

# ANTI-MONEY LAUNDERING (AML) AND COMBATTING THE FINANCING OF TERRORISM (CFT) REGULATIONS

Updated as of 31 December 2023

BANGKO SENTRAL AUTHORITY TO CHECK COMPLIANCE WITH THE AMLA, AS AMENDED .....	2
POLICY STATEMENT .....	2
SCOPE OF REGULATIONS .....	2
DEFINITION OF TERMS .....	3
BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING.....	10
<b>RISK MANAGEMENT</b>	
RISK MANAGEMENT .....	11
<b>PREVENTIVE MEASURES</b>	
CUSTOMER DUE DILIGENCE.....	15
COVERED AND SUSPICIOUS TRANSACTION REPORTING .....	29
ADDITIONAL PREVENTIVE MEASURES FOR SPECIFIC CUSTOMERS AND ACTIVITIES.....	31
RECORD KEEPING .....	35
<b>TRAINING PROGRAM</b>	
AML TRAINING PROGRAM.....	36
<b>ENFORCEMENT ACTIONS</b>	
SANCTIONS AND PENALTIES .....	37
SEPARABILITY CLAUSE .....	39

## ANTI-MONEY LAUNDERING (AML) AND COMBATTING THE FINANCING OF TERRORISM (CFT) REGULATIONS

### 901 BANGKO SENTRAL AUTHORITY TO CHECK COMPLIANCE WITH THE ANTI-MONEY LAUNDERING ACT (AMLA), AS AMENDED

In the course of a periodic or special examination, the Bangko Sentral may inquire into or examine bank accounts or investments, including customer identification, account opening, and transaction documents, for the purpose of checking compliance by covered persons under its supervision or regulation with the requirements of these rules, the AMLA, as amended, and the Terrorism Financing Prevention and Suppression Act (TFPSA), their respective Revised Implementing Rules and Regulations (RIRR), other Anti-Money Laundering Council (AMLC), and Bangko Sentral issuances.

The Bangko Sentral may likewise conduct annual testing solely limited to the determination of the existence and true identity of the owners of numbered and similar accounts.

In the course of the periodic and special examination for purposes of complying with the provisions of the AMLA, as amended, its RIRR, and this Part, the covered person, their officers and employees, and the Bangko Sentral, shall not be deemed to have violated the provisions of R. A. No. 1405, as amended, R.A. No. 6426, as amended, R.A. No. 8791 and other similar laws, and Sec. 922 (*Confidentiality provision*) when disclosing information to Bangko Sentral relative to covered and suspicious transaction reports filed with the AMLC.

### 902 POLICY STATEMENT

The Bangko Sentral adopts the policies of the State to (a) protect and preserve the integrity of the Philippine financial system, including the confidentiality of bank accounts; (b) ensure that the Philippines, in general, and the covered persons, in particular, shall not be used as money laundering sites and conduit for the proceeds of unlawful activities as herein defined; (c) protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it and reinforce the fight against terrorism by criminalizing the financing of terrorism and related offenses; (d) recognize terrorism and terrorist financing as inimical and dangerous to national security and the welfare of the people; and make the financing of terrorism a crime against the Filipino people, against humanity and against the law of nations; and (e) adhere to international commitments to combat financing of terrorism, specifically 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.

### 903 SCOPE OF REGULATIONS

These regulations shall apply to all covered persons supervised and regulated by the Bangko Sentral. The term “covered persons” shall refer to banks, non-banks, QBs, trust entities, NSSLAs, pawnshops, foreign exchange dealers, money changers, remittance and transfer companies, EMLs and other financial institutions which under special laws are subject to Bangko Sentral supervision and/or regulation, including their subsidiaries and affiliates, which are also covered persons, wherever they may be located. For this purpose, subsidiary and affiliate shall be defined as:

- a. A *subsidiary* means an entity more than fifty percent (50%) of the outstanding voting stock of which is owned by a covered person.
- b. An *affiliate* means an entity the voting stock of which, at least twenty percent (20%) to not more than fifty percent (50%), is owned by a covered person.

Pursuant to Section 20 of the General Banking Law of 2000, a bank authorized by Bangko Sentral to establish branches or other offices within or outside the Philippines shall be responsible for all business conducted in such branches and offices to the same extent and in the same manner as though such business had all been conducted in the head office. A bank and its branches and offices shall be treated as one (1) unit.

If the host country does not permit the proper implementation of this Part or any of the provisions of the AMLA, as amended, the TFPSA, or their Implementing Rules and Regulations (IRR), and other AMLC and Bangko Sentral issuances by reason of local laws, regulations or a supervisory directive, the covered person shall (1) formally notify the Bangko Sentral of this situation and furnish a copy of the applicable laws and/or regulations or the supervising

authority's directive, as the case may be; and (2) apply appropriate additional measures or mitigating controls to manage the ML and TF risks.

In cases where the minimum AML/CFT requirements of the host country are less strict, covered persons, including their foreign branches and majority-owned subsidiaries abroad, shall apply AML/CFT measures consistent with the AMLA and the TFPSA and their respective RIRR, and other AMLC and Bangko Sentral issuances, to the extent that the laws and regulations of the host country permit.

#### 904 DEFINITION OF TERMS

Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the AMLA, as amended, targeted financial sanctions (TFS)-related laws and their respective IRR.

- a. *Money laundering* is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:
- (1) transacts said monetary instrument or property;
  - (2) converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
  - (3) conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
  - (4) attempts or conspires to commit money laundering offenses referred to in Items "(1)", "(2)" or "(3)" above;
  - (5) aids, abets, assists in or counsels the commission of the money laundering offenses referred to in Items "(1)", "(2)" or "(3)" above; and
  - (6) performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in Items "(1)", "(2)" or "(3)" above.

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

- b. *Financing of terrorism* is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (1) to carry out or facilitate the commission of any terrorist act; (2) by a terrorist organization, association or group; or (3) by an individual terrorist.
- c. *Covered transaction* (CT) refers to a transaction in cash or other equivalent monetary instrument exceeding P500,000.
- d. *Suspicious transaction* (ST) refers to a transaction with a covered person, regardless of the amount involved, where any of the following circumstances exists:
- (1) There is no underlying legal or trade obligation, purpose or economic justification;
  - (2) The client is not properly identified;
  - (3) The amount involved is not commensurate with the business or financial capacity of the client;
  - (4) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA, as amended;
  - (5) Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the covered person;
  - (6) The transaction is in any way related to an unlawful activity or any money laundering activity or offense, that is about to be committed, is being or has been committed; or
  - (7) Any transaction that is similar, analogous or identical to any of the foregoing.

Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as ST.

- e. *Monetary instrument* shall include, but is not limited to the following:
- (1) Coins or currency of legal tender of the Philippines, or of any other country;
  - (2) Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property;
  - (3) Drafts, checks, and notes;
  - (4) Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character including those enumerated in Section 3 of the Securities Regulation Code;
  - (5) A participation or interest in any non-stock, non-profit corporation;
  - (6) Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts or deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments;
  - (7) Contracts or policies of insurance, life or non-life, contracts of suretyship, pre-need plans and member certificates issued by mutual benefit association; and
  - (8) Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.
- f. *Unlawful activity* refers to any act or omission or series or combination thereof involving or having direct relation to the following:
- (1) Kidnapping for ransom under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code (RPC), as amended;
  - (2) Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15 and 16 of R.A. No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;
  - (3) Section 3 paragraphs "B", "C", "E", "G", "H" and "I" of R.A. No. 3019, as amended, otherwise known as the Anti-Graft and Corrupt Practices Act;
  - (4) Plunder under R.A. No. 7080, as amended;
  - (5) Robbery and extortion under Articles 294, 295, 296, 299, 300, 301 and 302 of the RPC, as amended;
  - (6) Jueteng and masiao punished as illegal gambling under P.D. No. 1602;
  - (7) Piracy on the high seas under the RPC, as amended, and P.D. No. 532;
  - (8) Qualified theft under Article 310 of the RPC, as amended;
  - (9) Swindling under Article 315 and "Other Forms of Swindling" under Article 316 of the RPC, as amended;
  - (10) Smuggling under R.A. Nos. 455 and 1937, as amended, otherwise known as the Tariff and Customs Code of the Philippines;
  - (11) Violations under R.A. No. 8792, otherwise known as the Electronic Commerce Act of 2000;
  - (12) Hijacking and other violations under R.A. No. 6235, otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the RPC, as amended;
  - (13) Terrorism and conspiracy to commit terrorism as defined and penalized under Sections 3 and 4 of R.A. 9372;
  - (14) Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of R.A. No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012;
  - (15) Bribery under Articles 210, 211 and 211-a of the RPC, as amended, and Corruption of Public Officers under Article 212 of the RPC, as amended;
  - (16) Frauds and illegal exactions and transactions under Articles 213, 214, 215 and 216 of the RPC, as amended;
  - (17) Malversation of public funds and property under Articles 217 and 222 of the RPC, as amended;
  - (18) Forgeries and counterfeiting under Articles 163, 166, 167, 168, 169 and 176 of the RPC, as amended;
  - (19) Violations of Sections 4 to 6 of R.A. No. 9208, otherwise known as the Anti-Trafficking in Persons Act of 2003, as amended;
  - (20) Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
  - (21) Violations of Sections 86 to 106 of Chapter IV, of R.A. No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
  - (22) Violations of Sections 101 to 107, and 110 of R.A. No. 7942, otherwise known as the Philippine Mining Act of 1995;
  - (23) Violations of Section 27(C), (E), (F), (G) and (I), of R.A. No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;

- (24) Violation of Section 7(B) of R.A. No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act;
- (25) Violation of R.A. No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;
- (26) Violations of Sections 1, 3 and 5 of P.D. No. 1866, as amended, otherwise known as the Decree Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives;
- (27) Violation of P.D. No. 1612, otherwise known as the Anti-Fencing Law;
- (28) Violation of Section 6 of R.A. No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995, as amended by R.A. No. 10022;
- (29) Violation of R.A. No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;
- (30) Violation of Section 4 of R.A. No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;
- (31) Violation of Section 4 R.A. No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;
- (32) Violations of Sections 5, 7, 8, 9, 10 (C), (D) and (E), 11, 12 and 14 of R.A. No. 7610, otherwise known as the Special Protection of Children Against Abuse, Exploitation and Discrimination;
- (33) Fraudulent practices and other violations under R.A. No. 8799, otherwise known as the Securities Regulation Code of 2000; and
- (34) Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

In determining whether or not a felony or offense punishable under the penal laws of other countries is "of similar nature", as to constitute an unlawful activity under the AMLA, the nomenclature of said felony or offense need not be identical to any of the unlawful activities listed above.

- g. *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.
- h. *Proceed* refers to an amount derived or realized from any unlawful activity.
- i. *Monetary instrument or property related to an unlawful activity* refers to:
  - (1) All proceeds of an unlawful activity;
  - (2) All monetary, financial or economic means, devices, accounts, documents, papers, items or things used in or having any relation to any unlawful activity;
  - (3) All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds and other similar items for the financing, operations, and maintenance of any unlawful activity; and
  - (4) For purposes of freeze order and bank inquiry: related and materially-linked accounts.
    - (a) *"Related accounts"* refer to those accounts, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.
    - (b) *"Materially-linked accounts"* shall include the following:
      - (i) 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;
      - (ii) 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;
      - (iii) 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;
      - (iv) All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the

freeze order or order of inquiry; and

- (v) All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing.
- j. *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;
  - (4) Persons whose assets are managed by an asset manager;
  - (5) Trustors/grantors/settlers of a trust;
  - (6) Insurance policy holders, whether actual or prospective; and
  - (7) Juridical person. The term juridical person shall refer to an entity other than a natural person as defined under the Civil Code of the Philippines, including corporate clients who keep or maintain an account with a covered person.
- k. *Shell company* refers to a legal entity which has no business substance in its own right but through which financial transactions may be conducted.
- l. *Shell bank* refers to a shell company incorporated as a bank or made to appear to be incorporated as a bank but has no physical presence and no affiliation with a regulated financial group. It can also be a bank that (a) does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorized to engage; (b) does not employ one (1) or more individuals on a full time basis at this fixed address; (c) does not maintain operating records at this address, and (d) is not subject to inspection by the authority that licensed it to conduct banking activities.
- m. *Beneficial Owner* refers to any natural person(s) who ultimately owns or controls a customer and/or on whose behalf a transaction is being conducted; or those who have ultimate effective control over a juridical person or legal arrangement.

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

Beneficial owner shall be:

- (1) The natural persons, if any, who ultimately have controlling ownership interest in a juridical person.

A shareholding or ownership interest of at least twenty percent (20%) in the customer held by a natural person shall be an indication of direct ownership. A shareholding or ownership interest of at least twenty percent (20%) in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.

- (2) The natural persons, if any, exercising control over the juridical person through other means, to the extent that there is a doubt under Item “(1)” 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.

Control through other means, includes control exerted by means of trusts, agreements, arrangements, understandings, or practices, or when an individual can exercise control through making decisions about financial and operating policies. In addition, control also includes: (a) power to govern the financial and operating policies of the enterprise under statute or an agreement; (b) power to appoint or remove the majority of the members of the board of directors or equivalent governing body; (c) power to cast the majority votes at a meeting of the board of directors or equivalent governing body; or (d) any other arrangements similar to any of the above.

- (3) The natural person(s) who hold the position of senior managing official(s) or equivalent ranks, where no person under Items “(1)” and “(2)” is identified, or if there

is any doubt that the person(s) identified are the beneficial owners(s).

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

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

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

*Immediate family members of PEPs* refer to individuals who are related to a PEP within the second degree of affinity or consanguinity.

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

- o. *Correspondent banking* refers to the provision of banking services by one (1) bank (the “correspondent bank”) to another bank (the “respondent bank”).
- p. *Payable-through account* refers to a correspondent account that is used directly by third parties to transact business on their own behalf.
- q. *Fund/wire transfer* refers to any transaction carried out on behalf of an originator (both natural and juridical) through an FI (originating institution) by electronic means with a view to making an amount of money available to a beneficiary at another FI (beneficiary institution). The originator person and the beneficiary person may be the same person.
- r. *Cross border transfer* refers to any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfer that has at least one (1) cross border element.
- s. *Domestic transfer* refers to any wire transfer where the originating and beneficiary 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 effect the fund/wire transfer may be located in another country.
- t. *Originating 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.
- u. *Beneficiary financial institution* refers to the financial institution which receives the wire transfer from the originating financial institution, directly or through an intermediary financial institution, and makes the funds available to the beneficiary.
- v. *Intermediary financial institution* refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the originating financial institution and the beneficiary financial institution, or another intermediary financial institution.
- w. *Official document* refers to any of the following identification documents:
- (1) For Filipino citizens: Those issued by any of the following official authorities:
    - (a) Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
    - (b) Government-Owned or -Controlled Corporations (GOCCs);
    - (c) Covered persons registered with and supervised or regulated by the Bangko Sentral, SEC or IC; or
    - (d) Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys)

- (2) For foreign nationals: Passport or Alien Certificate of Registration;
  - (3) For Filipino students: School ID signed by the school principal or head of the educational institution;
  - (4) For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity; and
  - (5) Other identification document that can be verified using reliable, independent source documents, data or information.
- x. *Juridical person* refers to an entity other than a natural person as defined under Chapter 3 of the Civil Code of the Philippines, that can establish a permanent customer relationship with any financial institution or otherwise own property.
  - y. *Money or Value Transfer Service (MVTs) or Money Service Business (MSB)* 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.
  - z. *Originator* refers to the account holder who allows the wire transfer from an account, or where there is no account, the person that places an order with the originating financial institution to perform a wire transfer.
  - aa. *Philippine Identification Card (PhilID)* refers to the non-transferable identification card issued by the PSA to all citizens and resident aliens registered under the PhilSys, which serves 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.
  - bb. *Cover Payment* refers to a wire transfer that combines a payment message sent directly by the originating financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the originating financial institution to the beneficiary financial institution through one or more intermediary financial institutions.
  - cc. *Serial Payment* refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the originating financial institution to the beneficiary financial institution, directly or through one (1) or more intermediary financial institutions.
  - dd. *Settlor/Grantor/Trustor* refers to a person who transfers ownership of his assets to trustees by means of a trust deed or a similar arrangement.
  - ee. *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.
  - ff. *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, investments, foreign remittance, inheritance and donation
  - gg. *Straight-through Processing* refers to payment transactions that are conducted electronically without the need for manual intervention.
  - hh. *Designated persons* refer to:
    - (1) Any person or entity designated as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations (UN) Security Council (UNSC) Resolutions (UNSCR) and their successor resolutions; or
    - (2) Any person, organization, association, or group of persons designated under Paragraph 3, Section 25 of the Anti-Terrorism Act of 2020 (ATA); and
    - (3) Any person or entity designated under UNSCR Nos. 1718 (2006) and 2231 (2015) and their successor resolutions.

- ii. *Name Match* refers to an individual or entity whose name matches with a name in the UNSC Consolidated List, any list of designations made by the Anti-Terrorism Council (ATC) under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.
- jj. *Property or Fund* refers to financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, traveler's cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends, or other income on or value accruing from or generated by such funds or other assets.
- kk. *Potential Target Match* refers to an individual or entity whose identity matches most, but not all, of the identifier information provided in the UNSC Consolidated List, any list of designations made by the ATC under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.
- ll. *Prohibition against dealing* prohibits any person from (1) dealing, directly or indirectly, in any way and by any means, with any property or funds that he knows or has reasonable ground to believe is owned or controlled by a designated person, organization, association or group of persons, including funds derived or generated from property or funds owned or controlled, directly or indirectly, by a designated person, organization, association or group of persons; or (2) making available any property or funds, or financial services or other related services to a designated person, organization, association or group of persons.
- mm. *Proliferation of Weapons of Mass Destruction (WMD) Financing/Proliferation Financing (PF)* refers to an action or circumstance when a person makes available an asset; or provides a financial service; or conducts a financial *transaction*; and the person knows that, or is reckless as to whether, the asset, financial service or transaction is intended to, in whole or in part, facilitate proliferation of WMD in relation to UNSCR Nos. 1718 (2006) (Democratic People's Republic of Korea or DPRK) and 2231 (2015) (Islamic Republic of Iran or Iran) and their successor resolutions.
- nn. *Proliferation of WMD* refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of WMD, in *contravention* of national laws or, where applicable, international obligations.
- oo. *Sanctions risk* refers to the risk of losses arising from failure to implement relevant sanctions requirements, including TFS. This includes risks of potential breach, non-compliance/non-implementation or evasion of TFS obligations.
- pp. *Targeted asset freeze* applies to named individuals, entities and bodies, restricting access to funds and economic resources. Someone subject to an asset freeze will be listed on the Consolidated List, designated or proscribed and posted under the Anti-Money Laundering Council (AMLC) or ATC websites.
- qq. *Targeted Financial Sanctions* refer to:
  - (1) *For TFS related to terrorism and TF*: both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and those proscribed by the Court of Appeals under Section 26 of the ATA.
  - (2) *For TFS related to PF*: both asset freezing and prohibition to prevent funds or other assets from being made available, directly or indirectly, for the benefit of any individual, natural or legal persons or entity designated pursuant to UNSCR and its designation process.
- rr. *Target Match* refers to an individual or entity whose identity matches all the identifier information and is identified to be the designated person in the UNSC Consolidated List, any list of designations made by the ATC under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.
- ss. *UNSC Consolidated List* refers to the integrated list of individuals and entities subject to measures imposed by the UNSC, as relevant to the Philippines' sanctions regime. This includes those designated under UNSCR Nos. 1267/1989/2253 (Al Qaeda/ISIL Da'esh), 1988 (Taliban), 1718 (2006) (DPRK) and 2231 (2015) (Iran) and their successor resolutions.

- tt. *Weapons of Mass Destruction* refer to chemical, biological, radiological, or nuclear weapons which are capable of high order of destruction or causing mass casualties. It excludes the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

## **905 BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING**

In line with the declaration of policy, covered persons shall apply the following principles:

- a. Conduct business in conformity with high ethical standards in order to protect its safety and soundness as well as the integrity of the national banking and financial system;
  - b. Know sufficiently your customer at all times and ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening or maintaining an account or transacting with the covered person by himself or otherwise;
  - c. Adopt and effectively implement a sound AML and terrorist financing prevention risk management system that identifies, assesses, monitors and controls risks associated with money laundering and terrorist financing (ML/TF);
  - d. Comply fully with this Part and existing laws aimed at combating money laundering and terrorist financing by making sure that officers and employees are aware of their respective responsibilities and carry them out in accordance with a superior and principled culture of compliance; and
  - e. Fully cooperate with AMLC for the effective implementation and enforcement of the AMLA, as amended, and its RIRR.
- f.

## RISK MANAGEMENT

### 911 RISK MANAGEMENT

All covered persons shall develop sound risk management policies and practices to ensure that risks associated with ML/TF such as reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of this Part, to the end that covered persons shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.

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

**Board and senior management oversight.** Notwithstanding the provisions specifying the duties and responsibilities of the compliance office and internal audit, it shall be the ultimate responsibility of the board of directors to fully comply with these rules, the AMLA, as amended, the TFPFA and their RIRR. It shall ensure that ML/TF risks are effectively managed and that this forms part of the covered person's enterprise risk management system.

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

- a. **Compliance office.** Management of the implementation of the covered person's Money Laundering and Terrorist Financing Prevention Program (MTPP) shall be a primary task of the compliance office. To ensure the independence of the office, it shall have a direct reporting line to the board of directors or any board-level or approved committee on all matters related to AML and CTF compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by senior management and the board, to wit:
  - (1) Ensure compliance by all responsible officers and employees with this Part, the AMLA, as amended, the RIRR and its own MTPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including ongoing monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It shall also report compliance findings to the board or any board-level committee;
  - (2) Ensure that infractions, discovered either by internally initiated audits, or by special or regular examination conducted by the Bangko Sentral, or other applicable regulators, are immediately corrected;
  - (3) Inform all responsible officers and employees of all resolutions, circulars and other issuances by the Bangko Sentral and the AMLC in relation to matters aimed at preventing ML and TF;
  - (4) Alert senior management, the board of directors, or the board-level or approved committee if it believes that the covered person is failing to appropriately address AML/CFT issues; and
  - (5) Organize the timing and content of AML training for officers and employees including regular refresher trainings as stated in Sec. 931.
- b. **Group-wide Money Laundering and Terrorist Financing Prevention Program.** Financial groups shall implement a group-wide MTPP, which shall be applied to their branches and majority-owned subsidiaries as provided under Sec. 903 (*Scope of Regulations*). The group-wide MTPP shall include the measures set out under this Section (*Money laundering and terrorist financing prevention program*).

The group-wide compliance officer or in his absence, the compliance officer of the parent entity, shall oversee the AML/CFT compliance of the entire group with reasonable

authority over the compliance officers of said branches, subsidiaries or offices.

**Money Laundering and Terrorist Financing Prevention Program.** All covered persons shall adopt a comprehensive and risk-based MTPP geared toward the promotion of high ethical and professional standards and prevention of the covered person from being used, intentionally or unintentionally, for ML/TF activities. The MTPP shall include policies, controls and procedures to enable the covered persons to manage and mitigate the risks that have been identified in their risk assessment, including taking enhanced measures for those classified as posing higher risks. The MTPP shall also be consistent with the AMLA, as amended, the TFPSA, their respective RIRR and the provisions set out in this Part. It shall be in writing, approved by the board of directors or by the country/regional head or its equivalent for local branches of foreign banks, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same. Where a covered person has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated ML/TF risk management system to ensure the coordination and implementation of policies and procedures on a group-wide basis, taking into account local business considerations, the requirements of the host jurisdiction and the level of country risk.

The MTPP shall also be readily available in a user-friendly form, whether in hard or soft copy. The covered person must put up a procedure to ensure an audit trail evidencing the dissemination process for new and amended policies and procedures. The program shall embody the following at a minimum:

- a. Detailed procedures of the covered person's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, and this Part, to wit:
  - (1) Customer identification process including acceptance policies and ongoing monitoring processes;
  - (2) Record keeping and retention;
  - (3) Covered transaction reporting; and
  - (4) ST 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 conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregated amounts breach the threshold. The ST reporting shall include a reporting chain under which an ST will be processed and the designation of a board-level or approved committee that will ultimately decide whether or not the covered person should file a report to the AMLC. If the resources of the covered person do not permit the designation of a committee, it may designate the compliance officer to perform this function instead: *Provided*, That the board of directors is informed of the decision.
- 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 this Part, the AMLA, as amended, its RIRR and their internal policies and procedures as embodied in the MTPP. The training program shall also include refresher trainings to remind these individuals of their obligations and responsibilities as well as update them of any changes in AML laws, rules and internal policies and procedures.
- c. An adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed to assume sensitive banking functions;
- d. An internal audit system in accordance with this Section;
- e. An independent audit program with a written scope of audit that will ensure the completeness and accuracy of the information and identification documents obtained from clients, the covered and suspicious transactions reports submitted to the AMLC, and the records retained in compliance with this Part, as well as the adequacy and effectiveness of the training program on the prevention of money laundering and terrorism financing;
- f. A mechanism that ensures all deficiencies noted during the audit and/or Bangko Sentral regular or special examination or other applicable regulator's examination are immediately corrected and acted upon;
- g. Cooperation with the AMLC and Bangko Sentral;

- h. Designation of an AML compliance officer, who shall at least be at senior officer level, as the lead implementer of the program within an adequately staffed compliance office. The AML compliance officer may also be the liaison between the covered person, the Bangko Sentral and the AMLC in matters relating to the covered person's AML/CFT compliance. Where the resources of the covered person do not permit the hiring of an AML compliance officer, the compliance officer shall also assume the responsibility of the former; and
- i. Policies and procedures for sharing information required for the purposes of customer due diligence (CDD) and risk management;
- j. A provision that the group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information on the 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. The MTPP may require a potential and/or existing customer to sign a waiver on the disclosure of information within the group;
- k. Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off;
- l. A mechanism to comply with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC; and
- m. A mechanism to comply with the prohibitions from conducting transactions with designated persons and entities, as set out in the relevant United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing and financing of proliferation of weapons of mass destruction.

***Submission of the revised and updated MTPP. Approval by the board of directors or country head.*** Within six (6) months from 05 April 2017, all covered persons shall prepare and have available for inspection an updated MTPP, approved by the board of directors, embodying the principles and provisions stated in this Part.

Henceforth, each MTPP shall be regularly updated at least once every two (2) years to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent Bangko Sentral issuances. Any revision or update in the MTPP shall likewise be approved by the board of directors or the country/regional head or its equivalent for local branches of foreign banks.

***Monitoring and reporting tools.*** All covered persons shall adopt an AML/CFT monitoring system that is appropriate for their risk profile and business complexity and in accordance with this Part. 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/CFT compliance.

- a. *Electronic monitoring and reporting systems for AML/CFT.* UBs, KBs and digital banks and such covered persons that are considered complex pursuant to Sec. 131 (*Definition of terms*) shall adopt an electronic AML 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, in addition to the functionalities mentioned in Sec. 922 (*Electronic monitoring systems for AML/CFT*).
- b. *Manual monitoring.* Covered persons not required to adopt an AML/CFT electronic system must ensure that they have the means of complying with this Section.

***Internal audit.*** The internal audit function associated with money laundering and terrorist financing should be conducted by qualified personnel who are independent of the office being audited. It must have the support of the board of directors and senior management and have a direct reporting line to the board or a board-level audit committee.

The internal audit shall, in addition to those specified by this Part, be responsible for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, CT and ST reporting and record keeping and retention, as well as the adequacy and

effectiveness of other existing internal controls associated with money laundering and terrorist financing.

For covered persons with an electronic AML/CFT transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities as required by this Section and Sec. 922 (*Electronic monitoring systems for AML/CFT*).

The results of the internal audit shall be timely communicated to the board of directors and shall be open for scrutiny by Bangko Sentral examiners in the course of the regular or special examination without prejudice to the conduct of its own evaluation whenever necessary. Results of the audit shall likewise be promptly communicated to the Compliance Office for appropriate monitoring of corrective actions taken by the different business units concerned. The Compliance Office shall regularly submit reports to the board to inform them of management's action to address deficiencies noted in the audit.

**Risk assessment.** Consistent with risk-based approach, covered persons are required to identify, understand and assess their ML/TF/PF<sup>1</sup> and sanctions risks or risks of potential breach, non-compliance, non-implementation or evasion of TFS obligations, arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels, among others. The assessment methodology shall be appropriate to the nature of operations and complexity of the business of the covered person. The institutional risk assessment shall (a) consider all relevant risk factors, including the results of national and sectoral risk assessments; (b) adequately document results and findings; and (c) be updated periodically or as necessary. The institutional risk assessment shall be conducted at least once every two (2) years, or as often as the Board or senior management may direct, depending on the level of risks identified in the previous risk assessment, or other relevant AML/CFT developments that may have an impact on the covered person's operations.

Based on the results of the risk assessment, the covered person shall take appropriate measures to manage and mitigate ML/TF/PF and sanctions risks and take enhanced measures on identified high-risk areas, which should be incorporated in its MTPP. The risk assessment shall be made available to the Bangko Sentral during examination or in other circumstances deemed necessary as part of continuous supervision.

**New products and business practices risk assessment.** Covered persons are also required to identify and assess the ML/TF/PF and sanctions 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. Such risk assessment should be an integral part of the product or service development process and should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Covered persons should take appropriate measures to manage and mitigate the identified risks.

---

<sup>1</sup> A particular type of financial institution may be exempted from the requirements to identify, assess, monitor, manage and mitigate PF risks provided there is proven low risk of PF relating to such financial institution.

## PREVENTIVE MEASURES

### 921 CUSTOMER DUE DILIGENCE

a. In conducting CDD, a risk-based approach shall be undertaken depending on the type of customer, business relationship or nature of the product, transaction or activity. In this regard, a covered person shall maintain a system that will ensure the conduct of CDD which shall include:

- (1) Identifying the customer and verifying the true identity of the customer based on official documents or other reliable, independent source documents, data or information. In case of corporate and juridical entities, verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf;
- (2) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner based on official documents, or using relevant information or data obtained from reliable sources, such that the covered person is satisfied that it knows who the beneficial owner is. The covered person should have a system to understand the nature of the customer's business and its ownership and control structure, in case of juridical persons or legal arrangements;

Where the customer, or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, the covered person is not required to verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

The covered person shall keep records of the actions taken in order to identify the beneficial owner.

- (3) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- (4) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the covered person's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Where a covered person is unable to comply with the relevant CDD measures, considering a risk-based approach, it shall (a) not open the account, commence business relations, or perform the transaction; or (b) terminate the business relationship; but in both cases, it shall consider filing a suspicious transaction report (STR) in relation to the customer.

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

b. A covered person shall be required to undertake customer due diligence when:

- (1) It establishes business relations with any customer;
- (2) It undertakes any occasional but relevant business transaction for any customer who has not otherwise established relations with the covered person;
- (3) There is a suspicion of ML or TF; or
- (4) There is doubt about the veracity or adequacy of previously obtained customer identification data.

c. *"Business relations"* means the opening or maintenance of an account or the provision of financial advice by the covered person to a customer.

d. *“Relevant business transaction”* shall refer to:

- (1) A transaction with a value exceeding P100,000, except for money changing or remittance transactions;
- (2) Two (2) or more transactions believed to be linked and with an aggregate value exceeding P100,000; or
- (3) In relation to remittance and money changing transactions, any transaction or two (2) or more transactions believed to be linked, with an aggregate value exceeding P5,000.00.

For this purpose, covered persons should have an appropriate system to identify and determine occasional customers or transactions.

e. *For existing customers.* Covered persons shall apply CDD requirements to existing customers on the basis of materiality and risk, and conduct due diligence on existing relationships at appropriate times, taking into account CDD measures previously undertaken as well as the adequacy of information and documents obtained.

***Customer acceptance and identification policy.*** Every covered person shall develop clear, written and graduated customer acceptance and identification policies and procedures, which shall include sanctions screening. Covered persons shall ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening an account or establishing a relationship. A covered person shall formulate a risk-based and tiered customer acceptance, identification and retention policy that involves reduced CDD for potentially low-risk clients and enhanced CDD for higher-risk accounts.

a. *Criteria for type of customers: low, normal and high risk; Standards for applying reduced, average and enhanced due diligence.* Covered persons shall specify the criteria and description of the types of customers that are likely to pose low, normal or high ML/TF risk to their operations, as well as the standards in applying reduced, average and enhanced due diligence, including a set of conditions for the denial of account opening or services.

Enhanced due diligence shall be applied to customers that are assessed by the covered person or under this Part as high risk for ML/TF. For customers assessed to be of low risk such as small account balances and transactions, a covered person may apply reduced due diligence. Some entities may likewise be considered as low-risk clients, e.g., banking institutions, trust entities and QBs authorized by the Bangko Sentral to operate as such and publicly listed companies subject to regulatory disclosure requirements.

In designing a customer acceptance and risk profiling policy, the following criteria relating to the product or service, the customer, and geographical location, at a minimum, shall be taken into account:

- (1) The nature of the service or product to be availed of by the customers and the purpose of the account or transaction;
- (2) Source of funds, source of wealth/nature of business, employment;
- (3) Public or high-profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;
- (4) Country of origin and residence of operations or the fact that a customer came from a high-risk jurisdiction;
- (5) The existence of ST indicators;
- (6) Watchlist of individuals and entities engaged in illegal activities or terrorist-related activities as circularized by the Bangko Sentral, 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 Security Council; and
- (7) Such other factors, e.g., the amount of funds to be deposited by a customer or the size of transactions, and regularity or duration of the transaction, as the covered person may deem reasonable or necessary to consider in assessing the

risk of a customer to ML/TF.

In assessing the risk profile of customers which are juridical entities, the covered person should also consider the financial profile and other relevant information of the active authorized signatories.

The covered person shall document the risk profiling results as well as how a specific customer was profiled and what standard of CDD (reduced average or enhanced) was applied.

- b. *Enhanced due diligence* (EDD). Whenever EDD is applied as required by this Part, or by the covered person's customer acceptance policy, or where the risk of ML/TF is higher, the covered person shall do all of the following, in addition to profiling of customers and monitoring of their transactions:
- (1) Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of average due diligence as enumerated in this Section and Sec. 924.
    - (a) In case of individual customers:
      - (i) supporting information on the intended nature of the business relationship/source of funds/ source of wealth (such as financial profile, ITR, Loan Application, Deed of Donation, Deed of Sale, etc.);
      - (ii) reasons for intended or performed transactions;
      - (iii) list of companies where he is a stockholder, director, officer, or authorized signatory;
      - (iv) other relevant information available through public databases or the internet; and
      - (v) a list of banks where the individual has maintained or is maintaining an account.
    - (b) In case of entities:
      - (i) prior or existing bank references;
      - (ii) the name, present address, nationality, date of birth, nature of work, contact number and source of funds of each of the primary officers (e.g., President, Treasurer);
      - (iii) volume of assets, other information available through public databases or the internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial Statement, Loan Application, Deed of Donation, Deed of Sale, etc.); and
      - (iv) reasons for intended or performed transactions.
  - (2) Conduct validation procedures in accordance with this Section on any or all of the information provided;
  - (3) Secure senior management approval to commence or continue the business relationship/transacting with the customer;
  - (4) Conduct enhanced ongoing monitoring of the business relationship by, among others, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
  - (5) 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
  - (6) Perform such other measures as the covered person may deem reasonable or necessary.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, the covered person shall deny banking relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

- c. *Minimum validation procedures for EDD.* The procedures performed must enable the covered person to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

Validation procedures for individual customers shall include, but are not limited to, the following:

- (1) Confirming the date of birth from a duly authenticated official document;
- (2) Verifying the address through evaluation of utility bills, bank or credit card statements, sending thank you letters, or other documents showing address or through on-site visitation;
- (3) Contacting the customer by phone or e-mail;
- (4) Determining the authenticity of the identification documents through validation of their issuance by requesting a certification from the issuing authority or by any other effective and reliable means; or
- (5) Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include, but are not limited to, the following:

- (1) Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
- (2) Inquiring from the supervising authority the status of the entity;
- (3) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
- (4) Contacting the entity by phone or e-mail.

- d. *Reduced due diligence.* Where lower risks of ML/TF have been identified through an adequate analysis of risk by the covered person and based on the results of the institutional risk assessment, reduced due diligence procedures may be applied commensurate with the lower risk factors. The reduced due diligence procedures shall not be applied in cases of suspicion of higher ML/TF risk scenarios.

Whenever reduced due diligence is applied as provided in this Part or in the covered person's customer acceptance policy, the following rules shall apply:

- (1) For individual customers, a covered person may open an account/establish relationship under the true and full name of the account owner/s or customers upon presentation of an acceptable identification card (ID) or official document as defined in this Part or other reliable, independent source documents, data or information: *Provided*, That, for accounts used purely for digital or electronic payments, the covered person may define appropriate reduced due diligence procedures provided that ML/TF risks are effectively managed.
- (2) For corporate, partnership, and sole proprietorship entities, a covered person may open an account under the official name of these entities by presenting a Board Resolution duly certified by the Corporate Secretary, or equivalent document, authorizing the signatory to sign on behalf of the entity, obtained at the time of account opening.

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

- e. *Restricted account.* To promote financial inclusion and ensure that micro-business owners and low-income households are able to manage their finances through the

financial system, customers who may not be able to provide any of the required information or valid reasons or any valid identification document under this Section on *Customer identification* may be allowed to open a restricted account with a covered person, provided:

- (1) the aggregate credits in a year shall not exceed P100,000; and
- (2) the account shall not be allowed to receive/send foreign remittances.

In lieu of a valid ID, the covered person shall obtain the customer's complete name, birth date, address and nationality and ensure that it has in its records a clear photograph and signature or biometric of the customer.

The account opening shall be subject to the condition that the customer shall obtain a valid ID within twelve (12) months; otherwise the account shall be closed and the remaining balance therein shall be returned to the customer. An extension of another twelve (12) months may be allowed: *Provided*, That the customer is able to show the covered person a proof of application for a valid ID.

The covered person shall ensure that the above conditions are not breached; otherwise complete information and a valid ID shall immediately be required or the account shall be closed accordingly.

***Customer identification.*** Covered persons shall establish and verify the true identity of their customers based on official documents as defined in this Part or other reliable, independent source documents, data or information.

a. Minimum information/documents required:

- (1) *New individual customers.* Covered persons shall develop a systematic procedure for establishing the true and full identity of new individual customers, and shall open and maintain the account/relationship only in the true and full name of the account/relationship owner/s.

Unless otherwise stated in this Part, average CDD requires that the covered person obtain from individual customers, at the time of account opening/establishing the relationship, the following minimum information and verify the customer's identity with official or valid identification documents or other reliable, independent source documents, data, or information:

- (a) name of customer and/or PhilSys Card Number (PCN) or the PhilSys Number (PSN) derivative;
- (b) date and place of birth;
- (c) address;
- (d) contact number or information;
- (e) citizenship or nationality;
- (f) specimen signature or biometric of the customer; and
- (g) name, address, date and place of birth, contact number or information and citizenship or nationality of the beneficiary or beneficial owner, whenever applicable;

Pursuant to Republic Act No. 11055 or the Philippine Identification System Act and its Revised Implementing Rules and Regulations, the Philippine Identification System is the government's central identification platform for all citizens and resident aliens of the Philippines. An individual's records in the PhilSys shall be considered as an official and sufficient proof of identity. Considering its identity proofing, enrolment, authentication and identity life cycle management processes, the PhilSys is considered a reliable and independent source for verifying the customer's identity. Where the PCN or PSN derivative, or the Philippine Identification Card, in physical or digital form, is presented by the customer, it shall be accepted as official and sufficient proof of identity, subject to proper authentication, and the covered person shall no longer require additional documents to verify the customer's identity.

- (2) *New juridical persons.* A covered person shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities, as well as their stockholders/partners/owners, directors, officers and authorized signatories. It shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in the

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

Unless otherwise stated in this Part, average due diligence requires that the covered person obtain the following minimum information and/or documents before establishing business relationships:

- (a) Customer information
    - (i) Name of juridical person;
    - (ii) Name, address, citizenship or nationality of beneficial owner, if applicable, and authorized signatories;
    - (iii) Official address;
    - (iv) Contact numbers or information;
    - (v) Nature of business; and
    - (vi) Specimen signatures or biometrics of the authorized signatory.
  - (b) Identification documents
    - (i) Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission (SEC) for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance agents and transfer companies;
    - (ii) Secondary license or certificate of authority issued by the supervising authority or other government agency;
    - (iii) Articles of incorporation/partnership;
    - (iv) Latest General Information Sheet;
    - (v) Board or Partners' resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity; and
    - (vi) For entities registered outside of the Philippines, similar documents and/or information shall be obtained, duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.
- (3) For legal arrangement (e.g., Trust), the following must be obtained:
- (a) Name of legal arrangement and proof of existence;
  - (b) Address and country of establishment;
  - (c) Nature, purpose and objects of the legal arrangement;
  - (d) The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement;
  - (e) Description of the purpose/activities of the legal arrangement;
  - (f) Expected use of the account; and
  - (g) Amount, number, type, purpose and frequency of the transaction expected.

In addition, the following rules shall apply to trustees:

- (a) *trustees of any express trust* shall obtain and hold adequate, accurate, and current information on the identity of the trustor/settlor/grantor, the trustee, the beneficiary or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust.

Covered persons shall likewise obtain sufficient information, such as the full name, place and date of birth or date of registration of the beneficiary/ies of these trusts, or of similar legal arrangements. This is to ensure that covered persons are able to identify and verify the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

- (b) *trustees of any trust* shall hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors;

- (c) trustees shall disclose their status when forming a business or professional relationship, or in carrying out an occasional transaction above the threshold under “d” of Sec. 921 (*Customer due diligence*); and
  - (d) trustees shall make available to competent authorities, to the extent allowed by law, 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.
- (4) *Identification and Verification of Agents and Authorized Representatives.* Covered persons shall verify that any person purporting to act on behalf of a customer is so authorized and shall identify and verify the identity of that person.

For this purpose, the covered person shall obtain the name, address and citizenship or nationality of agents and authorized representatives.

- b. Customer verification process. Covered persons shall verify the identity of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. They may complete the verification process after the establishment of the business relationship: *Provided, That*:
  - (1) this occurs as soon as reasonably practicable;
  - (2) this is essential not to interrupt the normal conduct of business; and
  - (3) the ML/TF risks are effectively managed, taking into consideration risk and materiality.

Covered persons shall adopt appropriate risk management measures with respect to how the customer may use the business relationship prior to verification. These measures may include, among others, setting up of transaction limits and monitoring of transactions that are beyond the expected activities or norms for the type of relationship.

- c. Valid identification documents.
  - (1) Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with a covered person for the first time shall be required to present an official identification document which shall include any of the official documents as defined in this Part or other identification information which can be verified from reliable, independent sources, documents, data or information, such as a third-party verified customer information database.
  - (2) If the official document presented is not the PhilID, PCN or PSN derivative, a covered person may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer and ensure that risks are mitigated.

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

In customer identification process, covered persons shall implement appropriate systems of data collection and recording, such as: (1) photocopying/scanning of identification document presented; (2) using Information and Communication Technology (ICT) to capture and record the biometric and other personal information of customers; and/or (3) manual recording of identification information.

In cases where the PhilID is presented, only the front portion/face should be photocopied/scanned. The PSN located at the back portion of the PhilID must remain confidential subject to applicable laws and regulations. In this regard, covered persons may only obtain either the PCN or PSN derivative indicated in the PhilID presented as part of customer identification and verification.

Covered persons shall also comply with the required digitization of customer records, as applicable, pursuant to relevant Bangko Sentral and AMLC issuances.

Relief in case of calamity. In case of a disastrous calamity and subject to a declaration by the Bangko Sentral on the applicability of this relief, any requirement for the presentation of a valid ID shall be relaxed, subject to the following conditions:

- (a) The amount of transactions shall not exceed P50,000.00 per day;
  - (b) The customer is either a permanent or temporary resident or who conducts business in a severely affected area which has been declared to be under a state of calamity by a competent authority;
  - (c) The customer shall submit a written certification, which need not be notarized, that he/she is a victim of the subject disastrous calamity and has lost his/her valid IDs; and
  - (d) The customer's account activities shall be subject to strict monitoring by the covered person to identify potential abuse of the relaxed requirement and any STs shall be reported to the AMLC within the prescribed period.
- d. *Face-to-Face contact.* Covered persons shall conduct face-to-face contact and/or personal interview at the commencement of the relationship. Face-to-face contact may likewise be conducted as soon 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, there are policies and procedures to address any specific risk associated with the same including a clear definition of instances when it will be allowed.

The use of ICT in the conduct of face-to-face contact and/or interview may be allowed: *Provided*, That the covered person has measures in place to mitigate the ML/TF risks and that key CDD processes are documented or with adequate audit trail.

- e. *Outsourcing of the customer identification and verification procedures.* Subject to existing rules on outsourcing of specified banking activities, a covered person may, without prior Monetary Board approval, outsource to a counterparty, which may or may not be a covered person as herein defined, the customer identification and verification procedures under Items "a", "b" and "d" above: *Provided*, That the ultimate responsibility for knowing the customer, keeping the identification documents, and managing attendant risks shall rest with the covered person and the following conditions are complied with.

For covered person counterparty:

- (1) There is a written service level agreement approved by the board of directors or senior management of the covered persons and its counterparty;
- (2) The counterparty has a reliable and acceptable customer identification system and training program in place.

For non-covered person counterparty:

- (1) All conditions required for covered person counterparty;
- (2) The covered person outsourcing the activity shall ensure that the employees or representatives of the counterparty gathering the required information/documents of, and/or conducting face-to-face contact with, the customer undergo equivalent training program as that of the covered person's own employees undertaking a similar activity; and
- (3) The covered person shall monitor and conduct annual review of the performance of the counterparty to determine whether or not to continue with the arrangement.

All identification information and/or documents shall be turned over within a period not exceeding ninety (90) calendar days to the covered person, which shall carefully review the documents or information and conduct the necessary risk assessment of the customer. The covered person may, however, include in the coverage of the outsourcing agreement the safekeeping of the documents gathered subject to the condition that customer identification documents shall be made available to the covered person or to the competent authorities within three (3) banking days from the date of request.

- f. *Third party reliance.* A covered person may rely on third parties to perform the CDD procedures under Item "(a) 1 to 3" of Sec. 921 (*Customer due diligence*) subject to the following rules:

- (1) *Where the third party is a covered person specifically defined by this Part and as generally defined by AMLA, as amended, and its RIRR – The covered person shall obtain from the third party a written sworn certification containing the following:*
  - (a) The third party has conducted the prescribed customer identification procedures in accordance with this Part and its own MTPP, including the face-to-face contact requirement, to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and
  - (b) The relying covered person shall have the ability to obtain identification documents from the third party upon request without delay.
- (2) *Where the third party is a financial institution operating outside the Philippines that is other than covered persons referred to in Item “1” above but conducts business operations and activities similar to them. All the contents required in the sworn certification mentioned in Item “1” above shall apply, with the additional requirement that the laws of the country where the third party is operating has equal or more stringent customer identification process requirement and that it has not been cited in violation thereof.*

When determining which countries the third party that meets the requirements above can be based, covered persons should consider available information on the level of country risk.

- (3) For both Items “(1)” and “(2)” above, it shall, in addition to performing normal due diligence measures, do the following:
  - (a) Gather sufficient information about the third party and the group to which it belongs to understand fully the nature of its business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to ML or TF investigation or regulatory action. Satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with CDD and record-keeping requirements;
  - (b) Document the respective responsibilities of each institution; and
  - (c) Obtain approval from senior management at inception of relationship before relying on the third party.
- (4) Covered persons may rely on a third party that is part of the same financial group under the following circumstances:
  - (a) the group applies CDD, record-keeping and MTPP requirements;
  - (b) the implementation of CDD and record-keeping requirements, and the MTPP is supervised at a group level by a competent authority, such as a Group Compliance Officer; and
  - (c) any higher country risk is adequately mitigated by the group’s AML/CFT policies.

A Bangko Sentral-accredited custodian may likewise rely, in accordance with this Part, on the face-to-face contact and gathering of minimum information performed by the seller or issuer of securities or by the global custodian to establish the existence and full identity of the customer: *Provided*, That the said third party has an equivalent customer identification requirement.

Notwithstanding the foregoing, the ultimate responsibility for identifying the customer still lies with the covered person relying on the third party.

In cases where the customer is assessed as high risk by the third party, the covered person shall conduct its separate enhanced due diligence procedure.

- g. *Electronic Know Your Customer (e-KYC)*<sup>1</sup> e-KYC refers to the process of electronically verifying the credentials of a customer.

Covered persons may use different methods to conduct customer identification and verification including e-KYC through digital ID system. For this purpose, digital ID systems are systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital. The digital ID system to be used in conducting CDD must be supported by robust technology, adequate governance, processes and procedures that provide an appropriate level of confidence that the system produces accurate results. It should also be soundly protected against cyber-attacks and internal malfeasance or external manipulation/falsification by unauthorized users to fabricate false or synthetic identities.

When employing e-KYC using a digital ID system, the covered person should ensure that it is anchored on, among others, robust, effective, and reliable information and communication technology architecture. Where the tiering is based on, among others, level of access and authentication assurance levels, it shall adopt tiered or risk-based e-KYC policies and procedures (e.g., low-tier level has access to basic authentication which requires minimum assurance levels or controls; access to subsequent tier level and additional services requires higher assurance/controls). Assurance levels refer to the extent of trustworthiness or confidence in the reliability of each of the three (3) stages of the digital ID process, from identity proofing and enrolment to authentication, and identity lifecycle management. In implementing e-KYC through digital ID system, the covered person shall:

- (1) Understand the basic components of the digital ID system, particularly how they apply to the CDD requirements, as these will support customer identification and verification process.
  - (a) Identity proofing and enrolment. This involves the collection, validation, deduplication and verification of identity evidence and information provided by the person; and establishing an identity account (enrolment) and binding the individual's unique identity to authenticators possessed and controlled by the person;
  - (b) Authentication. This establishes, based on possession and control of authenticators, that the person asserting an identity (the on-boarded customer or claimant) is the same person who was identity proofed and enrolled; and
  - (c) Identity lifecycle management. This refers to the actions that should be taken in response to events that can occur over the identity lifecycle and affect the use, security and trustworthiness of authenticators, for example, loss, theft, unauthorized duplication, expiration, and revocation of authenticators and/or credentials.
- (2) Apply informed risk-based approach to reliance on digital ID system for CDD that includes the requirement under item "(1)" above and ensure that the assurance level/s are appropriate for the ML/TF risks presented by the customer, product, delivery channel, geographical location, among others. This will enable the implementation of a tiered customer identification and acceptance process that leverages digital ID systems with various assurance levels to support financial inclusion. For example, in case of non-face-to-face channels, if the customer identification and verification depend on a reliable, independent digital ID system with appropriate risk mitigation measures, this may pose normal risk, or even lower risk where higher assurance levels are implemented. The assurance level will determine if the digital ID system is reliable and independent for AML/CFT purposes.
- (3) Utilize anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT measures such as customer identification/verification at onboarding and ongoing due diligence and transaction monitoring.

A covered person may rely on another entity in the conduct of customer identification and verification, using a digital ID system, subject to existing rules on outsourcing and third-party reliance requirements, as applicable. Moreover, the relying

---

<sup>1</sup> Covered persons with existing e-KYC, using a digital ID system, as of 28 April 2023 shall comply with the requirements prescribed herein within one (1) year from said date. For covered persons without existing e-KYC and intend to adopt the same, they shall ensure strict compliance with the e-KYC requirements prescribed in this Section prior to implementation.

party should ensure that the third party's digital ID system enables the former to (i) immediately obtain the necessary information concerning the identity of the customer (including the assurance levels, where applicable); and (ii) take adequate steps to satisfy itself that the third party will make available copies or other appropriate forms of access to the identity evidence (documents, data and other relevant information) upon request without delay.

In any case, the relying covered person has the ultimate responsibility for the customer identification/verification process, and effective authentication, using the digital ID system provided by the digital ID service provider, and ensure that a risk-based approach is applied in the use of the digital ID systems for customer identification/verification and authentication.

The covered person shall ensure that its conduct of e-KYC complies with relevant user consent and data sharing and protection/privacy laws, rules and regulations for data processing, storage, and management. All related transaction/s and their attendant risks or obligations, including the roles and responsibilities of each party involved, must be explicitly, clearly, and adequately provided by the covered person, and are explained to, understood, and accepted by the customer.

In this regard, pursuant to R.A. No. 11055 and its IRR, the PhilSys-enabled e-KYC is recognized as an acceptable system for e-KYC using digital ID system in the Philippines, including the PhilSys-issued credentials in physical or digital form, or authentication against the PCN, PSN derivative, or other tokens that will be issued by PhilSys, and an authentication factor such as biometric or demographic information. Further, covered persons, as relying parties, must comply with the onboarding and other e-KYC related guidelines issued by the Philippine Statistics Authority (PSA) prior to use of or access to the PhilSys-enabled e-KYC. For covered persons that will utilize the PhilSys-enabled e-KYC, they shall ensure compliance with the applicable guidelines and full implementation of the authentication procedures/methods and other related systems under the PhilSys.

Covered persons implementing e-KYC must perform customer identification and verification process under the same standards equivalent to those for face-to-face basis and shall establish appropriate risk management processes.

Consistent with Sec. 002, the Bangko Sentral may deploy appropriate supervisory enforcement actions to promote adherence with the requirements set forth in this Section and bring about timely corrective actions.

- h. *Trustee, nominee, agent or intermediary account.* Where (1) an account is opened by; (2) relationship is established through; or (3) any transaction is conducted by a trustee, nominee, agent or intermediary, either as an individual or through a fiduciary relationship or similar arrangements, the covered person shall establish and record the true and full identity and existence of both the (1) trustee, nominee, agent or intermediary; and (2) trustor, principal, beneficial owner or person on whose behalf the account/relationship/transaction is being opened/established/conducted. The covered person shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of due diligence to be applied to both.

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

In case a covered person entertains doubts as to whether the trustee, nominee, agent, or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence in accordance with this Section on *Customer acceptance and identification policy* and file an ST report, if warranted.

- i. *Prohibited accounts.* A covered person shall maintain accounts only in the true and full name of the account owner. The provisions of existing law to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, numbered checking accounts and all other similar accounts shall be absolutely prohibited.

***Ongoing monitoring of customers, accounts and transactions.***

- a. Covered persons shall, on the basis of materiality and risk, ensure that pertinent identification 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. The covered person shall document the actions taken in connection with updating of customer's records/information, and accordingly update customer's risk profile.

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

- b. **Enhanced due diligence.** 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. Covered persons shall apply enhanced due diligence on the customer in accordance with this Section on *Customer acceptance and identification policy* if they acquire information in the course of customer account or transaction monitoring that:

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

If the covered person:

- (1) fails to satisfactorily complete the enhanced due diligence procedures; or
- (2) reasonably believes that performing the enhanced due diligence process will tip-off the customer,

it shall file an ST report, and closely monitor the account and review the business relationship.

***Targeted Financial Sanctions related to terrorism, terrorist financing, proliferation of weapons of mass destruction, and proliferation financing.*** Covered persons shall adopt appropriate policies and procedures to effectively implement TFS related to terrorism, TF, proliferation of WMD, and PF.

***TFS related to terrorism and TF.*** In relation to designated persons under relevant binding terrorism-related resolutions, including UNSCR No. 1373 pursuant to Article 41 of the UN Charter and the ATA, covered persons, upon receipt of the notice of AMLC resolution on the issuance of sanctions freeze order, are required to freeze without delay the following:

- a. property or funds that are in any way related to financing of terrorism or acts of terrorism; or

- b. property or funds of any person, group of persons, terrorist organization, or association, 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 financing of terrorism or acts of terrorism as defined under the Terrorism Financing Prevention and Suppression Act of 2012, the ATA and their respective IRRs.

The property or funds referred to in the immediately preceding paragraph shall include all property or funds:

- a. that are owned or controlled by the subject of designation and are not limited to those that are directly related or tied to a particular terrorist act, plot, or threat.
- b. that are wholly or jointly owned or controlled, directly or indirectly, by the subject of designation.
- c. derived or generated from funds or other assets owned or controlled, directly or indirectly, by the subject of designation.
- d. of persons or entities acting on behalf or at the direction of the subject of designation.

In case of asset freeze, covered persons are generally prohibited to:

- a. deal with the frozen funds or economic resources, belonging to or owned, held or controlled by a designated person;
- b. make funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person; and/or
- c. engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions.

The freeze orders shall also cover those persons or entities included in subsequent updates, modifications and amendments to the UNSC Consolidated List, as well as those designated by the ATC under Section 25 of the ATA and those proscribed by the Court of Appeals under Section 26 of the ATA.

All covered persons shall submit to the AMLC a detailed written return, pursuant to, and containing details required under, Rule 16.c of the TFPSA IRR.

***TFS related to proliferation of WMD and PF.*** In relation to designated persons pursuant to UNSCR Nos. 1718 (2006) and 2231 (2015), and their successor resolutions, as well as any binding resolution of the Security Council, covered persons are required to:

- a. Freeze the following within a matter of hours from the time that the designation and the freeze order is published on the AMLC website:
  - (1) all funds or other assets that are owned or controlled by the designated persons, and not just those that can be tied to a particular act, plot or threat of proliferation of WMD and PF;
  - (2) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons;
  - (3) the funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by designated persons; and
  - (4) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons;
- b. Block or restrain specific properties or funds that are owned or controlled by a designated person from being transacted, converted, concealed, moved, or disposed; and
- c. Prohibit any person or entity from making any funds or other assets available for the benefit of designated persons, unless licensed, authorized or otherwise notified in accordance with the relevant UNSCR.

TFS related to terrorism, TF, proliferation of WMD, and PF, requires full application or implementation. The TFS shall be effective until the basis for its issuance has been lifted.

***General Requirements to Implement TFS related to terrorism, TF, proliferation of WMD, and PF.*** Covered persons shall adopt risk-based and proportionate measures to reinforce and complement the full implementation of the TFS requirements which shall include, at a minimum, the following:

- a. *Sanctions Policies and Procedures.* Informed by the results of the sanctions risk assessment, covered persons shall adopt proportionate and risk-based sanctions policies

and procedures approved by the Board of Directors or equivalent body/authority to facilitate the implementation of TFS without delay.

b. *Sanctions Screening Procedures.* As part of the customer due diligence process, covered persons shall develop sanctions screening system and procedures, which include, among others:

- (1) Screening of (a) customers, including beneficial owners or any persons purporting to act on behalf of the customer and their authorized signatories, (b) transactors/non-accountholders transacting with the covered person, and (c) counterparties/other credentials or relevant information in wire transfers or trade transactions, at the minimum.
- (2) Defining the timing of the conduct of screening such as (a) upon establishment of relationship or opening of an account, or at the latest prior to the first transaction, regardless of the customer risk profile, (b) periodically over the course of the relationship, especially whenever new designations or updates are issued, and (c) whenever there are updates to the client's information, such as change of ultimate beneficial owners or authorized signatories.

Sanctions screening procedures for transactions under the National Retail Payment System (NRPS) shall be governed by items "c(1)" and "c(2)" on AML Requirements of Sec. 803, wherein the originating/sending institution and beneficiary/receiving institution shall be responsible for the appropriate screening of their respective clients.

c. *Sanctions Database.* Covered persons shall adopt and maintain suitable sanctions database (electronic and/or manual) that is commensurate to its risk profile and complexity of operations to facilitate screening of customers and their transactions.

The sanctions database must include, at the minimum, the following and their successor resolutions:

- (1) UNSC Consolidated List that includes UNSCR Nos. 1267/1989 (Al Qaeda), 1988 (Taliban), and 2253 (ISIL Da'esh) for TFS on terrorism and TF;
- (2) UNSC Consolidated List that includes UNSCR Nos. 1718/2006 (DPRK) and 2231/2015 (Iran) for TFS on proliferation of WMD and PF; and
- (3) Domestic designations by the ATC pursuant to UNSCR No. 1373 and Paragraph 3, Section 25 of the ATA, and those proscribed by the Court of Appeals under Section 26 of the ATA.

Covered persons shall adopt mechanisms to ensure that the sanctions database is accurate, complete, and up-to-date. All new designations shall be included in the sanctions database and checked or screened against existing customer base without delay to adhere to the TFS requirements under applicable laws and regulations.

Covered persons may consider including other unilateral sanctions lists (e.g., Office of Foreign Assets Control of the United States Department of the Treasury and European Union) based on the applicable laws and implementing regulations, internal policy and results of their sanctions risk assessment, in line with their risk profile and operations, for purposes of risk management and ST reporting, among others.

d. *Disposition of Matches and Handling of Freeze Order.* Covered persons shall adopt suitable name screening policies and procedures to determine name match, potential target match, and target match, as well as the corresponding actions to take, in accordance with the procedures, reporting requirements and timelines prescribed by the AMLC.

For name match, covered persons should have a defined hierarchy of actions and references to disambiguate or resolve the name match. This includes inquiring or requesting additional information and identification documents from the customer and/or other reliable parties/relevant government agencies, such as the AMLC, to verify whether the name match is a potential target match or target match.

In case of potential target match, the covered person shall freeze without delay the funds or other assets of designated persons that it has control over and inform the AMLC on the same day the freeze is implemented. An ST report shall also be submitted to the

AMLC, including for attempted transactions or dealings. A detailed electronic return shall be filed to the AMLC within twenty-four (24) hours from receipt of the AMLC's confirmation of the propriety of the freeze. In case no confirmation is received from the AMLC within thirty-six (36) hours from receipt of the information, the freeze shall be automatically lifted.

In case of target match, the covered person shall freeze the account or assets and file a detailed electronic return to the AMLC within 24 hours from effecting the freeze.

- e. *Delisting and Unfreezing.* A designated person may be delisted by the UNSC or its appropriate Sanctions Committee, or by other competent authorities, and the AMLC may issue unfreezing orders, both in accordance with the applicable laws and regulations. Accordingly, upon receipt of the unfreezing order from the AMLC, or upon knowledge of the delisting made by the UNSC or its Committee, or other competent authorities, the covered person holding the frozen funds and other assets shall implement the unfreezing order or unfreeze without delay, and submit a detailed report to the AMLC. The detailed report shall be filed within 24 hours from the lifting of the freeze order, and include the time and date of unfreezing and a list of the unfrozen funds and other assets. Covered persons shall refer to the delisting process and/or unfreezing procedures under applicable UNSC Committee and AMLC guidelines and issuances.

For uniform and effective implementation of TFS requirements, covered persons shall regularly refer to the relevant and up-to-date legislation as well as specific AMLC and BSP rules and regulations on TFS.

***Non-discrimination against certain types of customers.*** The provisions of this Part shall not be construed or implemented in a manner that will discriminate against certain customer types, such as PEPs, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny these persons access to the covered person's services. In this regard, covered persons shall have appropriate policies and procedures to ensure non-discrimination against certain customer types when implementing AML/CFT regulations. Covered persons who commit said discriminatory act shall be subject to appropriate sanctions provided under existing laws and regulations.

## **922 COVERED AND SUSPICIOUS TRANSACTION REPORTING**

Covered persons shall report to the AMLC all covered and STs within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

For STs, "*occurrence*" refers to the date of determination of the suspicious nature of the transaction, which determination should be made not exceeding ten (10) calendar days from the date of transaction. However, if the transaction is in any way related to, or the person transacting is involved in or connected to, an unlawful activity or money laundering offense, the 10-day period for determination shall be reckoned from the date the covered person knew or should have known the suspicious transaction indicator.

Should a transaction be determined to be both a covered and suspicious transaction, the covered person shall be required to report the same as an ST.

Covered persons shall ensure the accuracy and completeness of covered and ST reports, which shall be filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.

***Deferred reporting of certain covered transactions.*** Covered persons shall refer to the issuances of the AMLC from time to time on transactions that are considered as "non-cash, no/low risk covered transactions", hence subject to deferred reporting.

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

***Electronic monitoring systems for AML/CFT.*** Covered persons required under Sec. 911 (*Monitoring and reporting tools*) to have an electronic monitoring system for AML/CFT 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 CT or ST 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/CFT monitoring.

The system must have at least the following automated functionalities:

- a. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
- b. Watch list monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
- c. Investigation – checks for given names throughout the history of payment stored in the system;
- d. Can generate all the CTRs of the 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 STs and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.

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.

**Manual monitoring.** Covered persons which are not required, under the AML/CFT Regulations, to have an electronic system of flagging and monitoring transactions shall ensure that they have the means of flagging and monitoring the transactions mentioned in this Section on *Electronic monitoring systems for AML/CFT*. 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.

**Electronic submission of reports.** The CTR and STR shall be submitted to the AMLC in a secured manner, in electronic form and in accordance with the reporting procedures prescribed by the AMLC. The covered persons shall provide complete and accurate information of all the mandatory fields required in the report. In order to provide accurate information, the covered person shall regularly update customer identification information at least once every three (3) years.

For the purpose of reporting in a secured manner, all covered persons shall register with the AMLC within ninety (90) days from 27 January 2011 by directly coordinating with that office for the proper assignment of their institution code and facilitation of the reporting process. All covered institutions that have previously registered need not re-register.

Only their respective compliance officers shall electronically sign their CTRs and STRs.

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

**Exemption from bank secrecy laws.** When reporting covered or suspicious transactions to the AMLC, covered persons and their officers and employees shall not be deemed to have violated R.A. No. 1405, as amended, R.A. No. 6426, as amended, R.A. No. 8791 and other similar laws, but are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person, the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. In case of violation thereof, the concerned officer and employee of the covered person shall be criminally liable in accordance with the provision of the AMLA, as amended.

**Confidentiality provision.** When reporting CTs and STs to the AMLC, covered persons, their directors, officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction report was made, the contents thereof, 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 director, officer and employee of the covered person shall be criminally liable.

**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 in good faith, whether or not such reporting results in any criminal prosecution under the AMLA, as amended, its RIRR or any other law.

**Private banking/wealth management operations.** These services, which by their nature involve a high measure of client confidentiality, are more open to the elements of reputational risk especially if the customer identification process is not diligently followed. Covered persons shall therefore establish and record the true and full identity and take reasonable measures to establish the source of wealth and source of funds, of the customer and beneficial owners, if any, and establish a policy on what standard of due diligence will apply to them. They shall also require approval by a senior officer other than the private banking/wealth management/similar activity relationship officer or the like for acceptance of customers of private banking, wealth management and similar activities.

**PEP.** Covered persons shall establish and record the true and full identity of PEPs, as well as their immediate family members and entities related to them.

- a. In case of domestic PEPs or persons who have been entrusted with a prominent function by an international organization, or their immediate family members or close associates, in addition to performing the applicable due diligence measures, covered persons shall:
  - (1) Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
  - (2) In cases when there is a higher risk business relationship, adopt measures under paragraphs "b(2)" to "b(4)" below.
- b. In relation to foreign PEPs or their immediate family members or close associates, in addition to performing the applicable customer due diligence measures, covered persons shall:
  - (1) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
  - (2) Obtain senior management approval before establishing (or continuing, for existing customers) such business relationship;
  - (3) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
  - (4) Conduct enhanced ongoing monitoring on that relationship.

**Correspondent banking.** Covered persons shall adopt policies and procedures to prevent correspondent banking activities from being utilized for ML/TF activities, and designate an officer responsible for ensuring compliance with these regulations and the covered person's policies and procedures.

The Guidelines on Correspondent Banking Relationships are provided in *Appendix 140*.

**Supervisory enforcement action.** Consistent with Sec. 002, the Bangko Sentral may deploy enforcement actions to promote adherence to the requirements set forth in this Section and bring about timely corrective actions.

**Fund/Wire transfer.** Because of the risks associated with dealing with fund/wire transfers, where a covered person may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, it shall establish policies and procedures designed to prevent it from being utilized for that purpose which shall include, but not limited to, the following:

- a. Originating financial institution:
  - (1) Shall not accept instructions to fund/wire transfer from a non-customer originator, for occasional transactions exceeding the set threshold as defined in this Part, unless it has conducted the necessary CDD to establish the true and full identity and existence of said originator;
  - (2) Shall ensure that all wire transfers are always accompanied by the required information such that:
    - (a) Cross border and domestic fund/wire transfers and related message not exceeding P50,000.00 or its equivalent in foreign currency, shall include accurate and meaningful originator and beneficiary information. The following information shall remain with the transfer or related message through the payment chain:

- (i) Name of the originator;
  - (ii) Name of the beneficiary; and
  - (iii) Account number of the originator and beneficiary, or in its absence, a unique reference number.
- (b) For cross border and domestic fund/wire transfers and related message amounting to P50,000.00 or more, or its equivalent in foreign currency, the following information shall be obtained and accompany the wire transfer:
- (i) Name of the originator;
  - (ii) Originator account number where such an account is used to process the transaction or a unique transaction reference number which permits traceability of the transaction;
  - (iii) Originator's address, or national identity number, or customer identification number, or date and place of birth;
  - (iv) Name of the beneficiary; and
  - (v) Beneficiary account number where such an account is used to process the transaction, or unique transaction reference number which permits traceability of the transaction.

For domestic wire transfers, the originating institution should ensure that the required information accompanies the wire transfers, unless this information can be made available to the beneficiary institution and relevant authorities by other effective means. In the latter case, the originating institution shall include only the account number or a unique identifier within the message or payment form which will allow the transaction to be traced back to the originator or beneficiary. Originating institutions are required to provide the information within three (3) working days from receiving the request either from the beneficiary institution or from relevant authorities or agencies.

- (3) May be exempted from the requirements of Item "(2)" above in respect of originator information, where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries: *Provided*, That it includes the originator's account number or unique transaction reference number and that the batch file contains the required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country;
  - (4) Need not verify for accuracy the information mentioned in Item "(2)(a)" hereof. However, the originating financial institution shall verify the information pertaining to its customer where there is a suspicion of ML/TF;
  - (5) Shall ensure that, for domestic wire transfers, 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 relevant authorities by other effective means;
  - (6) Shall only include the account number or a unique transaction reference number, where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other effective means: *Provided*, That this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The information shall be made available within three (3) working days from receipt of the request either from the beneficiary financial institution or from appropriate authorities;
  - (7) Shall maintain all originator and beneficiary information collected, in accordance with Sec. 924; and
  - (8) Should not execute the wire transfer if the requirements under Item "a" of this Section (*Fund/wire Transfer*), as applicable, are not complied with.
- b. Intermediary financial Institution shall:
- (1) Ensure that, for cross-border wire transfers, all originator and beneficiary information that accompany a wire transfer are retained in the payment message.

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 keep a record of all the information received from the originating financial institution or another intermediary financial institution for at least five (5) years;

- (2) 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;
  - (3) Conduct transactional sanction screening on the payment parties, both for the originator and beneficiary;
  - (4) Adopt 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.
- c. Beneficiary financial institution shall:
- (1) Verify the identity of the beneficiary, if the identity has not been previously verified and maintain this information in accordance with Sec. 924 (*Record Keeping*). Should the originator and beneficiary be the same person, the beneficiary institution may rely on the customer due diligence conducted by the originating institution provided the rules on third party reliance under Sec. 921 (*Customer identification*) are met, treating the originating institution as third party as therein defined;
  - (2) 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 or beneficiary information, as applicable; and
  - (3) Adopt risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information, as applicable; and (b) the appropriate follow-up action.
- d. In case a Money or Value Transfer Service (MVTs) provider controls both the originating and the beneficiary sides of a wire transfer, it shall:
- (1) consider all the information from both the originating and beneficiary sides in order to determine whether an STR has to be filed; and
  - (2) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the AMLC.

***Buyers of cashier's, manager's or certified checks.*** A covered person may sell cashier's, manager's or certified checks only to its existing customers and shall maintain a register of said checks indicating the following information:

- a. True and full name of the buyer or the applicant if buying on behalf of an entity;
- b. Account number;
- c. Date of issuance and the number of the check;
- d. Name of the payee;
- e. Amount; and
- f. Purpose of such transaction.

***Buyers of cashier's, manager's or certified checks other than its existing customer.*** Where an individual or an entity other than an existing customer applies for the issuance of cashier's, manager's or certified checks, the covered person shall, in addition to the information required in Sec. 921 (*Customer identification*), obtain all the identification documents and minimum information required under this Part to establish the true and full identity and existence of the applicant. In no case shall reduced due diligence be applied to the applicant and, where circumstances warrant, enhanced due diligence should be applied.

***Buyers of cashier's, manager's or certified checks in blank or payable to cash, bearer or numbered account.*** A covered person may issue cashier's, manager's or certified checks or other similar instruments in blank or payable to cash, bearer or numbered account subject to the following conditions:

- a. The amount of each check shall not exceed P10,000;
- b. The buyer of the check is properly identified in accordance with its customer acceptance and identification policies and as required under Sec. 921;
- c. A register of said checks indicating all the information required under Sec. 921;
- d. A covered person which issues as well as those which accepts as deposits, said cashier's, manager's or certified checks or other similar instruments issued in blank or payable to cash, bearer or numbered account shall take such measure(s) as may be necessary to ensure that said instruments are not being used/resorted to by the buyer or depositor in furtherance of an ML activity;
- e. The deposit of said instruments shall be subject to the same requirements of scrutiny applicable to cash deposits; and
- f. Transactions involving said instruments should be accordingly reported to the AMLC if there is reasonable ground to suspect that said transactions are being used to launder funds of illegitimate origin.

**Second-endorsed checks.** A covered person shall enforce stricter guidelines in the acceptance of second-endorsed checks including the application of enhanced due diligence to ensure that they are not being used as instruments for money laundering or other illegal activities.

For this purpose, a covered person shall limit the acceptance of second-endorsed checks from properly identified customers and only after establishing that the nature of the business of said customer justifies, or at least makes practical, the deposit of second-endorsed check. In case of isolated transactions involving deposits of second-endorsed checks by customers who are not engaged in trade or business, the true and full identity of the first endorser shall be established and the record of the identification shall also be kept for five (5) years.

**Foreign exchange dealers/money changers/remittance and transfer companies.** A covered person shall require its customers who are remittance and transfer companies, foreign exchange dealers and money changers to submit proof of registration with the Bangko Sentral as part of their customer identification document, and shall only deal with these entities if they are duly registered as such. Also, these customers shall be required to use company accounts for their remitting, foreign exchange dealing and money changing business.

Remittance and transfer companies, foreign exchange dealers and money changers presenting greater risk shall be subject to enhanced due diligence, which includes, among others, requiring proof of registration with the AMLC, reviewing and assessing their AML/CFT program to have reasonable assurance on their AML compliance, obtaining additional information and securing senior management approval for establishing business relationship.

**Other high-risk customer, jurisdiction or geographic location.** A customer from a foreign jurisdiction that is recognized as having inadequate internationally accepted AML standards, or presents greater risk for ML/TF or its associated unlawful activities, shall be subject to enhanced customer due diligence. Information relative to these are available from publicly available information such as the websites of Financial Action Task Force (FATF), FATF Style Regional Bodies (FSRB) like the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities like the OFAC of the U.S. Department of the Treasury, or other reliable third parties such as regulators or exchanges, which shall be a component of a covered person's customer identification process.

Covered persons shall apply countermeasures (such as conduct of enhanced due diligence, limit business relationship or financial transactions with the identified country or persons in that country) proportionate to the risks when called upon to do so by the FATF, or independently of any call by the FATF to do so, when warranted.

**Shell company/shell bank/bearer share entities.** A covered person shall undertake banking relationship with a shell company with extreme caution and always apply enhanced due diligence on both the entity and its beneficial owner/s.

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

*Bearer share entities* refer to those juridical entities where the ownership is accorded to those who possess the bearer share certificate. A covered person dealing with bearer share entities shall conduct enhanced due 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 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.

**Numbered accounts.** No peso and foreign currency non-checking numbered accounts shall be allowed without establishing the true and full identity and existence of customers and applying enhanced due diligence in accordance with Sec. 921 (*Customer acceptance and identification policy*).

Peso and foreign currency non-checking numbered accounts existing prior to 17 October 2001 shall continue to exist but the covered person shall establish the true and full identity and existence of the beneficial owners of such accounts and apply enhanced due diligence in accordance with Sec. 921 (*Customer acceptance and identification policy*).

## 924 RECORD KEEPING

All customer identification records of covered persons shall be maintained and safely stored as long as the account exists. All transaction records and documents of covered persons shall be maintained and safely stored for five (5) years from the date of transaction.

Said records and files shall contain the full and true identity of the owners or holders of the accounts involved in the transactions such as the ID card and photo of individual customers and the documents mentioned in Sec. 921 (*Customer identification*) for entities, customer information file, signature card of authorized signatory/ies, and all other pertinent customer identification documents as well as all factual circumstances and records involved in the transaction. Covered persons shall undertake the necessary adequate security measures to ensure the confidentiality of such files, including all information shared by the group-wide compliance. Covered persons shall prepare and maintain documentation, in accordance with the aforementioned client identification requirements, on their customer accounts relationships and transactions such that any account, relationship or transaction can be reconstructed as to enable the AMLC, and/or the courts to establish an audit trail for money laundering.

**Closed accounts and terminated relationships.** Covered persons shall maintain and safely store all records of customer identification and transactions documents, including the results of any analysis undertaken, for at least five (5) years following the closure of the account, termination of the business relationship or after the date of the occasional transaction.

**Retention of records where the account or customer is the subject of a case.** If a money laundering case has been filed in court involving the account or customer, records must be retained and safely kept beyond the 5-year retention period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

**Safekeeping of records and documents.** The covered person shall designate at least two (2) officers who will be jointly responsible and accountable for the safekeeping of all records and documents required to be retained by the AMLA, as amended, its RIRR and this Part. They shall have the obligation to make these documents and records readily available without delay during Bangko Sentral regular or special examinations.

**Form of records.** Covered persons shall retain all records as originals or in such forms as are admissible in court pursuant to existing laws, such as the E-Commerce Act and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court.

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

For low-risk customers, it is sufficient that covered persons shall maintain and store, in any form, a record of customer information and transactions, but should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

## TRAINING PROGRAM

### 931 AML TRAINING PROGRAM

Covered persons shall formulate an annual AML training program aimed at providing all their responsible officers and personnel with efficient, adequate and continuous education program to enable them to fully and consistently comply with all their obligations under this Part, the AMLA, as amended, and its RIRR.

Training for officers and employees shall include awareness of their respective duties and responsibilities under the MTPP particularly in relation to the customer identification process, record keeping requirements and CT and ST reporting and ample understanding of the internal processes including the chain of command for the reporting and investigation of suspicious and money laundering activities.

The program shall be designed in a manner that will comprise of various focuses for new staff, front-line staff, compliance office staff, internal audit staff, officers, senior management, directors and stockholders. Regular refresher trainings shall likewise be provided in order to guarantee that officers and staff are informed of new developments and issuances related to the prevention of money laundering and terrorism financing as well as reminded of their respective responsibilities vis-à-vis the covered person's processes, policies and procedures.

Covered person's annual AML training program and records of all AML seminars and trainings conducted by the covered institution and/or attended by its personnel (internal or external), including copies of AML seminar/training materials, shall be appropriately kept by the compliance office/unit/department, and should be made available during periodic or special Bangko Sentral examination.

## ENFORCEMENT ACTIONS

### 941 SANCTIONS AND PENALTIES

In line with the objective of ensuring that covered persons maintain high AML/CFT standards in order to protect their safety and soundness as well as protecting the integrity of the national banking and financial system, violation of this Part shall constitute a major violation subject to the following enforcement actions against the board of directors, senior management and line officers, not necessarily according to priority and whenever applicable:

- a. Written reprimand;
- b. Restriction on certain licenses/product, as appropriate;
- c. Suspension or removal from the office they are currently holding; and/or
- d. Disqualification from holding any position in any covered institution.

In addition to the non-monetary sanctions stated above, the Bangko Sentral may also impose monetary penalties computed in accordance with existing regulations and in coordination with the AMLC.

Enforcement action shall be imposed on the basis of the overall assessment of the covered person's AML risk management system. Whenever a covered person's AML compliance system is found to be grossly inadequate, this may be considered as unsafe and unsound banking that may warrant initiation of prompt corrective action.

To implement the enforcement action provision of this Part along with the AML Risk Rating System (ARRS), the following rules shall apply:

- a. An AML Composite rating of 4 and 3 will require no enforcement action.
- b. An AML Composite rating of 2 or 1 will require submission by the covered person to the appropriate department of the Bangko Sentral, of a written action plan duly approved by the BOD aimed at correcting the noted inefficiency in BOD and SM oversight, inadequacy in AML and TF policies and procedures, weakness in internal controls and audit, and/or ineffective implementation within a reasonable period of time.

The appropriate department of the Bangko Sentral shall assess the viability of the plan and shall monitor the covered person's performance.

In the event of non-submission of an acceptable plan within the deadline or failure to implement its action plan, the appropriate department of the Bangko Sentral shall recommend appropriate enforcement action on the covered person and its responsible officers including monetary penalties to be computed on a daily basis until improvements are satisfactorily implemented.

- c. An AML rating of 1 shall also be considered as an unsafe and unsound banking. For this reason, prompt corrective action shall be initiated on the covered person.

***Escalation of enforcement action.*** In cases of heightened AML/CFT supervisory concern as reflected in the overall AML risk rating over a certain period of time, the Bangko Sentral shall impose escalated enforcement action which shall include corrective action, sanction and/or additional supervisory enforcement action, consistent with Sec. 002 on *Supervisory Enforcement Policy*.

***Monetary penalty guidelines.*** These guidelines are divided into three (3) parts.

Part I - *Monetary penalty matrices.* The monetary penalty matrices, where monetary penalties are categorized based on the (1) Composite rating and (2) Asset size of the Bangko Sentral covered institution.

Part II - *Guiding principles.*

- a. The first step is to determine the over-all risk rating of the Bangko Sentral covered institution for purposes of identifying which penalty matrix will be used. If the Composite rating is "1" or "2", penalty matrix A or B, respectively shall be used. If the over-all rating is "3" and "4", no monetary penalty shall be imposed.

- b. Second step is to establish the asset size of the Bangko Sentral covered institution as of the cut-off period of examination;
- c. Third step is to identify the aggravating and mitigating factors. If the aggravating factors are more than the mitigating factors, then the maximum range shall be used. On the other hand, if the mitigating factors are more than the aggravating factors, then the minimum range shall be applied. In case there are no aggravating and mitigating factors or there is a tie, the medium range shall be used.
- d. For Composite ratings of 1 and 2 where the covered institution concerned was required to submit within a reasonable period of time an acceptance plan, non-submission of the plan within the deadline or failure to implement the action plan shall be a basis for imposition of monetary penalties computed on a daily and continuing basis from the time the covered institutions is notified until corrective measures are satisfactorily effected. The penalty may be imposed on the covered institution itself or directly on the Board of Directors as a body, or the individual directors who have direct oversight, or the line officers involved in the management of money laundering and terrorist financing prevention.

Part III - *Aggravating and mitigating factors.*

a. *Aggravating factors*

- (1) *Frequency of the commissions or omissions of specific violation* - Majority of the following violations were noted:
  - (a) Deficient Know Your Customer process
  - (b) Unsatisfactory Covered Transaction reporting system
  - (c) Non-reporting of and Improper Suspicious Transaction reporting
  - (d) Non-compliance with the Record keeping requirement
  - (e) Inadequate AML Training Program
  - (f) Deficient AML Electronic system
- (2) *Duration of violations prior to notification* - This pertains to the length of time prior to the latest notification on the violation. Violations that have been existing for a long time before they were revealed/discovered in the examination or are under the evaluation for a long time due to pending requests or correspondences from covered institutions on whether a violation has actually occurred shall be dealt with through this criterion. Violations *outstanding* for more than one (1) year prior to notification, at the minimum, will qualify as violations outstanding for a long time.
- (3) *Continuation of offense or omission after notification* - This pertains to the persistence of an act or omission after the latest notification on the existence of the violation, either from the appropriate department of the Bangko Sentral or from the Monetary Board and/or Deputy Governor, in cases where the violation has been elevated accordingly. This covers the period after the final notification of the existence of the violation until such time that the violation has been corrected and/or remedied. The corrective action shall be reckoned with from the date of notification.
- (4) *Concealment* - This factor pertains to the cover up of a violation. In evaluating this factor, one shall consider the intention of the party/ies involved and whether pecuniary benefit may accrue accordingly. The act of concealing an act or omission constituting the violation carries with it the intention to defraud regulators. Moreover, the amount of pecuniary benefit, which may or may not accrue from the offense or omission, shall also be considered under this factor.

Concealment may be apparent when a covered institution's personnel purposely complicate the transaction to make it difficult to uncover or refuse to provide information and/or document that would support the violation/offense committed.

- (5) *Loss or risk of loss to bank* - In asserting this factor, "*potential loss*" refers to any time at which the covered institution was in danger of sustaining a loss.

b. *Mitigating factors*

- (1) *Good faith* - is the absence of intention to violate on the part of the erring

individual/entity.

- (2) *Full cooperation* - covered person's personnel or the covered institution immediately took action to correct the violation after it is brought to its attention either verbally or in writing.
- (3) *With positive measures* - covered person's personnel or the covered institution commits to undertake concrete action to correct the violation but is being restrained by valid reasons to take immediate action.
- (4) *Voluntary disclosure of offense* - covered person's personnel or the covered person disclosed the violation before it is discovered in the course of a regular or special examination or off-site monitoring.

#### **942 SEPARABILITY CLAUSE**

If any provision, sections of this Part, or its application to any person or circumstance is held invalid, the other provisions or sections of this Part, and the application of such provision or section to other persons or circumstance shall not be affected thereby.

**REVISION HISTORY**  
**[Version Updated as of 31 December 2023]**

<b>Section</b>	<b>Issuance</b>	<b>Date</b>
904	Circular No. 1182	10 Nov 2023
911	Circular No. 1182	10 Nov 2023
	1154	14 Sep 2022
	Memo No. 2022-030	30 Jun 2022
921	Circular No. 1182	10 Nov 2023
	1170	30 Mar 2023
	Memo No. 2022-044	14 Oct 2022
923	Circular No. 1182	10 Nov 2023
	Memo No. 2022-038	05 Sep 2022
	2022-007	02 Feb 2022
	Circular No. 1078	09 Mar 2020
	1065	03 Dec 2019