. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the board of directors and senior management on AML/CTF compliance.

5.2. *Electronic Monitoring and reporting systems for AML/CTF.*

5.2.1. Covered persons that are considered complex, as determined by SAs shall adopt an electronic AML/CTF system capable of monitoring risks associated with ML/TF as well as generating timely reports for the guidance and information of its board of directors and senior management. It should ensure that the system, at a minimum, shall detect and

raise to the covered person's attention, transaction and/or accounts that qualify either as covered transaction or suspicious transaction, as herein defined. The covered person shall endeavor to interface the electronic monitoring system with the systems of its branches, subsidiaries and affiliates, if any, for group-wide AML/CTF monitoring.

5.2.2. The system must have, at least, the following automated functionalities:

a. CTR/STR Monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;

b. Watchlist Monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;

c. Investigation – checks for given names throughout the history of payment stored in the system;

d. Can generate all the CTRs of the covered person accurately and completely with all the mandatory field properly filled up;

e. Must provide a complete audit trail;

f. Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and

g. Has the capability to record all suspicious transactions and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC.

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

5.2. *Manual Monitoring.*

Covered persons which are not required to have an electronic system of flagging and monitoring transactions, as determined by SAs shall ensure that they have the means of flagging and monitoring the transactions mentioned in Section 5.1. They shall maintain a register of all STs that have been brought to the attention of Senior Management whether or not the same was reported to the AMLC.

Section 5. Safe Harbor Provision.

No administrative, criminal or civil proceedings shall lie against any person for having made a CTR or an STR in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law.

Section 6. Confidentiality of Reporting.

6.1. When reporting covered or suspicious transactions, covered persons, and their officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction

has been or is about to be reported, the contents of the report, or any other information in relation thereto.

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

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

Section 7. Registration and Reporting Guidelines.

Covered persons shall ensure compliance with registration and reporting guidelines in complying with their obligations under Rule 22 hereof.

CHAPTER VII
BENEFICIAL OWNERSHIP

RULE 23 – BENEFICIAL OWNERSHIP OF JURIDICAL PERSONS

Section 1. Mechanism for Identification of Juridical Persons.

1.1. The SEC is hereby enlisted to develop mechanisms that identify and describe the following:

(a) Different types, forms and basic features of legal persons in the country;

(b) Processes for the creation of those legal persons; and

(c) Processes for obtaining and recording of basic and beneficial ownership information.

1.2. The SEC shall develop a mechanism to make the information on the legal persons and their beneficial owners publicly available, as may be allowed under existing laws.

1.3. In the conduct of risk assessments, all stakeholders, including SAs and covered persons, shall assess the risks associated with all types of legal person created in the country.

Section 2. Basic Information.

2.1. The SEC, as may be allowed under existing laws, shall, at the time of registration, require all companies to submit the following basic information:

(a) company name;

(b) proof of incorporation;

(c) legal form and status;

(d) official address;

(e) organizational structure; and

(f) list of directors and responsible officers.

2.2. The SEC, as may be allowed under existing laws, require their juridical persons to maintain records of, and submit, the information set out in Rule 23, Section 2.1 hereof, and maintain a register of their shareholders or members, containing the number of shares held by each shareholder or member, and the categories of shares, including the nature of the associated voting rights.

2.3. The SEC, as may be allowed under existing laws, shall develop mechanisms to make the information referred to in Rule 23, Sections 2.1 and 2.2 hereof are maintained in a location within the Philippines that is known to SEC.

2.4. The SEC shall develop mechanisms to ensure that the information referred to in Rule 23, Sections 2.1 and 2.2 hereof are accurate and regularly updated on a timely basis.

Section 3. Beneficial Ownership Information.

3.1. *Mechanism to Ensure Accessibility.*

To ensure that information on the beneficial ownership of a company is accessible to the AMLC or SAs in a timely manner, the following mechanisms shall be observed:

(a) The SEC shall obtain and hold up-to-date information on the companies' beneficial ownership;

(b) The SEC shall require companies and clients that are legal persons, respectively, to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Use existing information, including:

(1) information obtained by covered persons in the course of CDD;

(2) information held by other competent authorities on the legal and beneficial ownership of companies;

(3) information held by the company and submitted to the SEC as required under Rule 24, Section 2.1; and

(4) available information on companies listed on a stock exchange, where disclosure requirements ensure adequate transparency of beneficial ownership.

3.2. *Accuracy of Beneficial Ownership Information.*

The SEC shall require companies and corporate clients, respectively, to submit accurate and regularly updated beneficial ownership information.

3.3. *Cooperation by Juridical Persons with the AMLC and/or SAs.*

The SEC, as may be allowed under existing laws, shall ensure that juridical persons cooperate with the AMLC and all SAs, to the fullest extent possible, in determining the beneficial owner, by:

(a) requiring that, at least, one (1) natural person resident in the Philippines is authorized by the company, and accountable to the AMLC and the SAs, for providing all basic information and available beneficial ownership information, and giving further assistance to them; and/or

(b) requiring DNFBPs in the country to provide AMLC and SAs basic information and available beneficial ownership information; and/or

(c) taking other comparable measures, specifically identified by the SEC.

3.4. *Record-Keeping After Dissolution of Company.*

The information and records referred to under Rule 23, Section 2 and 3 hereof shall, as may be allowed under existing laws, be maintained by the following entities, at least, five (5) years after the date on which the company is dissolved or otherwise ceases to exist, or five (5) years after the date on which the company ceases to be a customer of the covered person, subject to the following conditions:

(a) The SEC; and

(b) All companies; or its administrators, liquidators or other persons involved in the dissolution of the company, upon the directive of the SEC.

Section 4. Other Requirements.

4.1. The AMLC, SAs, LEAs and OGAs shall, in accordance with their respective powers and functions, have timely access to the basic and beneficial ownership information held by the SEC, covered persons or juridical persons.

4.2. Covered persons shall not be allowed to issue bearer shares or bearer share warrants, in accordance with the Corporation Code of the Philippines.

4.3. The SEC, as may be allowed under existing laws, shall apply, at least, one (1) of the following mechanisms to juridical persons that are able to have nominee shares and nominee directors to ensure they are not misused:

(a) requiring nominee shareholders and directors to disclose the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register;

(b) requiring nominee shareholders and directors to be licensed, for their nominee status to be recorded in company registries, and for them to maintain information identifying their nominator, and make this information available to the competent authorities upon request; or

(c) using other mechanisms identified by the SEC.

4.4. The SEC shall, as may be allowed under existing laws, hold liable, and impose proportionate and dissuasive sanctions, as appropriate for any juridical person that fails to comply with the requirements under Rule 23 hereof.

RULE 24 – BENEFICIAL OWNERSHIP OF LEGAL ARRANGEMENTS

Section 1. Trustees and other Legal Arrangement.

Covered persons, as the case may be, shall require clients that are:

(a) *trustees of any express trust are required* to obtain and hold adequate, accurate, and current information on the identity of the trustors/grantors/settlors, the trustee, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. For beneficiaries of trusts that are designated by characteristics or by class, financial institutions should obtain sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

(b) *trustees of any trust are required* to hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors; and

(c) *professional trustees are required* to maintain this information for, at least, five (5) years after their involvement with the trust ceases.

Section 2. Accuracy of Beneficial Ownership Information.

Covered persons shall ensure that any information held pursuant to Rule 24 hereof is kept accurate and as up to date as possible, and is updated on a timely basis.

Section 3. Disclosure of Status of Trustees.

Covered persons shall require trustees to disclose their status when forming a business or professional relationship, or carrying out an occasional transaction above the threshold.

Section 4. Submission of Beneficial Ownership Information to Covered Persons.

Covered persons shall, depending on its risk assessment, require clients that are trustees to submit information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business or professional relationship.

Section 5. Other Requirements.

5.1. The AMLC, SAs, LEAs and OGAs shall, in accordance with their respective powers and functions, be able to obtain timely access to information held by trustees and covered persons, on the beneficial ownership and control of the trust, including:

(a) the beneficial ownership;

(b) the residence of the trustee; and

(c) any assets held or managed by the financial institution or DNFBP, in relation to any trustees with which they have a business relationship, or for which they undertake an occasional transaction.

5.2. The applicable SAs shall, as may be allowed under existing laws, hold liable, and impose proportionate and dissuasive sanctions, as appropriate for any legal arrangement that fails to grant to competent authorities timely access to information regarding the trust referred to in Rule 24, Section 1 hereof.

CHAPTER VIII
SANCTIONS

RULE 25 – CRIMINAL SANCTIONS

Section 1. Penalties for ML.

The following are the penalties to be imposed on persons convicted of ML:

(a) *Penalties for Section 4(a), (b), (c) and (d) of the AMLA.*

The penalty of imprisonment ranging from seven (7) to fourteen (14) years and a fine of not less than three million pesos (PHP3,000,000.00), but not more than twice the value of the monetary instrument or property involved in the offense, shall be imposed upon a person convicted under Section 4(a), (b), (c) and (d) of the AMLA, as amended.

(b) *Penalties for Section 4(e) and (f) of the AMLA.*

The penalty of imprisonment from four (4) to seven (7) years and a fine of not less than one million five hundred thousand pesos (PHP1,500,000.00) but not more than three million pesos (PHP3,000,000.00), shall be imposed upon a person convicted under Section 4(e) and (f) of the AMLA, as amended.

(c) *Penalties for the Last Paragraph of Section 4 of the AMLA.*

The penalty of imprisonment from six (6) months to four (4) years or a fine of not less than one hundred thousand pesos (PHP100,000.00) but not more than five hundred thousand pesos (PHP500,000.00), or both, shall be imposed on a person convicted under the last paragraph of Section 4 of the AMLA, as amended.

Section 2. Penalties for Knowingly Participating in ML.

The penalty of imprisonment ranging from four (4) to seven (7) years and a fine corresponding to not more than two hundred percent (200%) of the value of the monetary instrument or property laundered shall be imposed upon the covered person, its directors, officers or personnel who knowingly participated in the commission of the crime of ML.

Section 3. Penalties for Failure to Keep Records.

The penalty of imprisonment from six (6) months to one (1) year or a fine of not less than one hundred thousand pesos (PHP100,000.00), but not more than five hundred thousand pesos (PHP500,000.00), or both, shall be imposed on a person convicted under Section 9(b) of the AMLA.

Section 4. Penalties for Malicious Reporting.

4.1. Any person who, with malice, or in bad faith, reports or files a completely unwarranted or false information relative to ML transaction against any person shall be subject to a penalty of six (6) months to four (4) years imprisonment and a fine of not less than one hundred thousand pesos (PHP100,000.00) but not more than five hundred thousand pesos (PHP500,000.00), at the discretion of the court: *Provided*, that the offender is not entitled to avail of the benefits of the Probation Law.

4.2. If the offender is a corporation, association, partnership or any other juridical person, the penalty of imprisonment and/or fine shall be imposed upon the responsible officers, who participated in, or allowed by their gross negligence the commission of the crime and the court may suspend or revoke its license. If the offender is an alien, he shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties herein prescribed. If the offender is a public official or employee, he shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office.

4.3. Any public official or employee who is called upon to testify and refuses to do the same or purposely fails to testify shall suffer the same penalties herein prescribed.

Section 5. Penalties for Breach of Confidentiality.

The punishment of imprisonment ranging from three (3) to eight (8) years and a fine of not less than five hundred thousand pesos (PHP500,000.00) but not more than one million pesos (PHP1,000,000.00), shall be imposed on a person convicted for a violation under Section 9(c) of the AMLA. In case of a breach of confidentiality that is published or reported by the media, the responsible reporter, writer, president, publisher, manager and editor-in-chief shall be liable under the AMLA.

Section 6. Criminal Liability of Corporate Entities.

If the offender is a corporate entity, the penalties herein shall be imposed upon the responsible officers who participated in, or allowed by their gross negligence the commission of the crime; and/or directors or trustees who willfully and knowingly voted for or assented to violate the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

RULE 26 – ADMINISTRATIVE SANCTIONS

Section 1. Coverage.

The Council shall, after due notice and hearing, impose administrative sanctions upon covered persons, and their responsible directors, officers and employees, or any other person for violations of the AMLA, this IRR, or for failure or refusal to comply with the orders, resolutions and other issuances of the AMLC.

Section 2. Independent Proceedings.

The administrative proceedings before the AMLC, including the imposition of administrative sanctions, shall be without prejudice to the filing of criminal charges against the persons responsible for the violation.

Section 3. Nature of the Proceedings.

The administrative proceedings before the AMLC shall be non-litigious and summary in nature, subject to the requirement of due process and substantial evidence.

Section 4. Rules on Imposition of Administrative Sanctions.

4.1. The AMLC shall promulgate or update the rules on the imposition of administrative sanctions, taking into consideration the following:

(a) Requirement of notice and hearing, and substantial evidence;

(b) Need for an independent and impartial administrative adjudication unit to hear and recommend actions on administrative cases;

(c) Exercise of AMLC's discretion in choosing the type and extent of sanctions to be imposed, if warranted;

(d) Types and extent of proportionate and dissuasive sanctions that may be imposed; and

(e) Attendant circumstances to be considered by the AMLC in determining, such as the nature and gravity of the violation or irregularity.

4.2. In the absence of any applicable provision in the rules on the imposition of administrative sanctions, and in order to effectuate the objectives of the AMLA, the pertinent provisions of the Rules of Court may, in the interest of expeditious dispensation of administrative cases, and whenever practicable and convenient, be applied by analogy or in a suppletory character and effect.

Section 5. Types of Administrative Sanctions.

5.1. The Council shall, at its discretion, impose sanctions, including reprimand, warning, fine, or such other measures as may be necessary and justified to prevent and counteract ML/TF, as identified in the rules on the imposition of administrative sanctions.

5.2. Fines shall be in amounts as may be determined by the Council to be appropriate, which shall not be more than five hundred thousand pesos (PHP500,000.00) per violation.

Section 6. Enforcement Actions by Covered Persons.

6.1. The SAs shall, consistent with their charters or laws, formulate rules on the imposition of enforcement actions for violation of their respective circulars and orders.

6.2. The findings of SAs with regard to violations of the AMLA and TFPSA, their respective IRR and other AMLC issuances shall be escalated to the AMLC for possible administrative sanctions.

Section 7. Non-discrimination Against Certain Types of Customers.

6.1. Whenever covered persons discriminate against certain customer types, such as politically-exposed persons, as well as their relatives; or against a certain religion, race, or ethnic origin; or such other attributes or profiles when used as the only basis to deny these persons access to the

services provided by the covered persons, the person or persons responsible for such violation shall be subject to sanctions as may be deemed appropriate by their respective SAs.

6.2. SAs shall promulgate or update their rules to timely and sufficiently address discrimination against customers committed by covered persons, and their respective directors, officers and employees.

RULE 27 – CIVIL SANCTIONS

Section 1. Asset Recovery.

Monetary instruments and properties related to ML/TF and associated unlawful shall be the subject of freeze order and civil forfeiture proceedings, as provided under Rules 10 and 12 hereof.

Section 2. Restitution.

Restitution for any aggrieved party whose rights were violated shall be governed by the provisions of the New Civil Code.

CHAPTER IX
DOMESTIC AND INTERNATIONAL COOPERATION

RULE 28 – DOMESTIC COOPERATION

Section 1. National AML/CTF Strategies.

The AMLC, in coordination with the relevant SAs, LEAs, OGAs, covered persons, and other stakeholders, shall formulate, and regularly review. update, and monitor the national strategies, which are informed by the risks identified, for a concerted effort in fighting ML/TF.

Section 2. AML/CTF Policies.

The AMLC shall, formulate policy directions for, and regulate the Philippines' AML/CTF regime. SAs, LEAs, OGAs, covered persons, and other stakeholders may propose AML/CTF policies to the AMLC, through the AMLC Secretariat.

Section 3. Mechanism for Cooperation and Coordination.

The AMLC, SAs, LEAs and OGAs shall establish mechanisms, including exchange of information, for cooperation and coordination in:

(a) Developing and implementing the national AML/CTF strategies, policies and activities; and

(b) Combating the financing of proliferation of weapons of mass destruction. *Provided*, that the financing thereof has any relation to ML/TF or associated unlawful activities.

Section 4. Confidentiality of Information.

The AMLC shall maintain the confidentiality of requests for information that they receive and the information received from SAs, LEAS and OGAs.

RULE 29 – MUTUAL LEGAL ASSISTANCE

Section 1. MLA Request from a Foreign State.

1.1. Where a foreign State makes an MLA request in the investigation or prosecution of a ML/TF offense, the AMLC may execute the request or refuse to execute the same and inform the foreign State of any valid reason for not executing the request or for delaying the execution thereof.

1.2. The AMLC may refuse to comply with any MLA request where the action sought in the request contravenes any provision of the Constitution or the execution of the request is likely to prejudice the national interest of the Philippines, unless there is a treaty between the Philippines and the requesting State relating to the provision of assistance in relation to ML/TF or associated unlawful activity.

Section 2. Basis for Making and Acting on MLA Request.

A foreign State may make, and the Philippines may execute, an MLA request pursuant to conventions, treaties and international agreements over which the Philippines is a party. The principles of mutuality and reciprocity shall, at all times, be recognized.

Section 3. Requirements for MLA Requests from Foreign States.

All MLA requests from a foreign State must:

(a) confirm that an investigation or prosecution is being conducted in respect of a money launderer or terrorism financer named therein, or that he has been convicted of any ML/TF offense or associated unlawful activity;

(b) state the grounds on which any person is being investigated or prosecuted for ML/TF or associated unlawful activity or the details of his conviction;

(c) give sufficient particulars as to the identity of said person, including specific monetary instrument or property;

(d) give particulars sufficient to identify any covered person believed to have any information, document, material or object which may be of assistance to the investigation or prosecution;

(e) specify the concerned covered person from which any information, document, material or object that may be of assistance to the investigation or prosecution may be gathered;

(f) specify the manner in which and to whom said information, document, material or object obtained pursuant to said request, is to be produced;

(g) give all the particulars necessary for the issuance by the court in the requested State of the writs, orders or processes needed by the requesting State; and

(h) contain such other information as may assist in the execution of the request, including the statement of the specific legal provision of the penal law on ML/TF or associated unlawful that was violated in the requested State. *Provided*, that the felonies or offenses punishable under the penal laws of the requesting State are of a nature similar to the unlawful activities as herein defined.

Section 4. Procedure for MLA Requests from Foreign States.

4.1. *Receipt of MLA Request.*

MLA requests shall be received by the following government agencies:

(a) All MLA requests from foreign States shall be filed with the DOJ, as the central authority on all MLA matters; or

(b) The AMLC may directly receive and act on MLA requests made on the basis of reciprocity; *Provided*, that all actions taken on such requests shall be transmitted to the DOJ for formal response to the requesting State.

4.2. *Powers of the AMLC to Act on MLA Requests.*

The AMLC may execute an MLA request from a foreign State by:

(a) tracking down, freezing, restraining and seizing assets alleged to be proceeds of or related to any unlawful activity under the procedures laid down in the AMLA and TFPSA, their respective IRR, and other AMLC issuances;

(b) giving information or documents needed by the foreign State, for evidentiary purposes, within the procedures laid down in the AMLA and TFPSA, their respective IRR, and other AMLC issuances; and

(c) applying for an order of forfeiture of any monetary instrument or property with the court: *Provided*, that the court shall not issue such an order unless the application is accompanied by an authenticated copy of the order of a court in the requesting State ordering the forfeiture of said monetary instrument or property of a person who has been convicted of a ML/TF offense or an unlawful activity in the requesting State, and a certification or an affidavit of a competent officer of the requesting State stating that the conviction and the order of forfeiture are final and that no further appeal lies in respect of either.

4.3. *Investigation, Freeze Order, Bank Inquiry and Civil Forfeiture.*

4.3.1. The provisions on AMLC investigation, and freeze order, bank inquiry and civil forfeiture, shall apply to MLA requests when necessary to effect the assistance to be extended.

4.3.2. The AMLC shall adopt a flexible mechanism for:

(a) coordinating with other States regarding requests for freezing and forfeiture of assets; and
(b) managing, including disposal, of frozen, preserved and forfeited assets.

4.3.1. The AMLC shall coordinate, if necessary, with the requesting State on the, procedure for, and mode of, turnover of the portion of the forfeited assets that belongs to the relevant persons in the requesting State.

4.4. *Suppletory Application of the Rules of Court.*

For attachment of Philippine properties in the name of persons convicted of any unlawful activity, execution and satisfaction of final judgments of forfeiture, application for examination of witnesses, procuring search warrants, production of bank documents and other materials, and all other actions not specified in the AMLA and TFPSA, their respective IRR, and other AMLC issuances, and assistance for any of the aforementioned actions, which is subject of a request by a foreign State, resort may be had to the proceedings pertinent thereto under the Rules of Court.

4.5. *Results of AMLC Action.*

The results of the actions taken by the AMLC shall be transmitted to the DOJ for formal response to the requesting State.

Section 5. Authentication of Documents.

5.1. A document is authenticated if it is signed or certified by a judge, magistrate or equivalent officer in or of, the requesting State, and authenticated by the oath or affirmation of a witness or sealed with an official or public seal of a minister, secretary of state, or officer in or of, the government of the requesting State, or of the person administering the government or a department of the requesting territory, protectorate or colony.

5.2. The certificate of authentication may also be made by a secretary of the embassy or legation, consul general, consul, vice consul, consular agent or any officer in the foreign service of the Philippines stationed in the foreign State in which the record is kept, and authenticated by the seal of his office.

Section 6. MLA Request to a Foreign State.

6.1. The AMLC may make an MLA request to foreign States pursuant to Rule 29, Section 2 hereof.

6.2. The AMLC may make an MLA request to any foreign State in:

(a) tracking down, freezing, restraining and seizing assets alleged to be proceeds of any unlawful activity;

(b) obtaining pertinent information and documents that it needs relating to any ML/TF offense or any other matter directly or indirectly related thereto;

(c) to the extent allowed by the law of the foreign State, applying with the proper court therein for an order to enter any premises belonging to or in the possession or control of, any or all of the persons named in said request, and/or search any or all such persons named therein and/or remove any document, material or object named in said request: *Provided*, that the documents accompanying the request in support of the application have been duly authenticated in accordance with the applicable law or regulation of the foreign State; and

(d) applying for an order of forfeiture of any monetary instrument or property in the proper court in the foreign State: *Provided*, that the request is accompanied by an authenticated copy of the order of the Regional Trial Court ordering the forfeiture of said monetary instrument or property and an affidavit of the clerk of court stating that the order of forfeiture is final and that no further appeal lies in respect of it.

6.3. All MLA requests to a foreign State shall be coursed through the DOJ.

Section 7. Prioritization and Monitoring of MLA Requests.

7.1. The AMLC shall formulate processes for the timely prioritization and execution of mutual legal assistance requests.

7.2. The AMLC shall maintain a case management system to monitor progress of MLA requests.

Section 8. Confidentiality of MLA Requests.

The AMLC shall maintain the confidentiality of MLA requests that they receive and the information contained in them, subject to the requirements of the necessary legal remedies to execute them, in order to protect the integrity of the investigation or inquiry.

RULE 30 – EXTRADITION

Section 1. ML as an Extraditable Offense.

With respect to the state parties that are signatories to the United Nations Convention Against Transnational Organized Crime that was ratified by the Philippine Senate on October 22, 2001, ML is deemed to be included as an extraditable offense in any extradition treaty existing between said state parties, and the Philippines shall include ML as an extraditable offense in every extradition treaty that may be concluded between the Philippines and any of said state parties in the future.

Section 2. TF as an Extraditable Offense.

The Philippines may, at its option, subject to the principle of reciprocity, consider the *International Convention for the Suppression of the Financing of Terrorism* as a legal basis for requesting or granting extradition in respect of any offenses set forth under the TFPSA.

Section 3. Extradition Requirements and Procedure.

Presidential Decree No. 1069 (*Prescribing the Procedure for the Extradition of Persons Who Have Committed Crimes in a Foreign Country*) shall govern extradition proceedings.

Section 4. Negotiation of Future Treaties.

The Philippines shall negotiate for the inclusion of ML offenses among the extraditable offenses in all future treaties.

Section 5. Prioritization and Monitoring.

The DOJ and the AMLC shall adopt a case management system, and clear processes for prioritization and timely execution of extradition requests.

RULE 31 – OTHER FORMS OF INTERNATIONAL COOPERATION

Section 1. Assistance to International Organizations.

1.1. The AMLC shall cooperate and act in respect of conventions, resolutions and other directives, including the implementation of targeted financial sanctions, of the United Nations, United Nations Security Council, and other international organizations of which the Philippines is a member, that has relation to the following:

(a) ML/TF and associated unlawful activities, and

(b) Financing of proliferation of weapons of mass destruction. *Provided*, that the financing thereof is in any way related to ML/TF and associated unlawful activities.

1.2. The AMLC may refuse to comply with the request of any international organization where the action sought therein contravenes the provision of the Constitution or the execution thereof is likely to prejudice the national interest of the Philippines, or if the requesting organization cannot effectively protect the confidentiality of the requested information.

Section 2. Request for Information from a Foreign Jurisdiction.

2.1. The AMLC may execute RFIs from a foreign jurisdiction's FIU, LEA or OGA, by giving information needed by the foreign jurisdiction, for intelligence or investigative purposes, within the procedures laid down in the AMLA and TFPSA, their respective IRR, and other AMLC issuances. The exchanges of information shall be made spontaneously or upon request.

2.2. The AMLC may refuse to comply with the RFI where the action sought therein contravenes the provision of existing laws or the execution thereof is likely to prejudice the national interest of the Philippines, or if the requesting party cannot effectively protect the confidentiality of the requested information.

2.3. The LEAs and OGAs may execute a RFI from their foreign counterparts or non-counterparts, as may be allowed by their respective charters or laws, or refer it to the proper agency for appropriate action. The exchanges of information shall be made spontaneously or upon request.

2.4. The SAs shall, consistent with their respective charters or laws, provide cooperation with their foreign counterparts, consistent with the applicable international standards for supervision, in particular, with respect to the exchange of supervisory information related to or relevant for AML/CTF purposes.

2.5. The SAs shall, consistent with their respective charters or laws, exchange with foreign counterparts, in accordance with existing laws, information domestically available to them, including information held by covered persons under their respective jurisdiction, in a manner proportionate to their needs.

2.6. The SAs shall, consistent with their respective charters or laws, exchange the following types of information when relevant for AML/CTF purposes, with foreign counterparts that have shared responsibility for financial institutions operating in the same group:

(a) Regulatory information, such as information on domestic regulatory system, and general information on the financial sectors;

(b) Prudential information, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness; and

(c) AML/CTF information, such as internal AML/CTF procedures and policies of financial institutions, and other information from or about the financial institutions

2.7. The SAs shall, consistent with their respective charters or laws, conduct inquiries in behalf of their foreign counterparts, and, as appropriate, to authorize or facilitate the ability of foreign counterparts to conduct inquiries themselves in the Philippines, in order to facilitate effective group supervision.

Section 3. Requests for Beneficial Ownership Information.

3.1. The AMLC, SAs, LEAs and OGAs shall, consistent with their respective mandates, provide international cooperation in relation to basic and beneficial ownership information in a timely manner, based on mutual legal assistance and informal exchange of information. This should include:

(a) facilitating access by foreign competent authorities to basic information held by the SEC;

(b) exchanging information on shareholders; and

(c) using their investigative powers, as may be allowed under existing laws, to obtain beneficial ownership information on behalf of foreign counterparts.

3.2. The AMLC, SAs, LEAs and OGAs shall, consistent with their respective mandates, rapidly provide international cooperation in relation to information, including beneficial ownership information, on trusts and other legal arrangements. This shall include:

(a) facilitating access by foreign competent authorities to basic information held by registries or other domestic authorities;

(b) exchanging domestically available information on the trusts or other legal arrangement; and

(c) using their competent authorities' investigative powers, in accordance with domestic law, in order to obtain beneficial ownership information on behalf of foreign counterparts.

Section 4. Requirements for Request for Information from a Foreign Jurisdiction.

All RFIs from a foreign jurisdiction shall, at the minimum:

(a) state the purpose for which the information is being requested;

(b) state the relevant LEAs or OGAs, if any, for whom the information is being requested or who will ultimately use the requested information; and

(c) undertake to extend the same assistance on the basis of reciprocity or existing agreement.

Section 5. Procedure for Requests for Information from a Foreign Jurisdiction.

5.1. *Receipt of RFI.*

The AMLC shall receive requests for information:

(a) directly from a requesting jurisdiction's FIU;

(b) directly from a requesting jurisdiction's LEA or OGA to which the AMLC has an existing agreement;

(c) indirectly, through requests coursed through domestic SAs, LEAs or OGAs, if the latter cannot act on the requests in accordance with their respective charter or laws.

5.2. *Powers of the AMLC to Act on Requests for Information.*

The AMLC may execute requests for information from a foreign jurisdiction by:

(a) identifying personalities, involved in suspicious transactions, or subject of ML/TF and associated unlawful activities investigation or prosecution;

(b) tracking down assets alleged to be proceeds of or related to any unlawful activity;

(b) giving information or documents needed by the foreign jurisdiction, for intelligence or investigative purposes, within the procedures laid down in the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

5.3. *Financial Analysis, Investigation and Bank Inquiry.*

The provisions on AMLC financial analysis and investigation, and bank inquiry, shall apply to requests for information when necessary in gathering the information requested.

5.4. *Results of AMLC Action.*

Intelligence information shall be shared through a secured mechanism to be developed or adopted by the AMLC.

Section 6. RFI to a Foreign Jurisdiction.

6.1. The AMLC may request information from its foreign counterpart or non-counterpart to assist in its transnational investigation of ML/TF and associated unlawful activities.

6.2. The SAs, LEAs and OGAs may request information from their foreign counterparts or non-counterparts, as may be allowed by their respective charters or laws, to pursue investigations involving transnational elements.

Section 7. Controls and Safeguards.

7.1. The AMLC shall establish controls and safeguards to ensure that information exchanged is used only for the purpose for, and by the authorities, for which the information was requested or provided.

7.2. The SAs shall ensure that they have prior authorization from the requested foreign counterpart for any dissemination of information exchanged, or use of that information for supervisory and non-supervisory purposes, unless the concerned SA is under obligation to disclose or report the information. In such cases, at a minimum, the requesting SA shall promptly inform the requested foreign counterpart of this obligation.

Section 8. Prioritization and Monitoring.

8.1. The AMLC, SAs, LEAs, and OGAs shall have clear and secure gateways, mechanisms or channels that will facilitate and allow for the transmission and execution of requests.

8.2. The AMLC, SAs, LEAs, and OGAs shall have clear processes for the prioritization and timely execution of requests and have clear processes for safeguarding the information received

Section 9. Confidentiality of Information.

The AMLC shall maintain the confidentiality of requests for information it receives and the information exchanged, in the same manner as it would protect similar request or information received from domestic sources.

CHAPTER X
MISCELLANEOUS PROVISIONS

RULE 32 – ASSET MANAGEMENT, FEEDBACK MECHANISM AND STATISTICS

Section 1. Management of Frozen, Preserved and Forfeited Assets.

The AMLC shall establish mechanisms for managing and/or disposing preserved and forfeited assets.

Section 2. Guidelines and Feedback Mechanism.

2.1. The AMLC and SAs shall provide guidelines and feedback to assist covered persons in implementing the AMLA and TFPSA, their respective IRR and other AMLC issuances, particularly in detecting and filing STRs.

2.2. The use of the feedback mechanism shall be maximized to improve the quality and timeliness of domestic cooperation, MLA, extradition, and other forms of international cooperation.

2.3. *Requesting Feedback.*

The AMLC and the relevant SAs, LEAs and OGAs, shall request feedback from the requesting parties, including foreign counterparts and non-counterparts, on the quality, timeliness and usefulness of the assistance, cooperation or information provided.

2.4. *Providing Feedback.*

The AMLC, and the relevant SAs, LEAs and OGAs shall, as far as practicable, monitor and assess the quality, timeliness and usefulness of the assistance, cooperation or information obtained, including responses to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad, they receive from the requested parties. The AMLC and the relevant SAs, LEAs and OGAs, shall, whenever required, provide feedback to the requested parties, including foreign counterparts and non-counterparts, on the quality, timeliness and usefulness of the assistance, cooperation or information obtained.

Section 6. Statistics.

The AMLC, SAs, LEAs and OGAs, as applicable, shall maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of their AML/CTF systems. This should include keeping statistics on:

(a) CTR, STR, RTR, and other reports, received, analyzed and shared;

(b) ML/TF and associated unlawful activity investigations, prosecutions and convictions;

(c) Monetary instruments and properties frozen and forfeited; and

(d) Mutual legal assistance and other international requests for cooperation received and made.

RULE 33 – NON-INTERVENTION IN THE OPERATIONS OF THE BUREAU OF INTERNAL REVENUE

The AMLC shall not intervene or participate in the operations of the Bureau of Internal Revenue.

RULE 34 – SEPARABILITY AND REPEALING CLAUSES

Section 1. Separability Clause.

If any provision of this IRR or the application thereof to any person or circumstance is held to be invalid, the other provisions of this IRR, and the application of such provision to other persons or circumstances, shall not be affected thereby.

Section 2. Repealing Clause.

2.1. This IRR shall supersede the “2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as Amended” and all previous IRRs of the AMLA.

2.1. All AML/CTF rules, regulations, orders, circulars, guidelines, and other issuances, or parts thereof, that are inconsistent with the AMLA and TFPSA, and their respective IRR are hereby repealed, amended or modified, accordingly. *Provided*, that the penal provisions shall not apply to acts done prior to the effectivity of the AMLA on October 17, 2001.

RULE 35 – TRANSITORY PROVISION, AMENDMENT AND EFFECTIVITY CLAUSES

Section 1. Transitory Provision.

1.1. Any violation of the previous IRRs of the AMLA that is discovered during the effectivity of this IRR shall be governed by the provisions of the IRR in effect at the time of the violation.

1.2. SAs shall update their respective AML/CTF guidelines within six (6) months from effectivity of this IRR.

1.3. Covered persons shall update or formulate their respective MTPP, as follows:

(a) *For existing covered persons*: update their MTPP within one (1) year from effectivity of this IRR.

(b) *For new covered persons*: formulate their MTPP within one (1) year from issuance of license by, or registration with, their respective SAs or the relevant government agencies.

1.4. Covered persons shall register with the AMLC, as follows:

(a) *For existing covered persons who are not yet registered*: they shall not be cited for non-registration. *Provided*, that they shall apply for registration within thirty (30) working days from effectivity of this IRR.

(b) *For new covered persons*: they shall apply for registration within thirty (30) working days from issuance of license by their respective SAs or the relevant government agencies.

Section 2. Modes of Amendment.

2.1. Total repeal of this IRR shall be effected through the promulgation of a new IRR by the Council, indicating in its title the year it was promulgated.

2.2. Bullet amendments, and specific rules or guidelines of implementation of the provisions, of this IRR shall be effected through the issuance of circulars by the Council.

2.3. Non-policy amendments, including those clarificatory in nature, to the rules or guidelines of implementation of the provisions of this IRR shall be effected through the issuance of memorandum circular by the Executive Director or, in his absence, the Officer-in-Charge.

2.4. All amendments of this IRR, and specific rules or guidelines of implementation, shall be properly documented and monitored for purposes of quasi-legislative history.

2.5. All amendments of this IRR, if applicable on their nature, shall undergo the required publication in the Official Gazette or newspaper of general circulation, and filing with the Office of the National Administrative Register, University of the Philippines, Diliman, Quezon City.

Section 3. Effectivity Clause.

This IRR shall take effect immediately after the completion of its publication in the Official Gazette or in a newspaper of general circulation, and filing before the Office of the National Administrative Register, University of the Philippines, Diliman, Quezon City.

The "2018 Implementing Rules and Regulations of Republic Act No. 9160, as Amended" is hereby approved by the **ANTI-MONEY LAUNDERING COUNCIL** this 22nd day of November 2018 in the City of Manila, Philippines.

(SGD.) NESTOR A. ESPENILLA, JR.
Chairman
(Governor, Bangko Sentral ng Pilipinas)

(SGD.) EMILIO B. AQUINO
Member
(Chairman, Securities and Exchange Commission)

(SGD.) DENNIS B. FUNA
Member
(Insurance Commissioner, Insurance Commission)