AMLC REGULATORY ISSUANCE (B) NO. 1
Series of 2018

Subject: **Anti-Money Laundering/Counter-Terrorism Financing Guidelines for Designated Non-Financial Businesses and Professions**

By the authority vested upon the Anti-Money Laundering Council (AMLC) to implement measures as may be necessary and justified to counteract money laundering, in accordance with Section 7(7) of Republic Act No. 9160, also known as the Anti-Money Laundering Act of 2001, as amended, the Council, in its Resolution No. 59, dated 09 May 2018, approved the adoption of the Anti-Money Laundering/Counter-Terrorism Financing Guidelines for Designated Non-Financial Businesses and Professions.

Anti-Money Laundering/Counter-Terrorism Financing Guidelines for Designated Non-Financial Businesses and Professions

PREFACE

Republic Act (RA) No. 10365, which amended RA No. 9160 or the Anti-Money Laundering Act of 2001 (AMLA), included certain types of Designated Non-Financial Businesses and Professions (DNFBPs), as covered persons. This document is formulated in accordance with the provisions of RA No. 9160, as amended, its 2016 Revised Implementing Rules and Regulations (RIRR) and the Financial Action Task Force (FATF) 40 Recommendations and is intended to ensure that covered persons understand and comply with the requirements and obligations imposed on them.

TITLE I
GENERAL PRINCIPLES

Section 1. Policies to Combat Money Laundering and Terrorism Financing. – DNFBPs, as covered persons, are to be regulated for anti-money laundering (AML) and countering the financing of terrorism (CFT) proportionate to the nature, scale and complexity of the DNFBP's operations

in order to prevent criminals from exploiting them. While the Anti-Money Laundering Council (AMLC) is mindful of concerns to minimize unnecessary regulatory burdens and compliance costs for business, money laundering is a serious crime that threatens the competitiveness and openness of the Philippine economy. DNFBPs must therefore apply the following principles throughout their businesses:

a. Conform with high ethical standards and observe good corporate governance consistent with these Guidelines in order to protect the integrity of DNFBPs;

b. Know sufficiently their customers and clients to prevent criminal elements and suspicious individuals or entities from transacting with, or establishing or maintaining relationship with the DNFBPs;

c. Adopt and effectively implement an appropriate AML/CFT risk management system that identifies, understand, assesses, monitors, and controls risks associated with money laundering and terrorist financing (ML/TF);

d. Comply fully with existing laws and regulations aimed at combating money laundering and terrorist financing by making sure that their officers and employees are aware of their respective responsibilities and carry them out in accordance with a superior and principled culture of compliance;

e. Cooperate fully with the AMLC for the effective implementation of the AMLA, RA No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA), their respective implementing rules and regulations, and amendments thereto, and directives and guidance from the AMLC and relevant government agencies.

Section 2. Scope. – These Guidelines shall apply to the following DNFBPs:

a. Jewelry dealers, dealers in precious metals, and dealers in precious stones;

b. Company service providers which, as a business, provide any of the following services to third parties:

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 legal person or arrangement; and

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

c. Persons, including lawyers and accountants, who provide any of the following services:

1. managing of client money, securities or other assets;

2. management of bank, savings, securities or accounts;

3. organization of contributions for the creation, operation or management of companies; and

4. creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

TITLE II
DEFINITION OF TERMS

Section 3. Definition of Terms. – For purposes of these Guidelines, the following terms are hereby defined as follows:

a. Account – refers to a business relationship between a DNFBP and a customer/client.

b. Anti-Money Laundering Act (AMLA) – refers to Republic Act (RA) No. 9160, as amended by RA Nos. 9194, 10167, 10365 and 10927, or other laws that may subsequently amend the AMLA.

c. Anti-Money Laundering Council (AMLC)– refers to the financial intelligence unit of the Republic of the Philippines which is the government agency tasked to implement the AMLA.

d. Beneficial Owner – refers to any natural person who:

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

   2. Has ultimate effective control over a legal person or arrangement.

e. Covered Persons – refers to the covered persons under Rule 3(E), of the 2016 Revised Implementing Rules and Regulations of Republic Act No. 9160, as Amended.

f. Covered Transaction – refers to:

   1. A transaction involving an amount in excess of Five Hundred Thousand Pesos (Php500,000.00) or its equivalent in any other currency;

   2. A transaction exceeding One Million pesos (Php1,000,000.00) or its equivalent in any other currency, in the case of jewelry dealers, dealers in precious metals and dealers in precious stones.

g. Customer/Client – refers to any person who transacts or attempts to transact with a DNFBP.

h. 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.

i. Identification Document – refers to any of the following documents:

   1. For Filipino citizens: those issued by any of the following official authorities:

      a) Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;

b) Government-Owned or -Controlled Corporations (GOCCs); and

c) Covered persons registered with and supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), the Insurance Commission (IC) and the Securities and Exchange Commission (SEC);

2. For foreign nationals:

a) Passport; and
b) Alien Certificate of Registration; and
c) Alien Employment Permit.

j. Jewel – refers to organic substances that have a market-recognized gem level of quality, beauty and rarity, such as pearl, amber and coral.

k. 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.

l. Monetary Instrument – refers to:

1. Coins or currency of legal tender in the Philippines, or in any other country;
2. Negotiable checks, such as personal checks and bank drafts; and
3. Other similar instruments where title thereto passes to another by endorsement, assignment or delivery;

m. Politically Exposed Person (PEP) – shall be used as defined under Section 3.R of the 2016 RIRR and amendments thereto;

n. 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.

o. 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.

p. Proceeds of an Unlawful Activity – refers to anything derived or realized from an unlawful activity. It shall include:

1. All material results, profits, effects and any amount realized from any unlawful activity;

2. All monetary, financial or economic means, devices, documents, papers or things used in, or having any relation to, any unlawful activity; and

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

q. Property – refers to anything or item of value, real or personal, tangible or intangible, or any interest therein, or any benefit, privilege, claim, or right with respect thereto, including:

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

a) cash;
b) jewelry, precious metals and stones, and other similar items;
d) works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;
e) perishable goods;
f) vehicles, vessels, aircraft, or any other similar conveyance; and
g) alternative currencies, virtual currencies, cryptocurrencies, and any other digital assets.

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

    a) computers, servers, and other electronic information and communication systems; and
    b) any conveyance, including any vehicle, vessel, and aircraft.

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

    a) derived from, or traceable to, any unlawful activity; or
    b) used as an instrumentality in the commission of any unlawful activity.

r. Suspicious Transaction – shall refer to suspicious transactions as defined under paragraph (b-1), Section 3 of the AMLA.

s. Terrorism Financing – refers to those acts defined and punished under Sections 4, 5, 6, 7 and 8 of RA No. 10168.

t. Transaction refers to any act establishing any right or obligation, or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person.

u. Unlawful activity – refers to the unlawful activities under Section 3(i) of the AMLA, as amended.

Definitions of terms under the 2016 RIRR not otherwise mentioned in these Guidelines are hereby adopted and deemed incorporated herein.

TITLE III
COMPLIANCE FRAMEWORK

Section 4. Responsibilities of DNFBPs. – DNFBPs shall:

a. Establish, implement, monitor and maintain an effective Anti-Money Laundering/Counter-Financing of Terrorism (AML/CFT) Compliance Program in line with these guidelines.

b. Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential ML/TF activities such as but not limited to the following:

    1. Compliance Regime;
    2. Risk Assessment;
    3. Customer Due Diligence;
    4. Record Keeping;
    5. Training and awareness;
    6. Employee screening;
    7. Detection of suspicious transactions; and
    8. Reporting of covered and suspicious transactions.

c. Ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

d. Establish an ongoing employee training program to ensure that those employees are kept informed of new developments, including information on current Money Laundering and Terrorist Financing risks, techniques, methods and trends.

e. Carry out on a regular basis, independent review of their AML/CFT program, as provided in Section 10 hereof.

Section 5. Institutional Risk Assessment. – DNFBPs shall:

a. Take appropriate steps to identify, assess and understand its AML/CFT risks in relation to its customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk-based approach. The risk assessment shall include both quantitative and qualitative factors.

b. Institute the following processes in assessing their ML/TF risks:

    1. Documenting risk assessments and findings;
    2. Considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

3. Keeping the assessment up-to-date through periodic review; and
4. Ensure submission of the risk assessment information to the AMLC, as may be required by the AMLC.

c. Maintain AML/CFT prevention policies, procedures, processes and controls that are relevant and up-to-date in line with the dynamic risk associated with its business, products and services and that of its customers.

d. Establish, implement, monitor and maintain satisfactory controls that are commensurate with the level of AML/CFT risk; and

e. Conduct additional assessment as and when required by the AMLC.

f. Institutional risk assessment shall be conducted at least once every two (2) years or as may be determined by the AMLC.

Section 6. Risk Management Policies. – All DNFBPs shall develop sound risk management policies and practices to manage and mitigate the ML/TF risks that have been identified; monitor the implementation of those policies, controls, procedures and to enhance them if necessary; and take enhanced measures to manage and mitigate the risks where higher risks are identified.

Section 7. Active Board and Senior Management Oversight. – The DNFBP's Board of Directors or other governing body, or the partners or the sole proprietor, as the case may be, is ultimately responsible for ensuring compliance with the AMLA, its rules and regulations and directives and guidance from the AMLC.

Section 8. Designation of a Compliance Officer and/or Office. – DNFBPs shall designate a compliance officer of senior management status with the authority and mandate to ensure day-to-day compliance with its AML/CFT obligations. The compliance officer shall have a direct line of communication to the DNFBP's Board of Directors or other governing body, or the partners or the sole proprietor, as the case may be, to report on matters pertaining to its AML/CFT obligations, including the DNFBP's failure to manage ML/TF risks and new AML/CFT obligations issued in the form of circulars and correspondence from the AMLC that require updates to the DNFBPs' compliance measures. The compliance officer shall also ensure that compliance measures reflect readily available information concerning new trends in ML and TF and detection techniques.

The DNFBP shall also designate another officer to be responsible and accountable for all record keeping requirements under these Guidelines. These officers will also be responsible for making these records readily available to the AMLC upon request.

Section 9. Implementation of a Money Laundering and Terrorism Financing Prevention Program (ML/TFPP). – The DNFBP's Board of Directors, or other governing body, the partners or the sole proprietor, as the case may be, shall approve, and the compliance officer shall implement, a comprehensive, risk-based ML/TFPP geared towards the promotion of high ethical and professional standards and the prevention of ML and TF. The ML/TFPP shall be in writing, consistent with the AMLA, and its provisions shall reflect the DNFBP's corporate structure and risk profile. It shall be readily available in user-friendly form, whether in hard or soft copy. Moreover, it shall be well disseminated to all officers and staff who are obligated, given their position, to implement compliance measures. The DNFBP shall design procedures that ensure an audit trail evidencing the dissemination of the ML/TFPP to relevant officers and staff.

Where a DNFBP operates at multiple locations in the Philippines, it shall adopt an institution-wide ML/TFPP to be implemented in a consolidated manner. Lastly, the ML/TFPP shall be updated at least once every two years or whenever necessary to reflect changes in AML/CFT obligations, ML and TF trends, detection techniques and typologies.

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

a. Detailed procedures of the covered person's compliance and implementation of the following major requirements of the AMLA, and these Guidelines:

    1. customer identification process, including acceptance policies and an on-going monitoring process;
    2. record keeping and retention;
    3. covered transaction reporting; and
    4. suspicious transaction reporting, including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of future reporting of such transactions to the AMLC. Suspicious transaction reporting shall include a reporting chain under which a suspicious transaction will be processed and the designation of a Board-Level or approved Committee or designation of a senior officer who will

ultimately decide whether or not the covered institution should file a report to the AMLC;

b. An effective and continuous AML/CFT training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under the AMLA, these Guidelines and other applicable issuances, their own internal policies and procedures, and such other obligations as may be required by the AMLC;

c. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personnel with no criminal record or integrity-related issues are employed or contracted by DNFBPs;

d. An internal audit system and an independent audit program that will ensure the completeness and accuracy of information obtained from customers. The DNFBP shall specify in writing the examination scope of independent audits, which shall include ensuring checking the accuracy and completeness of identification documents, covered transaction report (CTR) and suspicious transaction report (STR) submitted to the AMLC, and records retained in compliance with this framework, as well as assuring adequacy and effectiveness of the DNFBP's training programs;

e. A mechanism that ensures all deficiencies noted during the audit and/or regular or special inspection/examination are immediately corrected and acted upon;

f. Cooperation with the AMLC;

g. Designation of a Compliance Officer, who shall, at least, be of senior management level, as the lead implementer of the DNFBP's compliance program; and

h. The identification, assessment and mitigation of ML/TF risks that may arise from new business practices, services, technologies and products.

Within ninety (90) days from the effectivity of these Guidelines, all DNFBPs shall prepare and have available for inspection an updated ML/TFPP embodying the principles and provisions stated in these Guidelines. The compliance officer shall submit to the AMLC a sworn

certification that a new ML/TFPP has been prepared, duly noted and approved by the DNFBP's Board of Directors or other governing body.

Section 10. Internal Controls and Internal Audit Program. – The DNFBP shall establish internal controls to ensure day-to-day compliance with its AML/CFT obligations under the AMLA, these Guidelines, and other applicable issuances, taking into consideration the size and complexity of the its operations.

Qualified personnel who are independent of the unit being audited shall conduct internal audits for DNFBPs. The auditors shall have the support and a direct line of communication to the DNFBP's Board of Directors, or other governing body the partners or the sole proprietor, as the case may be. The DNFBP's internal audit program shall include periodic and independent evaluation of the DNFBP's risk management, as well as the sufficiency and degree of adherence to its compliance measures. Internal audit examination scope shall cover the accuracy of customer identification information, covered and suspicious transaction reports, and all other records and internal controls pertaining to compliance with AML/CFT obligations. Internal audits shall be conducted at least once every two (2) years or at such frequency as necessary, consistent with the risk assessment of the DNFBPs.

The results of the internal audit shall be timely and directly communicated to both the DNFBP's Board of Directors or senior management, or the partners or the sole proprietor, as the case may be, and the compliance officer. There shall also be a written procedure by which deficiencies in a compliance program are promptly remedied once identified by an internal audit. Moreover, audit results relative to AML/CFT compliance shall promptly be made available to the AMLC upon request.

The findings of the internal audit shall be periodically assessed by an independent third-party auditor accredited by the AMLC.

Section 11. Customer Due Diligence. – DNFBPs shall adopt a policy that before a business relationship is established, it should take steps to identify its customers and verify his/her identity on the basis of documents, data and information obtained from the customer and from reliable independent sources, and obtain information that should enable them to assess the extent of risk to which the customer may expose them.

Section 12. Monitoring and Reporting System. – All DNFBPs shall adopt an ML/TF monitoring system, including a name screening mechanism, whether electronic or manual, that is appropriate for their risk-profile and business complexity in accordance with these Guidelines. The system shall be capable of generating timely, accurate and complete reports, including

CTRs and STRs, and to regularly apprise the DNFBP's Board of Directors, or other governing body, the partners or the sole proprietor, as the case may be on AML and CFT compliance.

Section 13. Record Keeping. – All DNFBPs shall adopt a policy to keep records of their customer's/client's transactions and documents obtained during the customer due diligence for five (5) years.

Section 14. Employee Training Program. – DNFBPs shall create employee training programs that detail ML and TF prevention roles and hiring standards that promote high ethical standards in order to protect the safety and integrity of the DNFBP's business.

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

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

Section 15. Investigative, Administrative and Judicial Compliance. - DNFBPs shall have written procedures for cooperating and complying with investigations, assessments, directives and orders of the AMLC, the appropriate government agencies and the courts, as the case may be. When the DNFBP receives a request for information from any competent authority regarding inquiries into potential ML or TF activity carried on, the DNFBP shall promptly inform the AMLC in writing.

Section 16. New Products and Business Practices. – DNFBPs are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

TITLE IV
CUSTOMER DUE DILIGENCE

Section 17. Customer Due Diligence (CDD). – DNFBPs shall know their customers and, to the extent possible, the intermediary and the person or entity on whose behalf the transaction is being conducted. DNFBPs shall create a system that will first establish and then record the full identity of their customers and risk assessment results. In addition to using all information available to them, DNFBPs shall require customers to furnish the required Identification Documents.

Section 18. Risk-Based CDD Standards. – Consistent with all AML/CFT compliance measures, a DNFBP's CDD procedures shall be risk-based, requiring enhanced diligence for customers posing a high-risk of ML/TF and permitting reduced due diligence for customers posing a low-risk of ML/TF. DNFBPs shall therefore document clear policies and procedures, including guidelines and criteria for determining which customers pose low, normal, or high risk of ML and TF. A DNFBP's internal risk classifications shall reflect the idiosyncratic risks to its operations, requiring an intimate knowledge of the risks inherent to their operations and the acquisition of relevant expertise to make such risk assessments.

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

Section 19. When to Conduct CDD. – DNFBPs shall undertake satisfactory CDD measures when:

a. Establishing business relationship;
b. There is any suspicion of Money Laundering or Terrorist Financing; and
c. The DNFBP has doubts about the integrity or adequacy of previously obtained client identification information.

Provided, that where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, the DNFBP may complete verification after the establishment of business relationship so as not to interrupt normal conduct of business. The verification, however, should be undertaken

not later than five (5) working days or any other period as may be specified by the AMLC.

Section 20. CDD Standards. – DNFBPs shall implement the following standards of CDD. –

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

Section 21. Customer Identification. – DNFBPs shall establish appropriate systems and methods, and adequate internal controls, compliant with the AMLA, these Guidelines, and other AMLC issuances for verifying and recording the true and full identity of their customers based on reliable, independent sources, documents, data or information, as defined under Section 3.i of these Guidelines, upon establishment of a business relationship. In the case of corporate customers, including a trustee, agent, nominee, or intermediary arrangements, DNFBPs are required to maintain a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf.

Section 22. Minimum Customer Information and Identification Documents when Conducting Customer Due Diligence. – The following are the minimum customer information and identification documents required in the conduct of CDD:

A. For Individual Persons:

1. Name of customer;
2. Date and place of birth;
3. Present address;
4. Permanent address;
5. Contact number or information, if any;
6. Nationality;

7. Proof of Identification and Identification Number;
8. Nature of work, name of employer or nature of self-employment/business; and

Customers who transact business with a DNFBP shall be required to submit a copy of an identification document.

Provided that the absence of any of the foregoing information shall not be considered a violation of this provision so long as the identity of the customer is sufficiently known by the presence of the other identifying information and the covered person is able to risk profile the customer.

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

B. For Juridical Persons/Sole Proprietorships

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

    a. Certificates of registration issued by the Department of Trade and Industry (DTI) for single proprietors; and the SEC for corporations and partnerships;
    b. Articles of incorporation or association and the entity's by-laws;

c. A resolution by the ownership (board of directors or other governing body, partners, sole proprietor, etc.), authorizing the signatory to sign on behalf of the entity;
d. A list of names and identification documents of the owners, partners, directors, principal officers, authorized signatories and stockholders owning at least 20% of the business or outstanding capital stock, as the case may be.

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

DNFBPs should be able to understand the nature of the customer's/client's business, its ownership and control structure.

C. Legal Arrangements

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

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

2. For other types of legal arrangements, the identity of persons in equivalent or similar positions.

DNFBPs should be able to understand the nature of the customer's/client's business, its ownership and control structure.

Section 23. Identification and Verification of a Beneficial Owner, Trustee, Nominee, or Agent. – The DNFBPs shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of due diligence to be applied to both. In case it entertains doubts as to whether the account holder or transactor is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence or file a suspicious transaction report, if warranted.

Section 24. Customer Risk Assessment. - DNFBPs shall develop clear, written and graduated customer acceptance policies and procedures,

including a set of criteria for customers that are likely to pose low, normal, or high risk to their operations. The criteria may include:

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

DNFBPs or the AMLC shall set the standards in applying reduced, normal, and enhanced customer due diligence, including a set of conditions for the refusal to conduct the transaction.

Section 25. High-Risk Customers. – High-risk customers include those that originate from a country that is recognized as having inadequate, internationally-accepted anti-money laundering standards; does not sufficiently regulate businesses to counteract money-laundering; fails to incorporate Financial Action Task Force (FATF) recommendations into its regulatory regimes; or exhibits a relatively high prevalence or risk of crime, corruption, or terrorist financing. In making these determinations, DNFBPs should consult information from the websites of FATF; the Asia Pacific Group on Money Laundering; the Egmont Group; national authorities on money laundering, including domestic agencies like the AMLC and foreign agencies like the United States' Financial Crimes Enforcement Network; and other reliable regulators or expert sources on money laundering. High-risk customers also include shell companies and their beneficial owners.

Section 26. Enhanced Due Diligence (EDD). – A DNFBP should employ EDD if it acquires information that:

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

b. Justifies re-classification of the customer from low or normal risk to high-risk;

c. When establishing business relationship with any person from countries identified by the FATF or AMLC as having on-going or substantial ML/TF risks.

d. Warrants the filing of a Suspicious Transaction Report (STR) exists, including information that:

    1. The customer is transacting without any purpose, economic justification, or underlying legal or trade obligation; purpose, or economic justification;

    2. The customer is transacting an amount that is not commensurate to the business or financial capacity of the customer or deviates from the profile of that customer;

    3. The customer might have structured transactions to avoid being the subject of a Covered Transaction Report;

    4. The customer has been or is currently engaged in any unlawful activity; or

    5. Raises suspicions that an intermediary is being used to circumvent anti-money laundering compliance measures.

Commencing an account or business relationship with a high-risk customer shall require approval from a senior or management level officer in the DNFBP. For individual high-risk persons, EDD will include obtaining additional information on the customer and beneficial owner, including, but not limited to: list of banks where the customer or beneficial owner has maintained or is maintaining an account; a list of companies in which he is a director, officer, or stockholder; the specific services the customer is seeking to avail; and the source of wealth and funds. For juridical persons, EDD will include obtaining a list of banks where the entity has maintained or is maintaining an account; the verified name, nationality, present address, date and place of birth, nature of work, and sources of assets of the primary officers of the entity (i.e. President, Treasurer, authorized signatories, etc.), directors, trustees, partners, as well as all stockholders owning five percent (5%) or more of the business or voting stock of the entity, as the case may be.

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

A DNFBP shall make appropriate use of relevant findings issued by the AMLC concerning any named individuals, groups or entities that are the subject of money laundering or terrorist financing investigations or included in sanctions lists issued by international competent authorities. Regarding various individuals and entities, the DNFBP shall know prior to establishing a customer relationship:

a. The identity of the person;
b. The type of activity/relationship he/she wants to conduct with the DNFBP;
c. The complexity of the transaction;
d. Whether or not the customer is representing a third party; and
e. How to verify the information presented.

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

Section 27. Ongoing Monitoring of Customers, Accounts and Transactions. - DNFBPs are required to conduct on-going due diligence on the business relationship with its customers/clients.

a. DNFBPs shall scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with their knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

b. ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

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

Section 28. Ongoing CDD and Monitoring of Existing Clients. – DNFBPs shall, on the basis of materiality and risk, update all customer information and identification documents of existing customers required to

be obtained under the AMLA, these Guidelines, and other applicable issuances of the AMLC.

a. The customer's documentation standards are changed substantially with the introduction of compliance requirements with these guidelines; or

b. There is a material change in the nature of the relationship with the customer; or

c. The DNFBP becomes aware that it lacks sufficient information about an existing customer or is concerned about the accuracy of information recorded.

DNFBPs should have a system that will enable them to understand the normal and reasonable account activity of their customers

Section 29. Face-to-Face Contact. – DNFBPs shall conduct face-to-face contact at the time of establishment of the business relationship, or as reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business and the risks involved; provided that ML and TF risks are effectively managed. Provided further, that no transaction shall be processed without conducting a face-to-face contact.

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

Section 30. Third Party Reliance. – DNFBPs may rely on a third party to perform customer identification and face-to-face contact. The third party shall be:

a. a covered person as defined under Section 3 (A) of the AMLA; or

b. a financial institution or DNFBP operating outside the Philippines that is covered by equivalent customer identification and face-to-face requirements.

Notwithstanding the foregoing, the ultimate responsibility and accountability for identifying the customer and conducting CDD remains with the DNFBP relying on the third party. Provided that, in cases of high-

risk customers, the DNFBP relying on the third person shall also conduct enhanced due diligence procedure.

Section 31. Outsourcing the Conduct of Customer Identification and Due Diligence. – DNFBPs may outsource the conduct of customer identification and due diligence, including face-to-face contact, to a counterparty, intermediary or agent. The customer identification and due diligence performed by the counterparty or intermediary shall be regarded as those of the DNFBP itself. The ultimate responsibility and accountability for identifying the customer and keeping the identification documents remains with the DNFBP.

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

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

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

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

The counterparty, intermediary or agent in performing the conduct of customer identification and due diligence, as a minimum, must comply with the requirements provided under the AMLA and these guidelines.

Section 32. Politically Exposed Persons. – In addition to establishing the full identities of PEPs, DNFBPs shall also establish and record the identities of the immediate family members and entities if publicly known to be related to the PEP. DNFBPs shall carefully consider a PEP's position and the position's attendant risks with respect to money laundering and terrorist financing in determining what standard of due diligence shall apply to them.

Section 33. Customer Acceptance Policies. – DNFBPs shall have clear, written and graduated acceptance policies and procedures that will seek to prevent suspicious individuals or entities from transacting with, establishing or maintaining business relationship with them. DNFBPs shall develop guidelines to assist personnel to assess whether a customer's profile warrants refusal of service to protect the security and integrity of the business.

Section 34. Customer Refusal Policies. – DNFBPs should have written guidelines on when a customer's risk profile warrants refusal of service to protect the security and integrity of the DNFBP's business. Thus, if the prospective customer is unable to comply with any of the CDD measures, the DNFBP shall not commence business relations, accept instructions or perform any transaction. If necessary, the DNFBP should file an STR.

Section 35. Prohibited Accounts. – Anonymous accounts and accounts under fictitious names shall be prohibited, and DNFBPs shall maintain customers' account only in the true and full name of the account owner or holder.

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

Section 36. Termination of Business Relationship. – Where CDD obligations for existing business relationships and clients are not met, as a result of the client's refusal to comply or where the client causes unacceptable delays, the DNFBP shall terminate the business relationship and consider the filing of Suspicious Transaction Report (STR) to the AMLC.

Section 37. Tipping Off – In case where the DNFBP forms a suspicion of ML/TF and reasonably believes that performing CDD process would tip off the customer, the DNFBP is permitted not to pursue the CDD process. In such circumstances, the DNFBP may proceed with the transaction and immediately file a Suspicious Transaction Report.

TITLE V
RECORD KEEPING

Section 38. Record Keeping Management and Requirements. – DNFBPs shall maintain records in an organized and confidential manner, which allows the AMLC and the courts to establish an audit trail for money

laundering and terrorism financing, and in such forms as are admissible in court.

Section 39. Period to Keep Records. – A DNFBP shall maintain and safely store for five (5) years from the dates of transactions all records of customer identification and transaction documents, or as long as the business relationship exists. If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5)-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

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

Section 40. Records of Information on Covered and Suspicious Transaction Reports (CTRs and STRs). – DNFBPs shall maintain records concerning its internal reporting of CTRs and STRs, and decision-making whether to file or not to file said reports with the AMLC, for at least a period of five (5) years after the date of transaction.

Section 41. Access to Data. – A DNFBP is advised to ensure that there are no secrecy or data protection issues that would restrict prompt access to data, or impede the full application of these Guidelines with respect to any outsourced relationship.

TITLE VI
COVERED AND SUSPICIOUS TRANSACTION REPORTING

Section 42. Reporting of Covered and Suspicious Transactions. – DNFBPs shall report to the AMLC all covered transactions and suspicious transactions within five (5) working days from the occurrence thereof. For suspicious transactions, "*occurrence*" refers to the date of determination of the suspicious nature of the transaction, which determination shall be made not exceeding ten (10) calendar days from date of transaction.

In cases where the transaction is in any way related to an unlawful activity, or the person transacting is involved in or connected to an unlawful activity or money laundering offense, the ten (10) calendar day determination period shall be reckoned from the date the covered person knew of, or should have known, the suspicious transaction indicator. To determine whether the covered persons knew or should have known the suspicious transaction indicator, it shall be given a reasonable period of time,

which in no case shall exceed sixty (60) calendar days, to gather facts in order to enable the submission of a meaningful STR.

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

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

Section 43. Guidelines in Reporting of Covered and Suspicious Transactions. – The filing of CTRs and STRs shall otherwise be in accordance with the AMLC Registration and Reporting Guidelines (ARRG) issued by the AMLC.

Section 44. STR Framework. – DNFBPs shall observe the following rules in reporting suspicious transactions:

a. A DNFBP shall have relevant policies, procedures, processes and controls in place that would enable an employee to report to the Compliance Officer any suspicion or knowledge of ML or TF activity and/or transaction that is detected or identified;

b. If a DNFBP suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity or are related to Money Laundering or Terrorist Financing, the Compliance Officer shall promptly file an STR with the AMLC as provided for under the AML/CFT Reporting Guidelines for DNFBPs;

c. The Compliance Officer shall ensure that every employee is aware of his role and duty to receive or submit internal STRs;

d. The Compliance Officer shall investigate STRs internally, build an internal report outlining the outcome of his investigation including the decision on whether or not to file an STR with the AMLC;

e. Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing;

f. In the event the Compliance Officer concludes that no external report should be submitted to the AMLC, the justification of such a decision should be documented;

g. A DNFBP shall institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there is evidence for him/her to do so; and

h. DNFBPs shall monitor indicators of suspicious activities, such as, but not limited to, those listed in **Annex A** hereof, and perform EDD as necessary.

Section 45. Confidentiality of Reporting - When reporting covered or suspicious transactions, DNFBPs, 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.

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

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

Section 46. Safe Harbor Provision. - No administrative, criminal or civil proceedings shall lie against any person for having made a covered transaction or suspicious transaction report in the regular performance of his/her duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law.

Section 47. Exemption from Reporting. - Notwithstanding the foregoing, 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, shall not be deemed covered persons. Thus, they are not required for file a CTR or STR.

Lawyers and accountants, however, are not precluded from reporting to the AMLC in utmost confidentiality any knowledge or information that their client is committing or otherwise contemplating to commit money laundering or terrorism financing, or such information outside the coverage

of the rules on privileged communication. For this purpose, the AMLC shall accept electronic or paper-based submission.

TITLE VII
REGISTRATION

Section 48. Registration with the AMLC. – All DNFBPs shall register with the AMLC. The following documents shall be submitted/uploaded to the AMLC through its portal designated for the purpose:

a. Application letter expressing an intention to register as a DNFBP;
b. Business model, including target markets and customers;
c. List of owners/controlling stockholders, partners, directors and principal officers;
d. Copy of business registration/permit from the city/municipality currently having jurisdiction over the place of establishment and operation of the office;
e. Duly authenticated incorporation from the Securities and Exchange Commission (SEC), certificate of registration from the Department of Trade and Industry (DTI); or proof of registration with the Cooperative Development Authority (CDA);
f. Notarized Deeds of Undertaking of the entity, signed by the proprietor/partners/president/directors (attached to these Guidelines as **Annexes B** and **C**, respectively);
g. List of operating office locations;
h. Audited financial statements where applicable;
i. Proof of attendance of the proprietor / partners / directors / principal officers in an AML seminar; and
j. Clearance from the National Bureau of Investigation (NBI) or its equivalent in a foreign jurisdiction, of all directors and principal officers.

Section 49. Certificate of Registration. – The AMLC shall issue a Certificate of Registration upon determination of complete submission of documentary requirements mentioned in the preceding Section.

Section 50 Denial of Registration with the AMLC. – The AMLC may deny registration if the DNFBP fails to provide accurate or complete registration requirements.

Section 51. Period of Registration with the AMLC. – All existing DNFBPs shall register with the AMLC within six (6) months from effectivity

of these Guidelines, or, in the case of newly-established DNFBPs, registration must be done before the commencement of operation.

Section 52. Notification Requirements. – DNFBPs shall inform AMLC the occurrence of the following:

a. **At the commencement of operations**—The DNFBP shall notify AMLC within five (5) business days from the start of operations of each individual office of the DNFBP.

b. **Transfer of location**— The DNFBP shall notify AMLC within five (5) business days from the actual date of transfer.

c. **Closure of office**— The DNFBP shall notify AMLC within five (5) business days from the actual date of closure.

d. **Closure of business**— The DNFBP shall notify AMLC within five (5) business days from the actual date of closure. It shall also submit:

    1. A certification by the ownership attesting to the closure of the DNFBP; and

    2. The original copy of AMLC Certificate of Registration (COR).

e. **Change of name**—The DNFBP shall notify AMLC before the change of name takes effect. It shall also submit:

    1. A COR from the DTI, SEC, or Cooperative Development Authority, indicating the new business/registered name; and

    2. Original copy of AML COR issued under the old name. The AMLC will then issue a new COR indicating the new registered name.

f. **Change of ownership or control**—The DNFBP shall notify AMLC before the change of ownership or control takes effect. Change of ownership or control shall refer to any transaction involving the transfer of equity that will result in ownership or control of at least twenty percent (20%) of the assets or voting shares of stock, as the case may be, of the DNFBP by any person, whether natural or juridical, or any transfer of interest or equity, which will enable the buyers to elect or to be elected as, a director or officer of equivalent power or authority.

TITLE VIII
COMPLIANCE CHECKING AND INVESTIGATION BY THE AMLC AND/OR SELF-REGULATING AUTHORITY

Section 53. Authority to Check Compliance and Conduct Investigation. – Pursuant to Section 7(5)(7) of the AMLA, the AMLC shall have the authority to conduct compliance checking and investigation, as follows:

A. COMPLIANCE CHECKING

1. The AMLC and its Secretariat shall have the authority to conduct on-site compliance checking with at least twenty-four (24)-hours' prior notice, to validate the compliance of DNFBPs with the requirements of the AMLA, as amended, its implementing rules, these guidelines, and other AMLC issuances.

2. DNFBPs shall make available all documents including the customer identification documents, CTRs and STRS, and their respective MLPPs upon request by the AMLC.

B. INVESTIGATION

1. The AMLC shall investigate suspicious and covered transactions deemed suspicious, ML and TF activities, and other violations of the AMLA, its implementing rules and regulations, these Guidelines and other AMLC issuances.

   In the exercise of its investigative function, the AMLC and its Secretariat may perform the following in accordance with law:

   a. Direct DNFBPs to produce information, documents and objects, including video footages, clippings, recordings, and electronic data, necessary to determine the true identity of persons subject of investigation;

   b. Require responsible officers and employees of DNFBPs to give statements pertinent to transactions, persons or violations being investigated; and

   c. Request information, documents and objects from domestic government agencies; foreign states, including their financial intelligence units, law enforcement agencies, and financial regulators; or the United Nations and other international organizations and entities.

2. DNFBPs shall, in accordance with the AMLA, its implementing rules and regulations, issuances of the AMLC, and other laws and regulations, immediately provide authorized personnel of the AMLC and its Secretariat, full access to all information, documents or objects pertaining to the account, customer, transaction or violation subject of investigation.

   Certified true copies of the documents pertaining to the foregoing shall be submitted within five (5) working days from receipt of the request or order from the AMLC.

TITLE IX
INQUIRY, FREEZING AND FORFEITURE OF MONETARY INSTRUMENT OR PROPERTY

Section 54. Authority to Examine Customer's Transactions. – The AMLC and its Secretariat may examine all transactions of any customer, including related accounts with DNFBPs that are deemed related to any unlawful activity/predicate offense or money laundering offense as defined in these Guidelines, the AMLA, and its implementing rules and regulations, or the Terrorism Financing Law.

Section 55. Freezing and Forfeiture of Monetary Instruments or Properties. - The freezing or forfeiture of funds, monetary instruments or properties shall be governed by the AMLA, its implementing rules and prospective issuances of the AMLC. DNFBPs shall not lift the effects of any freeze order without seeking official confirmation from the AMLC.

Section 56. Rules of Procedure. – Proceedings for issuance of freeze order, and provisional asset preservation order or asset preservation 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 (AM No. 05-11-04-SC), or amendments thereto.

TITLE X
ENFORCEMENT ACTIONS

Section 57. Enforcement and Administrative Actions. – Pursuant to Sections 7(7), (11), and 14(f) of the AMLA, as amended, and the Rules on the Imposition of Administrative Sanctions, the AMLC may impose administrative sanctions, including monetary fines, on DNFBPs for violations of the AMLA, its implementing rules and regulations, and all other prospective issuances of the AMLC.

TITLE XI
MISCELLANEOUS PROVISIONS

Section 58. Separability Clause. – If any provision of these Guidelines is declared unconstitutional, the same shall not affect the validity and effectivity of other provisions hereof.

Section 59. Effectivity. – These Guidelines shall take effect fifteen (15) days following its publication in a newspaper of general circulation.

FOR THE AMLC:

MEL GEORGIE B. RACELA
Executive Director
AMLC Secretariat

10 May 2018

Annex A

Indicators of Suspicious Activity.

a. For jewelry dealers in precious stones and metals:

1. When the customer purchases items of high value without selecting any particular specifications or with no clear justification;

2. When the customer's purchases items of high value do not correspond with what is expected from him upon the identification of his profession or the nature of his business;

3. When the customer regularly purchases high value commodities or large quantities of a specific commodity in a way that does not suit the usual deals carried out by the customer or the usual pattern of the business for his income or appearance;

4. When the customer attempts to recover the amount of new purchases without a satisfactory explanation or when the customer tries to sell what he recently bought at a price that is much less than the purchasing price;

5. When the customer attempts to sell items of high value at a price much less than their actual or market value;

6. When the customer is willing to pay any price to obtain jewels of extravagant amounts without any attempt to reduce or negotiate the price; and

7. When the customer engages in any cash transactions equal to or above Php750,000.00 or its equivalent in foreign currency.

b. For persons, including lawyers and accountants, who provide the services mentioned in Section 2.d of the Guidelines:

1. When the customer appoints a lawyer in financial or commercial transactions and requests the concealment of the customer's name in any of these transactions;

2. When the customer resorts to lawyers to create companies, particularly international business companies, from outside the

country (offshore) in a way that shows that the objective of creating the company is to conceal the illicit source of the funds;

3. When the customer resorts to lawyers to invest in the real estate market but the purchase or sale prices are not commensurate with the real estate value;

4. When the customer requests, upon hiring a lawyer to incorporate a company, to transfer/deposit the incorporation fees or the capital to/in the bank account of the lawyer through multiple accounts that he has no relation to without a reasonable justification;

5. When the lawyer manages investments portfolios, in countries allowing such conduct, and receives instructions from the customer to make buying and selling transactions that have no clear economic reason;

6. When customers desire to create or buy a company that has a suspicious objective, does not realize profits or does not seem to be connected to his/her usual profession or related activities, without being able to submit sufficient explanations to the notary;

7. When a customer sells assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect;

8. When the customer who creates or wishes to create different companies in a short timeframe for his own interest or the interest of other persons, without reasonable financial, legal or commercial grounds;

9. When the customer uses another person as a facade to complete a transaction without any legitimate financial, legal or commercial excuse;

10. When the customer does not indicate concern in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business, or when the customer remains persistent in pursuing his activities;

11. When the volume of foreign transfers from/to the client's accounts is high or when the sudden increase of the revenue and cash amounts he obtains is not consistent with his usual income and this activity lacks justification;

12. When the customer receives cash money or high value checks, which do not suit the volume of his/her work or the nature of his/her activity, particularly if the transactions come from persons who are not clearly or justifiably connected to the client.

13. When unjustified amounts in or deposits to the customer's account whose origin or cause is difficult to identify are made;

14. When the customer transacts disproportionate amounts, and the frequency and nature of his transactions are not consistent with the nature of his business, profession or known and declared activity, particularly if these transactions are carried out with suspicious countries that are not connected to his apparent business domain; and

15. When cash transactions in large amounts, including foreign exchange transactions or cross-border fund movement, if such types of transactions are not consistent with the usual commercial activity of the customer.

c. For all Designated Non-Financial Businesses and Professions (DNFBPs):

1. When the customer has an unusually comprehensive knowledge of money laundering and terrorism financing issues and the AMLA, and the Terrorism Financing Law without any justification, as when the customer points out he wishes to avoid being reported;

2. When the customer attempts to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities regarding ML and TF suspicions;

3. When the customer has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a transaction;

4. When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT regime;

5. When the customer is reserved, anxious or reluctant to have a personal meeting;

6. When the customer uses different names and addresses;

7. When the customer requests or seeks to carry out the transactions without disclosing his identity;

8. When the customer refuses to submit original documentation particularly those related to his identification;

9. When the customer intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number;

10. When the customer uses a credit card issued by a foreign bank that has no branch or headquarters in the country of residence of the client while he does not reside or work in the country that issued said card;

11. When the customer conducts cash transactions where banknotes with unusual denominations are used;

12. When the customer conducts unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the customer;

13. When the customer conducts unnecessarily complex transactions or those that may not be economically feasible; and

14. When the customer's transaction involves a country that does not have an efficient AML/CFT regime, or is suspected to facilitate ML or TF operations. or where drug manufacturing or trafficking are widespread.

ANNEX B

Name of Applicant/Entity: _____

Address: _____

Tel. No.: _____ Fax No. _____ TIN: _____

DEED OF UNDERTAKING

I, _____ (name and designation), of legal age, and under oath, hereby abide to comply with the following requirements:

1. That I have been duly authorized by _____ (name of institution/business) and its Board of Directors/Partners/Owners to bind _____ (name of Designated Non-Financial Business or Profession [DNFBP]) to strictly comply with all the requirements, rules and regulations of the Anti-Money Laundering Council (AMLC) regarding the registration and operations of Designated Non-Financial Businesses and Professions (DNFBPs), and those issued by the appropriate regulatory, supervisory or professional authority over _____ (name of institution/proprietor).

2. That I certify that _____ (name of institution/business) undertakes to strictly comply with all the requirements, rules and regulations of the AMLC including those on registration, customer due diligence, record keeping and reporting of covered and suspicious transactions;

3. I/We shall notify the AMLC of the following events:

   (a) commencement of operations;

   (b) change of ownership; partners; officers and directors, and ownership of at least twenty percent (20%) of the outstanding capital stock;

   (c) transfer of location;

(d) closure of office; and

(e) closure of business;

4. I/we shall maintain an internal control system commensurate to the nature, size and complexity of the business and shall adhere to the guidelines prescribed by the AMLC.

_____
(Signature over printed name)

_____
(Designation)

SUBSCRIBED AND SWORN TO before me this _____ day of _____ 20____ affiant exhibiting to me his/her _____ issued at _____ on _____.

_____
(NOTARY PUBLIC)

Doc. No. _____
Page No. _____
Book No. _____
Series of 20__.

ANNEX C

Name of Owner, Partner or Director: _____

Address: _____

Tel. No.: _____ Fax No. _____ TIN: _____

DEED OF UNDERTAKING

I, _____ (name and designation), of legal age, and under oath, hereby abide to comply with the following requirements:

1. That I certify that I shall be responsible for any violation of any of the provisions of the Anti-Money Laundering Act of 2001 (Republic Act No. 9160), as amended, and its implementing rules and regulations, and any other directive, guidelines or other issuance of the Anti-Money Laundering Council; and other applicable laws, rules and regulations; and

2. I shall attend the required seminar on the Anti-Money Laundering Act of 2001, as amended, before commencement, continuance or resumption of actual operations.

_____
(Signature over printed name)

_____
(Designation)

SUBSCRIBED AND SWORN TO before me this _____ day of _____ 20____ affiant exhibiting to me his/her _____ issued at _____ on _____.

_____
(NOTARY PUBLIC)

Doc. No. _____
Page No. _____
Book No. _____
Series of 20__.