



DNFBPs) contains a series of rules that will require the OGOs and SPs (as new covered persons) to define its program and drive effective ways in which AML/CFT/PF practices are embedded throughout the fabric of its operations.

Section 2. Designation of Casinos, OGO and SPs as Covered Persons

Casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations, Offshore Gaming Operators and their Service Providers, as well as such other entities as may be hereafter determined by Casino Regulators, are hereby designated as covered persons under the AMLA.

Section 3. Definition of Terms

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

- (a) "Account" – refers to membership account, customer's credit account, check cashing account, deposit account or any other account opened with a casino, OGO or SP by or on behalf of a customer.
- (b) "Aggregation" – refers to the process of treating multiple or a series of financial transactions, as far as practicable or as soon as consolidated data becomes available, as a single financial transaction if done by or on behalf of a specific customer.
- (c) "Anti-Money Laundering Act" (AMLA) – refers to Republic Act (RA) No. 9160, as amended by RA Nos. 9194, 10167, 10365, 10927 and 11521.
- (d) "Anti-Money Laundering Council" (AMLC) – refers to the financial intelligence unit of the Republic of the Philippines which is the government agency tasked to implement the AMLA, as amended.
- (e) "Appropriate Government Agency" (AGA) – refers to APECO, CEZA, PAGCOR or any other government agency, as may be determined by law.
- (f) "Casino" – refers to a business authorized or operated by the appropriate Government agency to engage in gaming operations, including ship-based and internet-based casinos.
- (g) "Covered Person" – refers to casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations, mother licensees and junket operators (if any). This also includes offshore gaming operators, as well as their service providers by virtue of RA No. 11521.
- (h) "Covered Transaction" – for casinos (including internet and ship-based casinos), refers to a single casino transaction in cash or other monetary instrument involving an amount in excess of Five Million Pesos (Php



5,000,000.00) or its equivalent in any other currency within one (1) business day.

For OGOs and SPs, refers to a transaction in cash or other equivalent monetary instrument involving a total amount **in excess** of Five Hundred Thousand Philippine Pesos (Php500,000.00) or its equivalent in any other currency within one (1) business day.

- (i) "Online Gaming Account" - an electronic account opened by an internet-based casino player to conduct gaming and financial transactions through the Internet-based casino's website.
- (j) "Gaming Employee License" - is an authorization issued by the regulator granting a person the privilege to be employed as a gaming employee within the Philippine jurisdiction. It is a pre-employment and continuing requirement for employment in any gaming establishment in the country.
- (k) "Gaming Operations" – refers to games of chance and variations thereof offered by a covered person, and approved by the regulator under their enabling laws and other applicable issuances. It shall exclude:
 - 1. Traditional Bingo operations authorized by AGA;
 - 2. Lotteries and sweepstakes of the Philippine Charity Sweepstakes Office (PCSO); and
 - 3. Such other games of chance and variations as may be declared exempted by the AGA based on the result of their money laundering and terrorist financing risk assessment in consultation with AMLC.
- (l) "Identification Document" – refers to any of the following documents:
 - 1. For Filipino citizens: those issued by any of the following official authorities:
 - i. Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
 - ii. Government Owned or Controlled Corporations (GOCCs); and
 - iii. Covered persons registered with and supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), the Securities and Exchange Commission (SEC), or the Insurance Commission (IC).
 - 2. For foreign nationals: valid passport or Alien Certificate of Registration. For foreign nationals with low ML/TF risks a covered person may consider the following identification documents:
 - i. identification documents enumerated in Section 4 (l)(1); and
 - ii. National identification card issued by a foreign government.



- (m) "Internet-based Casinos" – refers to casino operations where persons participate by the use of remote communication facilities such as, but not limited to, internet, telephone, television, radio or any other kind of electronic or other technology to facilitate communication.
- (n) "Monetary Instrument" – refers to:
1. Coins or currency of legal tender in the Philippines, or in any other country
 2. Negotiable Checks such as casino checks, personal checks, and bank drafts
 3. Casino Value instrument such as casino chips, casino rewards cards, ticket/voucher in or ticket/voucher out, markers, cashier's orders, chip purchase orders/vouchers, chip checks, gift certificates, and casino drafts; and
 4. Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.
- (o) "Probity Check" - is the process of looking up and compiling criminal records, commercial records, and financial records of an individual or a corporation to determine/assess its suitability to be a licensee.
- (p) "Suspicious Transaction" – refers to transactions with covered persons, regardless of the amounts involved, where any of the following exist:
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.
- (q) "Terrorist Financing" (TF) – as defined under Section 4 of RA No. 10168.



Section 4. Basic Principles and Policies to Combat Money Laundering / Terrorist Financing (ML/TF)

- (a) Satisfactory evidence of the customer's identity should be obtained. The Licensee's Board of Directors and Senior Management shall ensure that the covered person is not used to facilitate ML/TF. They shall be responsible to direct all their employees to exercise utmost diligence to ensure that adequate measures are implemented to prevent the covered person from being unwittingly involved in such a criminal activity.
- (b) Covered persons shall in accordance with law, immediately give the authorized personnel of the AMLC, full access to all information, documents or objects pertaining to the account, casino transaction and/or person subject of the investigation.

Certified true copies of the documents pertaining to account, casino transaction and/or person subject of the investigation shall be submitted within five (5) working days from receipt of the request or order from the AMLC.

- (c) The covered person shall fully cooperate with the CEZA, AMLC, and Law Enforcement Agencies within the legal constraints relating to customer confidentiality, particularly on matters relating to the Data Privacy Act. Appropriate measures such as reporting to the AMLC shall be taken when there are reasonable grounds for suspecting money laundering.
- (d) Policies consistent with the principles set in RA No. 9160, as amended by RA Nos. 9194, 10167, 10365, 10927 and 11521 shall be adopted and properly disseminated. Specific control procedures for customer identification, records keeping and retention of transaction documents and reporting of covered and suspicious transactions shall be implemented.

Section 5. Creation and Implementation of Money Laundering and Terrorist Financing Prevention Program (MLPP)

The covered person's Board of Directors, shall approve, and the AML Compliance Officer shall implement, a comprehensive, risk-based MLPP geared towards the promotion of high ethical and professional standards and the prevention of Money Laundering and Terrorist Financing. The MLPP shall be in writing, consistent with the AMLA, and its provisions shall reflect the covered person's corporate structure and risk profile. It shall be readily available in user friendly form whether in hard or soft copy. Moreover, it shall be well disseminated to all officers and staff who are obligated, given their position, to implement compliance measures. The covered person shall design procedures that ensure an audit trail evidencing the dissemination of the MLPP to relevant officers and staff.

Where a covered person operates at multiple locations in the Philippines,



it shall adopt an institution-wide MLPP to be implemented in a consolidated manner. Lastly, the MLPP shall be updated at least once every two (2) years or whenever necessary to reflect changes in the AML/CFT obligations, Money Laundering and Terrorist Financing trends, detection techniques and typologies.

At a minimum, the MLPP provisions shall include:

- i. Detailed procedures of the covered person's compliance and implementation of the following major requirements of the AMLA, the CIRR, the DNFBP Guidelines and this regulation:
 - i.i Customer identification process, including acceptance policies and an on-going monitoring process;
 - i.ii Record keeping and retention;
 - i.iii Covered transaction reporting; and
 - i.iv Suspicious transaction reporting.

The covered person shall adopt a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount and a system to monitor aggregated transactions that would breach the threshold for a covered transaction report.

Suspicious transaction reporting shall include a reporting chain under which a suspicious transaction will be processed and the designation of a Board-level or approved Committee who will ultimately decide whether or not the covered institution should file a report to AMLC.

- ii. An effective and continuous AML/CFT training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under the AMLA, this CIRR and other applicable issuances, their own internal policies and procedures, and such other obligations as may be required by the AMLC and AGA;
- iii. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personnel with no criminal record or integrity-related issues are employed or contracted by the covered person;
- iv. An internal audit system and an independent audit program that will ensure the completeness and accuracy of information obtained from customers. The covered person shall specify in writing the examination scope of independent audits, which shall include ensuring checking the accuracy and completeness of identification documents, covered transaction report (CTR) and suspicious transaction report (STR) submitted to the AMLC, and records retained in compliance with this framework, as well as assuring



adequacy and effectiveness of the covered person's training programs;

- v. A mechanism that ensures all deficiencies noted during the audit and/or regular or special inspection/examination are immediately corrected and acted upon;
- vi. Cooperation with the AMLC and CEZA;
- vii. Designation of an AML compliance officer, who shall, at least, be of a senior management level, as the lead implementor of the covered person's compliance program; and
- viii. The identification, assessment, and mitigation of ML/TF risks that may arise from new business practices, services, technologies, and products.

Section 6. Customer Due Diligence (CDD)

A. Covered persons must apply CDD measures under the following circumstances:

- (a) When an uncarded customer:
 - i. participates or joins its membership program;
 - ii. when a customer creates an online gaming account for internet-casino;
 - iii. engages in an aggregate financial transaction in excess of Five Hundred Thousand (500,000.00) Philippine Pesos or its equivalent in foreign currency;
- (b) When customers make use of any financial services;
- (c) When it becomes aware of circumstances which alter the current ML/TF risk profile of a carded customer, including, but not limited to the following:
 - i. When there is an indication that the identity of the customer, or of the customer's beneficial owner, has changed.
 - ii. When customer's transaction is not reasonably consistent with the covered person's knowledge of the customer.
 - iii. When there is a change in the purpose or intended nature of the covered person's relationship with the customer.
 - iv. Any other circumstances which could affect the covered person's assessment of the ML/TF risk in relation to the customer.
- (d) When the covered person suspects money laundering or terrorist financing.
- (e) When the covered person doubts the veracity or adequacy of documents or information previously obtained for the purpose of identification or verification.



- B. Covered persons are required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that it is satisfied that it knows who the beneficial owner is.
- C. Covered persons are required to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.
- D. Covered persons are required to conduct ongoing due diligence on the business relationship, including:
 - (a) scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the covered persons knowledge of the customer, their risk profile, including where necessary, the source of funds; and
 - (b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.
- E. Covered persons are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:
 - (a) this occurs as soon as reasonably practicable;
 - (b) this is essential not to interrupt the normal conduct of business; and
 - (c) the ML/TF risks are effectively managed.
- F. Covered persons are required to adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.
- G. Covered persons are required to apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.
- H. Covered persons are required to perform enhanced due diligence where the ML/TF risks are higher.
- I. Covered persons may apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or by the covered person. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of ML/TF, or specific higher risk scenarios apply.
- J. Where the covered persons are unable to comply with relevant CDD measures:
 - (a) it should be required not to open the membership account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and
 - (b) it should be required to consider making a suspicious transaction report (STR) in relation to the customer.



- K. In cases where the covered persons form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they may not pursue the CDD process, and file an STR.
- L. Covered persons shall take all steps necessary to be able to establish the true and full identity of each customer and, to the extent possible, the intermediary and the person or entity on whose behalf the transaction is being conducted.

Section 6. Third Party Reliance

- (a) Covered persons may rely on third-party financial institutions and DNFBPs to perform elements the CDD measures (identification of the customer; identification of the beneficial owner; and understanding the nature of the business) or to introduce business, the ultimate responsibility for CDD measures should remain with the covered person relying on the third party, which should be required to:
- i. obtain immediately the necessary information concerning the CDD measures;
 - ii. take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
 - iii. 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) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.
- (c) Covered persons that rely on a third party that is part of the same business group, shall comply with requirements of the criteria above in the following circumstances:
- i. the group applies CDD and record-keeping requirements, and programmes against money laundering and terrorist financing;
 - ii. the implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and
 - iii. any higher country risk is adequately mitigated by the group's AML/CFT policies.

Section 7. Record-keeping

- (a) Record-keeping – all CDD records and business correspondence, and results of any analysis undertaken and covered person transactions of customers shall be maintained and safely stored for at least five (5)



years, except for records of video footage, where casinos may enforce a risk-based approach, provided that suspicious activities and STR-related footage are kept for 5 years or as otherwise allowed by the AMLC. If a case has been filed in court, records including video footage must be retained and safely kept beyond the five (5)-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved.

- (b) Record Safekeeping – a covered person shall designate an officer to be responsible and accountable for all record-keeping requirements. The officer will also be responsible for making these records available to the AMLC and AGA upon request. Covered persons shall maintain records in an organized and confidential manner which allows the AMLC, AGA, the courts and any auditor establish an audit trail for money laundering and terrorist financing activities, if any, and to assess its compliance program.
- (c) Form of Records – records should be sufficient to permit reconstruction of individual transactions and retained as originals or copies in such forms as admissible in court pursuant to existing laws, such as RA No. 8792 or the E-Commerce Act and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court.
- (d) For internet casino or proxy betting service - In addition to the required information above, the junket operator through the Licensee shall submit the names, IP address, and any other data pertaining to the identity of the person who logged in the site and was given access to view the video streaming for purposes of monitoring.
- (e) Covered persons are required to ensure that all CDD information and transaction records are available swiftly to the AMLC or AGA.

Section 8. Transaction Reporting

- (a) Reporting of Covered and Suspicious Transactions – covered persons shall report to the AMLC all: (i) covered transactions within five (5) working days from date of the transaction; and (2) suspicious transactions within the next working day from the occurrence thereof.

For suspicious transactions, “occurrence” refers to the date of determination of the suspicious transaction, which determination shall 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 period transacting is involved in or connected to, a predicate offense 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 transaction and a suspicious transaction, it shall be reported as a suspicious transaction.

- (b) **Substance and form of reports** – covered persons shall ensure the accuracy and completeness of CTRs and STRs, which shall be filed in the form prescribed by the AMLC and shall be submitted in a secured manner to the AMLC in electronic form. In order to provide accurate information, the casino shall regularly update customer identification information at least once every five (5) years on the basis of risk and materiality.
- (c) **Confidentiality of Reporting** – when reporting covered transactions, covered persons, and their officers and employees, are prohibited from communicating directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction has been or is about to be reported, the contents of the report, or any other information in relation thereto. 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.
- (d) **Safe Harbor** - Covered persons and their directors, officers and employees shall be exempt from any criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if the suspicious transaction report was performed in good faith. The exemption shall apply even if the underlying unlawful activity was reported is not accurate, and regardless of whether illegal activity actually occurred.

Section 9. Training

As part of an effective anti-money laundering program, this Regulation shall require all licensee to have an employee training program as determined by AML Compliance Officer and in coordination with the AMLC. This will ensure that training on the principles of anti-money laundering is provided to all employees engaged in the operation of Casino games, Casino marketing employees, Surveillance employees, Cage employees. The training shall cover, but not limited to:

- (a) Customer Due Diligence
- (b) Identifying suspicious activity
- (c) Records keeping Covered transaction reporting and Suspicious transaction reporting



Section 10. Employee Screening

To ensure that covered person being regulated by AGA are of integrity, all employees must be screened thoroughly before recruitment through interviews and/or other related documents pertaining to their identity.

Section 11. Independent Internal Audit System

All covered persons shall have an AML/CFT audit system whose report/findings shall be directly reported to the Board for appropriate action.

The internal audit function is responsible for the periodic and comprehensive evaluation of the AML/CFT risk management framework of covered persons and is independent of the units being audited. It should have the support and has a direct reporting line to the Board of Directors and Senior Management of the Company.

Covered person's MLPP should have a mechanism that ensures all deficiencies noted during the audit and/or regular or special inspection/examination are immediately corrected and acted upon.

Section 12. Cooperation with the AMLC and CEZA

Covered persons shall fully cooperate with the AMLC, CEZA as well as other regulatory and law enforcement agencies, within the legal constraints relating to customer confidentiality (particularly on matters relating to the Data Privacy Act of 2012), when an audit is being conducted or an investigation is being undertaken. Appropriate measures (such as reporting to CEZA and/or AMLC) shall be taken when there are reasonable grounds for suspecting ML/TF/PF.

Section 13. Designation of a Compliance Officer and/or Office

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

If a covered person's activities are complex or if it maintains multiple business locations, it shall make and document a decision as to whether or not it will be necessary to create a compliance office or to appoint a compliance officer for each of the covered person's locations. This decision shall take into consideration the



similarity of risks posed to the covered person's various operations, including but not limited to, distinctions in customers/clients, transactions, services offered, as well as the location between business locations.

The covered person shall also designate a separate officer to be responsible and accountable for all record-keeping requirements. These officers will also be responsible for making these records readily available to the AMLC or CEZA upon request.

Section 14. Risk Assessment

Covered persons are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Covered persons are required to:

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

Section 14. Higher Risk Jurisdictions

Covered persons are required to apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with its customers from countries for which this is called for by the FATF.

Section 15. AML/CFT Controls for Branches and Subsidiaries

- (a) Covered person groups should be required to implement group-wide MLPP, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the business group. These should include the minimum components of an MLPP and also:
 - a. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;
 - b. the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done). Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and
 - c. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.



- (b) Covered persons are required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the AMLA requirements, where the minimum AML/CFT requirements of the host country are less strict than those of the AMLA, to the extent that host country laws and regulations permit.

If the host country does not permit the proper implementation of AML/CFT measures consistent with the AMLA requirements, financial groups should be required to apply appropriate additional measures to manage the ML/TF risks, and inform AGA.

Section 15. List of Offenses and Corresponding Penalties, Sanctions, or Other Measures

(a) General Guidelines

1. Based on the nature of the offense, each offense will correspond to a penalty or sanction.
2. Grave offenses can be accorded with suspension or forfeiture of the Provisional License as AGA may deem justifiable.
3. In the event of non-compliance with the provisions of this Regulation or specific provisions of the AMLC guidelines/resolutions, GLDD shall issue a "Notice of Non-Compliance" to the Licensee who in turn shall pay or comply with the corresponding penalty or sanction.

(b) Nature of Offense – for this purpose, the nature of offense shall be classified as follows:

1. Customer Due Diligence - [Section 6(a-d)]
2. Record Keeping - [Section 7(a-c)]
3. Transaction Reporting - [Section 8(a-c)]
4. Money Laundering Prevention Program – (Section 5)
5. Violations of Orders, Resolutions and other Issuances of the AMLC

(c) The following are fines per violation based on the gravity of violation:

VIOLATION	AMOUNT OF FINE (IN PHP)
Grave	400,000.00 to 500,000.00
Major	300,000.00 to 400,000.00
Serious	200,000.00 to 300,000.00
Less Serious	100,000.00 to 200,000.00
Light	100,000.00 and below

(d) Table of Offenses



VIOLATIONS		SANCTION
Grave Violations		Fine is on a per account basis
1.	Non-compliance with the requirement to immediately give AMLC and/or its Secretariat full access to all information, documents or objects pertaining to the deposit, investment, account, transaction, and/or person subject of inquiry or investigation.	
Major Violations		
2.	Non-compliance with the requirement to establish and record the true identity of each customer and/or the person whose behalf the transaction is being conducted.	Fine is on a per customer basis
3.	Non-compliance with the requirement to retain and safely keep records beyond the five (5) year period, where the account is the subject of the case, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.	Fine is on a per account basis
4.	Non-compliance with the requirement to report to the AMLC covered and suspicious transactions.	Fine is on a per transaction basis
Serious Violations		
5.	Non-compliance with the requirements to monitor and update all information and identification of documents of existing customers	Fine is on a per customer basis
6.	Allowing the opening of anonymous accounts, accounts under fictitious names, and all other similar accounts.	Fine is on a per account basis
7.	Non-compliance with the requirement to maintain and safely store for five (5) years from the dates of transactions, or from dates the accounts were closed, all records of	Fine is on a per account basis



	transactions, including customer identification documents.	
8.	Non-compliance with the requirement to submit certified true copies of the documents pertaining to deposit, investment, account, transaction, and/or person subject of inquiry or investigation, within five (5) working days from receipt of the court order or AMLC Resolution	Fine is on a per account basis
9.	Non-compliance with the requirement to formulate a Money Laundering Prevention Program in accordance with the provisions of the AMLA, its RIRR, all AMLC issuances, and the anti-money laundering guidelines and circulars of the Supervising Authorities	Fine is on a per examination period
10.	Violation of orders, resolutions and other issuances of the AMLC	Fine is on a per resolution, rule, regulation, circular, order and guideline basis
Less Serious		
11.	Non-compliance with the requirement to obtain all the minimum information required from individual customer and juridical entities	Fine is on a per account basis
12.	Non-compliance with the requirement to indicate the true name of the account holder in Covered Transaction Reports (CTR) and Suspicious Transaction Reports (STR) involving non-checking numbered accounts	Fine is on a per transaction basis
13.	Non-compliance with the requirement to provide all responsible officers and personnel with efficient and effective anti-money laundering training and education programs	Fine is on a per examination period
Light Violations		
14.	Non-compliance with the requirement to keep electronic copies of all CTRs or STRs for, at least, five (5) years from the dates of submission to the AMLC	Fine is on a per violation basis

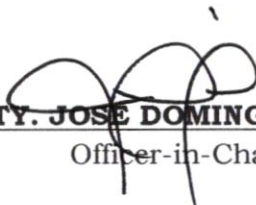


Section 14. Repealing Clause.

All administrative orders, memoranda, circulars and resolutions or any parts thereof which are inconsistent herewith are hereby repealed, amended or modified accordingly.


Section 15. Effectivity.

This Memorandum Circular shall take effect immediately upon its signing.


ATTY. JOSE DOMINGO L. TAN
Officer-in-Charge

Date: 04 / 13 / 2023



 APPROVED