Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila

Advisory No:	RS-2024-002
Classification:	**Regulatory and Supervisory Advisory**
Date:	30 January 2024

INSURANCE COMMISSION ADVISORY

TO : **All Insurance/Reinsurance Companies, Mutual Benefit Association, Trusts for Charitable Uses, Insurance and Reinsurance Brokers, Pre-Need Companies and Health Maintenance Organization**

SUBJECT : **Dissemination of the AMLC Advisory Urging Entities to Apply Risk-Based Measures Against Money Laundering (ML) and Terrorism Financing (TF) for Customers, Including Transactors**

The attached advisory from Anti-Money Laundering Council (AMLC) reminds Covered Persons (CPs) to implement risk-based preventive measures against money laundering (ML) and terrorism financing (TF) on its customers, including transactors.

Transactors are any person, other than the account owner/ holder, who transacts business with a covered person. Covered persons should conduct risk-based CDD measures, keep all CDD and transaction records for at least five years, and file covered and suspicious transaction records based on the latest AMLC Registration and Reporting Guidelines.

This Commission encourages all Insurance Commission Regulated Entities (ICREs) to adopt a proactive approach in implementing these requirements to maintain their compliance with the AMLC regulations.

For your information and guidance.

REYNALDO A. REGALADO
Insurance Commissioner

Republic of the Philippines
ANTI-MONEY LAUNDERING COUNCIL

ADVISORY

Subject: **Reminder for Covered Persons to Implement Risk-based Preventive Measures against Money Laundering and Terrorism Financing on Its Customers, including Transactors**

The Anti-Money Laundering Council (AMLC) reminds all covered persons of their duty to implement risk-based Customer Due Diligence (CDD), Record-keeping, and Transaction Reporting measures on its customers, particularly the transactors.

Transactors are Customers

Rule 2, Section 1(z) of the 2018 Implementing Rules and Regulations (IRR) of Republic act (RA) No. 9160, otherwise known as The Anti-Money Laundering Act of 2001, as amended (AMLA), defines the term "Customer/Client" as follows:

> *(z) "Customer/Client" refers to any person who keeps or maintains an account, or **otherwise transacts business with a covered person**. It includes the following:*
>
> *(1) Beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained or a transaction is conducted;*
> *(2) **Transactors**, agents and other authorized representatives of beneficial owners;*
> *(3) Beneficiaries of trusts, investment and pension funds, insurance policies, and remittance transactions;*
> *(5) Persons whose assets are managed by an asset manager;*
> *(5) Trustors/grantors/settlors of a trust;*
> *(6) Insurance policy holders, whether actual or prospective; and*
> *(7) Juridical person.*
>
> *For purposes of this Rule, 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.*

Under the foregoing definition, the term transactor is understood to mean any person, other than the account owner/holder who transacts business with a covered person. Transacting business includes all activities relative to the regular business, service, or product being offered or performed by a covered person, regardless if it results in account opening or actual movement of funds.

A transactor should be distinguished from the authorized agent or representative of the account owner/holder. A transactor acts on his or her behalf, thus, all his or her transactions should be attributed to him or her. On the other hand, an authorized agent or representative is the registered or official personnel acting for and on behalf of an account owner/holder.

Customer Due Diligence

Since transactors are customers, it is emphasized that the conduct of CDD measures applies to them, subject to the implementation of the risk-based approach. Considering that a transactor is acting for him or herself, the covered person should treat him or her as a principal customer that is not maintaining an account. However, for purposes of monitoring, it is advised that transactors be given unique identification or reference numbers—which will also be essential for *Transaction Reporting*.

Risk-based CDD

At the heart of an effective and efficient CDD is the implementation of the risk-based approach. Covered persons shall assess their customers, including transactors, to determine who are likely to pose low, normal, or high risk to money laundering/terrorism financing (ML/TF). The covered person shall document the risk profiling results, as well as how a customer was profiled and the standard of CDD applied.

Covered persons shall set the standards in applying Reduced Due Diligence (RDD), Average Due Diligence (ADD), and Enhanced Due Diligence (EDD), including a set of conditions for continuance or discontinuance of transaction or business relationship. This shall be indicated in the Money Laundering/Terrorism Financing Prevention Program (MTPP) of the covered persons.

Without a documented risk profiling/assessment that would support a finding that a particular transactor or transactors in general (as a category of customers) are low risk to ML/TF, the standards for ADD shall be applied to them by default.

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

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

Customer Identification Process

The Customer Identification Process (CIP) under Rule 18, Section 3 of the 2018 IRR is the most basic CDD measure. CIP is about obtaining the required identification information and identification document to capture the profile of customers, including transactors.

All the identification information and identification document under Rule 18, Section 3.4 of the 2018 IRR that are applicable to account owners/holders apply to transactors, unless they were found to be of low risk to ML/TF and RDD is applied to them—in which case, covered persons can reduce the information required to the bare minimum to identify the transactors:

(a) The minimum identification information to capture the identity of low-risk customers are the Name, Address, and Date of Birth.

(b) The identification document for low-risk customers shall be any document or information reduced in writing which the covered person deems sufficient to establish the client's identity. This may be in the form of manual entries in a logbook, spreadsheet, or electronic database.

The foregoing requirements, however, do not preclude the covered persons from requiring more identification information (but less than those required for ADD) or accept formal identification documents.

The presentation of the Philippine Identification System (PhilSys) Number (PSN) and the PhilSys ID (PhilID) card shall always be considered as official and sufficient proof of identity, subject to the authentication requirements under the PhilSys Act and its IRR.

Customer Verification Process

The Customer Verification Process (CVP) under Rule 18, Section 4 of the 2018 IRR is about validation of the truthfulness of the information and confirmation of the authenticity of the identification documents presented, submitted, and provided by customers, using reliable and independent sources, documents, data, or information.

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

(a) completion occurs as soon as reasonably practicable;

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

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

Notably, covered persons are allowed to adopt risk management procedures concerning the conditions under which customers, including transactors, may utilize the business or professional relationship prior to the conduct of CVP. This requirement is key to applying risk-based CDD on low-risk transactors.

Identification and Verification of Agents

The Identification and Verification of Agents (IVA) process under Rule 18, Section 5 of the 2018 IRR requires covered persons to verify that any person purporting to act on behalf of an account owner/holder is so authorized and identify and verify the identity of those person.

The authority of authorized agents and representatives can be validated through the registration (if the mechanism is available) with the covered person, or presentation of a power of attorney or equivalent document, which the covered person deems acceptable and sufficient to prove authority from the account owner/holder.

Beneficial Ownership Verification

The Beneficial Ownership Verification (BOV) process under Rule 18, Section 6 of the 2018 IRR requires covered persons 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 reliable sources, such that the covered person is satisfied that it knows who the beneficial owner is.

In relation to transactors, the beneficial owners are the beneficiary of the transactions, especially for the fund transfers.

Determination of the Purpose of Relationship

The Determination of the Purpose of Relationship (DPR) process under Rule 18, Section 7 of the 2018 IRR requires covered persons to understand and, as appropriate, obtain information on the purpose and intended nature of the account, transaction, or the business or professional relationship with their customers.

Conducting DPR as part of the CDD on transactors is particularly important considering the absence of a formal account being kept by the said customer. Each transaction of the transactor should have a clear purpose to reduce the risk of the transaction being used for ML/TF purposes.

Ongoing Monitoring Process

The Ongoing Monitoring Process (OMP) under Rule 18, Section 8 of the 2018 IRR requires covered persons, on the basis of materiality and risk, to conduct ongoing monitoring by establishing a system that will enable them to understand the normal and reasonable account or business activity of customers, including transactors, and scrutinize transactions undertaken throughout the course of the business or professional relationship to ensure that the customers' accounts, including transactions being conducted, are consistent with the covered person's knowledge of its customer, their business and risk profile, including where necessary, the source of funds.

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

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

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

(c) Indicates that any of the suspicious circumstances exists.

Failure to Satisfactorily Complete CDD

Covered persons who are unable to comply with the relevant CDD measures shall: (a) refuse to open an account, (b) commence business relations, or (c) terminate the business relationship. In cases of transactors who were not properly subjected to CDD, covered persons shall refuse to execute the transaction.

Updating of Account Opening Form/Customer Information Form

Covered persons are expected to strictly observe the foregoing CDD requirements. Accordingly, their *Account Opening Form/Customer Information Form* or other similar forms or records shall be updated.

For economy purposes, covered persons with stocks of pre-printed forms can still use the same, provided that the required information from transactors are stamped or attached to the said forms, or otherwise captured or recorded by the covered persons.

Record-Keeping

We further remind the covered persons of their duty to keep all CDD and transaction records, especially those who are subject of AMLC investigation/prosecution, for at least five (5) years, as prescribed under Rule 22 of the 2018 IRR.

Covered persons shall retain all transaction records either in:

(a) their original forms; or

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

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

The Guidelines on the Digitization of Customer Records (DIGICUR Guidelines) applies to transactors of all covered persons, except to those transacting with the Money Service Businesses (MSBs). However, if the business model of the MSB is such that the customers, including transactors,

are able to open, keep, and maintain an account as an electronic wallet or other similar electronic product or service, then that MSB must still observe the DIGICUR Guidelines.

Transaction Reporting

We also remind all covered persons to completely, accurately, and timely report covered and suspicious transactions, in accordance with the latest *AMLC Registration and Reporting Guidelines (ARRG)*.

Under the current ARRG, the covered and suspicious transactions of the transactors shall be reported as follows:

(a) For covered transactions, the covered persons shall report the same using the same process and requirements as reporting of.

The name of the transactor shall be included under Party Type T (Transactor). The covered person shall indicate the name and address of the transactor.

The Customer Reference number under Party Type T shall indicate a unique number which shall refer to the transactor being reported.

The recipient of the fund (i.e., account owner/holder) shall be indicated under Party Type A (Account Holder)

(b) For suspicious transactions, the covered person shall report the same using the appropriate transaction code.

The covered person shall indicate the name and address of the transactor under Party Type T. The covered person shall indicate the name and address of the transactor.

The Customer Reference number under Party Type T shall indicate a unique number which shall refer to the transactor being reported.

The recipient of the fund (i.e., account owner/holder) shall be indicated under the Party Type A (Account Holder) and all mandatory fields for a suspicious transaction report for Party Type A, as per the 2021 ARRG.

Further, covered persons shall ensure that the narrative field is enriched with supporting descriptions of the transaction. It should contain all the details and events leading to the suspicion including other information which might be of help or importance to the report.

Please note that the foregoing reporting process for transactors may change in the upcoming ARRG amendment, which is targeted to take effect by 2024.

Other Preventive Measures

New Technologies

Pursuant to Rule 19, Section 5.3 of the 2018 IRR, covered persons shall undertake risk assessments prior to the launch or use of such products, practices, and technologies. This requirement covers the adoption of non-face-to-face modes of fund transfers and other transactions, like in the case of Cash Deposit Machines (CDMs).

Covered persons shall take appropriate measures to manage and mitigate the risks arising from the launch or use of such products, practices, and technologies. The adoption of new technologies shall not be an excuse for covered persons not to implement the relevant preventive measures against ML/TF. Technology in not incompatible with CDD.

However, depending on the nature of the technology to be adopted, the mode and manner of conducting the preventive measures, especially CDD, may vary depending on how the covered person intends to integrate it with the new technology. These modes and manner of conducting the preventive measure shall be clearly indicated in the MTPP. For example, CDD can be conducted by integrating in the CDMs the capability to read specific identification cards, like ATM and debit/credit cards, u-MID cards, and PhilID cards. Another option is to incorporate in the CDMs the ability to require transactors to encode their personal information (i.e., name, address, and date of birth) and take their photos before proceeding with the transaction.

Should there be any queries or questions related to the matter, you may refer your concern to the AMLC's Counseling, Adjudication, and Mutual Legal Assistance Unit (CAMU) with contact number at 8708-7069 or the Compliance Supervision Group (CSG) with contact number at 8708-7067 and 5302-3848. You may also e-mail your concerns at secretariat@amlc.gov.ph.

Please be guided accordingly.