

AML AND CTF COMPLIANCE QUESTIONNAIRE

ARIANS INSURANCE BROKER INC.

NAME OF ICRE

July 15, 2021

Date Accomplished

A. BOARD OF DIRECTOR AND SENIOR MANAGEMENT OVERSIGHT

1. Board of Director (BOD) and Senior Management (SM) Oversight

- a. Is there a clear guidance from the BOD of the entity's strategic and operational plans and objectives in ensuring that the entity shall not be used as a ML and TF conduit? If so, please describe including the budget allocations to implement these plans and objectives. Have these plans and objectives been cascaded to Senior Management and responsible officers and employees? If so, state how this was done.

Yes. ARIANS has instituted its risk mitigation strategies and operational plans to arrest and address any attempt to utilize it as a conduit in ML and TF activities. The BOD's responsibility apart from its usual corporate responsibilities, monitors and ascertains that ARIANS complies with regulatory practices, in particular Republic Act No 9160, otherwise known as the Anti Money Laundering Act of the Philippines and its Implementing Rules and Regulations set by AML Council.

Moreover, the BOD and Senior Management are in consonance with the entity's adequate management and all information related to AML and TF is cascaded to the officers and employees through memorandums and providing them with pertinent IC Circulars and legal publications regarding the matter. Senior Management' awareness, involvement and responsibility are vital in ensuring adequate AML and TF systems and controls are in place and that appropriate resources are allocated to mitigate identified risks. The entity's policies and procedures relating to AML and TF is reviewed regularly to ensure that sound business practices is followed strictly.

- b. In relation to question no. 1, please describe the control policies and mechanisms (e.g. reportorial requirements, rewards and disciplinary system, training program, etc.) adopted by the BOD to attain these policies and objectives.

The BOD and Senior Management provide regular evaluation for the proper and efficient implementation of AML laws and TF laws and its program including on-going

monitoring of performance by staff and officers who may be involved in ML and TF prevention. Since the entity is comprised only of four (4) Officers and two (2) Staff, the company is able to trace quickly should there be anomalous transactions. Also, ARIANS was incorporated only in mid-2017 so the client base is still lean. Profiling of clients and risk evaluation is well-controlled and due diligence is practiced at all times.

- c. Please describe the entity's framework for ML and TF prevention. What are the roles of the BOD, Senior Management, Compliance Office, Internal Audit and other Offices in ML and TF prevention? What reports are required to be submitted to the BOD to assist them in their decision-making processes?

ARIANS framework for ML and TF are the ff:

- Good Board level and senior management understanding of the AML and TF risks , the materiality to the business ;
- Swift and effective senior management-led response to any significant AML and TF events should it arise;
- Accurate Information System is in place to determine the client's profile, nature of business and market relevance.

- d. Please describe the risk managementsystem relative to ML and TF prevention.

Risk Management System is a specific obligation that adequately addresses the money laundering risks which take into account any vulnerability of its products, services, and customers. It is established to limit the institution's exposure for AML and TF risk. An effective counter on the AML/TF risks arising from exposure to customers, products and services, delivery channels and other activities related thereto and other incidents which include mechanisms that must be reported when company's rules and guidelines have been breached.

- e. Does the Compliance Office/Officer report directly to the BOD? If not, to whom does the Compliance office/officer report? How frequent is this done?

Yes. The Compliance Officer shall report directly to the BOD on all matters related to AML and Terrorist Financing compliance and their insurance risk management.

- f. Please describe the authorities delegated by the BOD to the Compliance Office and the AML and CTF Compliance Officer related to ML and TF prevention.

The Compliance Officer is responsible for overseeing, coordinating and managing the proper and efficient implementation of AML / CTF program.

- g. What other relevant oversight does the BOD and Senior Management exercise to ensure attainment of the entity's plans and objectives relative to ML and TF prevention?

The BOD and Senior Management adopts and ensure attainment of the entity's plans and objectives in a comprehensive and risk-based approach geared towards the promotion of high ethical and professional standards in the prevention of the entity's being used, intentionally or unintentionally, for money laundering and terrorism financing.

2. Identification, Measurement, Monitoring and Controlling of Risks and Problems Related to ML and TF

- a. Have you conducted risk profiling of all existing customers? If not all, what percentage of the total customers count had been profiled?

Yes. The company verifies at a reasonable level of certainty the identities of existing clients through assessing and understanding its ML and TF risks.

- b. Have you conducted an assessment of the risks and vulnerabilities that your entity is exposed into? Please describe how the assessment was done.

Yes. Assessment of the risks and vulnerabilities of the company's exposure is done through the following:

- i. Document assessments and findings;
- ii. Considering all relevant risk factors before determining what level of overall risk and appropriate level and type of mitigation to be applied;
- iii. Keeping the assessment up-to-date through periodic review; and
- iv. Submission of the risk assessment information as may be required by the Insurance Commission.

- c. What identified risks and vulnerabilities is the entity exposed into and how are these risks and vulnerabilities measured, monitored and controlled by the BOD and/or SM?

These risks and vulnerabilities are measured, monitored and controlled by the BOD and/or SM either by adopting an AML and terrorist financing monitoring system that is appropriate for their risk-profile and business complexity and in accordance with

existing rules and regulations of AMLA under AMLC, SEC and the IC, and/or by manual monitoring, where an electronic system is not needed but ensures that it has the means of complying with the AML regulations, its internal policies.

3. Self-Assessment Systems that are either Pro-Active, through Compliance-Testing, or Reactive, through Internal Audit

- a. Have you conducted an over-all assessment of the entity's level of compliance with the Anti-Money Laundering Act of 2001 (AMLA), under Republic Act (R.A.) No. 9160, as amended by R.A. Nos. 9194, 10167, 10365 and 10927, the Terrorism Financing Prevention and Suppression Act (TFPSA), under R.A. No. 10168, their respective Implementing Rules and Regulations (IRR), Circular Letter (CL) No. 2018-48, as amended and other relevant laws, IC and AMLC issuances? Please describe how this was done and state the frequency of the assessment

Yes, the entity conducted an over-all assessment of its compliance through periodic review. The periodic updating, review of customer's KYC information, annual reports and trends of AML/TF facilitates ongoing monitoring of the company.

- b. Based on the assessment, please state in percentage the level of compliance of the entity.

Ninety (90%) percent, more or less.

- c. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

Guidelines are set to ensure quality assurance specifically the policies and procedures associated with assessing and verifying the reported data. Guidelines through Compliance-Testing examine the underlying self-assessment systems. Corrective measures on assessment of the company's current performance and ability to reliably meet quality or criteria to help the company manage risk, control quality and limit legal liability, as well as avoidance of any indications of fraud to the company management's attention.

- d. Has your entity recently undergone an internal audit on AML and CTF Compliance? If yes, please summarize the key findings and/or

recommendations that were noted in the most recent internal audit report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

Yes. No findings as the company adheres to the guidelines set by the BOD.

- e. Has your entity recently undertaken compliance testing of other departments, units, offices and branches that is independent of the internal audit? If yes, please describe the process (whether on-site inspections were conducted) and summarize the key findings and/or recommendations that were noted in the most recent compliance testing report and set out the measures that the BOD has undertaken to address these findings and to monitor the same.

Not applicable

4. Management Information System

- a. Has the entity carried out an assessment of the effectiveness of the management information system as well as the AML and CTF electronic or manual, as applicable, monitoring system? Please specify how this is done.

Yes. Management Information System as well as the AML and CTF electronic or manual monitoring system is done by monitoring the list of Customer Due Diligence that provides risk scoring for all clients, and Suspicious Activity Monitoring that provides red flag/alerts for dubious transactions, particularly, cash or electronic transactions.

- b. What reports are being submitted to the BOD or Board level/approved Committee to assist them in their decision making processes relative to ML and TF prevention, who signs them and how frequent are they being required?

Reports of anomalous, suspicious and doubtful transactions of customers that may put the company at risk and may be used as an intermediary for ML and TF transactions. Such reports are made after thorough continuous monitoring conducted by the designated officers/staff in which thereafter submitted and reported to the Compliance Officer for verification and approval of the results.

- c. Does the entity keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? If

so, which Office requires and maintains the same? Please provide copies of the statistics.

Yes, the office of the Compliance Officer and its designated custodian, keeps and maintains the company records of annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports and other documents related to AML.

- d. Does the entity keep track dispositions of red flag systems alerts? If so, which Office requires and maintains the same? Please provide copies of the tracking report.

Yes, the office of the Compliance Officer and its designated custodian, keeps and maintains the company records on track dispositions of red flag systems alerts.

5. Capability of Compliance Office in Managing the Entity's MTPP

- a. Provide the names and contacts details of AML and CTF Compliance and Alternate Compliance officers. Also, provide the name of another officer designated by the company who is responsible and accountable for all record keeping requirements under the AMLA, as amended, TFPISA, their respective IRR, CL No. 2018-48, as amended and other relevant laws, IC and AMLC issuances

Names and contact details are as follows:

Chona M. Jacinto
Compliance Officer
88163163

Jesus D. Gomez
Assistant Compliance Officer
88163271

- b. Describe the structure of the Compliance Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualifications and experience as well as standards in hiring new employees, and control mechanisms (such as the power to monitor and ensure compliance including the authority to impose sanctions or give incentives or rewards when necessary) of the Office in ensuring that the pre-set objectives are adhered by responsible officers and employees in the different Departments, Groups, Units and/or Branches?

The company formulates an in-house training program aimed to provide efficient, adequate and continuous education program for all its personnel, including officers and

directors, to ensure that they fully comply and are fully aware of their obligations and responsibilities in counter terrorism financing/money laundering and terrorism financing prevention program (CTF/MTPP) particularly in relation to insured identification process, record keeping requirements and CT/ST reporting and ample understanding of the internal reporting processes including the chain of command for the reporting and investigation of suspicious insurance and money laundering activities.

- c. How are newly adopted policies and procedures as well as subsequent changes thereto assessed (as adequate or inadequate) and how are the results of the assessment communicated to the BOD, to Senior Management, to different Departments, Units, Groups, Sub-groups and to the Branches up to the frontliners and/or agents?

Through a comprehensive company's framework and aligned with the guidance from AML provisions which enables the authorities to monitor and combat all transactions linked with AML and TF risks.

- d. How is the adequacy of AML and CTF training assessed? Please specify in detail.

The adequacy of AML and CTF training are assessed through comprehensive inspection, mainly oriented to verify the compliance with the requirements following the procedures contained in the questionnaires. Such questionnaires are standardized from AML/CFT procedures and use as guidance sufficient and risk-based.

- e. Have you taken the necessary measures to prevent criminals or their associates from holding or being the beneficial owners of a significant or controlling interest or holding a management function, including membership in the Board or any Committee within your entity? If yes, please describe the measures taken.

Yes. In line with the objective of ensuring that the ICREs maintain high anti-money laundering standards in order to protect its safety and soundness, violation of Guidelines of IC or AMLA shall constitute a grave violation subject to the following enforcement actions against the board of directors, senior management and officers:

1. Written reprimand;
2. Suspension or removal from the office they are currently holding; or
3. Disqualification from holding any position in any covered institutions.

- f. Do you have a screening process that ensures high standards when hiring employees? If yes, please indicate the specific policy provisions applicable.

Yes. The entity implements strict vetting of employees including checking of criminal records provided by the NBI. The duties and responsibilities of each employee is stated in the employment contract and violations of company policies is clearly stipulated prior to hiring of the employee.

- g. Are the directors and senior management subject to internal "fit and proper" requirements including a check on their expertise and integrity? If yes, please provide the relevant policy provisions. If election, selection or appointment is based on family ties, please indicate.

Yes. The Board of Directors shall have a high standard of best practices for the corporation, its stockholders and other stakeholders, the Board shall also conduct themselves with utmost honesty and integrity in the discharge of its duties, responsibilities and functions.

He must possess the necessary expertise, experience and skills in his conduct as a professional in the insurance industry.

- h. Do you ensure that your foreign branches and subsidiaries observe AML and CTF measures consistent with the Philippine's legal requirements? If yes, please indicate the specific policy provisions.

No. The company has no foreign branch and subsidiaries

- i. In connection with the last question, was there an instance when the home country supervisor where a foreign branch or subsidiary is located has prohibited the branch or subsidiary from observing the Philippine laws, rules and regulations because it is prohibited by local (i.e. host country) laws, regulations or other measures? If yes, have you notified the Insurance Commission (IC) of this directive? Please indicate the specific legal provision(s) that provide(s) the legal basis for this requirement.

Not applicable

- j. How are the provisions of the Money Laundering And Terrorist Financing Prevention Program (MTPP) disseminated to responsible officers, employees and agents and how are their compliance assessed and monitored?

Anti-Money Laundering and Terrorist Financing Prevention Program (MTPP) provisions are disseminated through internal communications and training programs (when available). Further, these are also disseminated to directors and staffs for their awareness of such policies, rules and procedures to prevent ML and TF.

- k. What other relevant management practices does the Compliance Office exercise to manage its MTPP and ensure attainment of the entity's plans and objectives relative to ML and TF prevention?

The Compliance Officer shall regularly circulate compliance bulletins covering amendments in the anti-money laundering law and changes in the pertinent rules and regulations as well as the Insurance Commissions Circulars. Developments in the Anti-Money Laundering campaign of the government shall also be advised to all concerned.

6. Nature of Weaknesses Noted and Ability to Address Existing and Potential Risks and Problems

- a. Has your entity undergone a previous AML and CTF Compliance Checking by the IC? If yes, please summarize the key findings and/or recommendations that were noted in the most recent AML and CTF report and set out the measures that the BOD has undertaken to address the findings and to monitor the same.

Since 2017, the entity has not undergone any issues nor incurred any findings related to AML and TF after its regular submission of pertinent documents to the Insurance Commission and SEC.

- b. How are deviation from pre-set guidelines as well as deficiencies and weaknesses noted during internal and external audits corrected and what are the mechanisms undertaken to monitor implementation of corrective measures?

The pre-set guidelines as well as deficiencies and weaknesses during internal and external audits are noted and corrected by:

1. When there is an unusual or suspicious transaction, investigation shall follow in relation to which report was made;
2. Special attention shall be focused on complex, unusual large transactions, or unusual patters of transactions and if there is no apparent or visible economic or lawful purpose, there are no specific requirements to make available to the competent authorities and auditors such findings.

7. Institutional Risk Assessment

- a. Has your entity undergone an Institutional Risk Assessment? If yes, when was this conducted?

None.

- b. Has your entity documented the risk assessment and findings? If yes, please summarize the key findings and/or recommendations that were noted in the most recent Institutional Risk Assessment and set out the measures undertaken to address the findings and to monitor the same.

No.

- c. Has your entity considered all the relevant risk factors, including the results of national and sectoral risk assessment, before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied? If yes, please provide a summary

The company will take appropriate preventive measures to be conducted, assess and determine in sectoral and national risk assessment before determining what is its level of overall risk and appropriate level and type of mitigation to be applied. Formal risk assessment is a better way to determine the overall risks and what initiative may be conducted. Local authorities' intervention may also be considered when greater weight and exposure to AML and TF risks on proper identification and assessment of sectoral and institutional risks.

B. MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM (MTPP)

1. Customer Identification, Verification and Ongoing Monitoring Process

- a. Does the entity apply a risk-based approach to combating money laundering and terrorist financing? If so, please provide an overview of these policies and procedures. The overview should (1) portray the entity's philosophy towards risk-based (does it form an integral part of the entity's business framework?), (2) indicate how the relevant risk assessments are undertaken and their bases to help determine the policy and its practical application, and (3) describe the mechanism by which permitted variations from the generally applicable standards are promulgated, and what arrangements, if any, are in

place to monitor the continuing suitability of the exceptions. Please provide the basis in the entity's MTPP.

1.) In accordance with the entity's nature of business by providing insurance services to its clients, The company does a risk-based approach for the customer identification and verification process. Policies and procedures are assessed through a comprehensive company's framework conformably with the provisions of AML which enables them not to be used as a median or business conduit to unlawful transactions linked with money laundering and terrorist financing activities;

2.) Risk assessments are undertaken, determine and applied by the company in the following manner:

- i. Prepare and record a risk assessment with respect to the customer;
- ii. Determine and assess the risk that any Business Relationship or Occasional Transaction involves, or will involve, money laundering or terrorist financing, depending upon the type of customer, Business Relationship, product or transaction and consider on a risk-sensitive basis, whether further identification or Relationship Information; and

3.) The company's MTPP is designed based on the standards and procedures required by the AMLC. The company is compliant and fully supports the program in countering money laundering and terrorist financing in business sectors particularly, insurance industry. In general, there is no exceptions whether the company has documented and verified the decision to perform simplified due diligence. Thus, all transactions shall be clearly documented in client files. When an exception has been given by adequate authority and the fact that inspections were not risk-based, assurance of compliance therewith with existing AML/CFT laws and regulations is a must.

b. Does your entity permit the opening of anonymous accounts, accounts in fictitious names and other accounts not otherwise under the true and full name of the customer/client? If yes, please indicate the approximate number of accounts, pertinent policies and procedures for opening and the level of approving authority.

The company does not permit the opening of anonymous accounts, fictitious accounts, incorrect name accounts, or customers who fail to provide the required evidence of identity. The company/ICRE maintains customer's account only in its true and full name of the account owner or holder. Customer identification requirements that could entail anonymous or fictitious accounts are effectively

prohibited. The same with anonymous accounts, accounts under fictitious names, numbered accounts and all other similar accounts shall be absolutely prohibited.

c. Does your entity undertake customer due diligence (CDD) measures when:

i. Establishing business relations?

For new customer/client. The company, shall develop a procedure for establishing the true and full identity of the new individual customer/client. Unless otherwise stated in this Guidelines, average customer due diligence (CDD) requires that company shall gather from individual customer/client before or during the course of establishment business relationship.

ii. Carrying out transactions with non-clients?

Yes. non-client's identity shall be obtained. It is the policy of the entity to direct all employees to exercise utmost diligence to ensure that adequate measures are implemented to prevent the Company from being unwittingly involved in such a criminal activity particularly when customer has not been physically presented for identification purposes.

iii. Carrying out occasional transactions?

Yes. When an account is an one-off or occasional transaction, the company shall also establish and record the true and full identity and existence of both account holder and person purporting to act on behalf of the customer, and the beneficial owner or the principal on whose behalf the transaction is being conducted.

iv. Dealing with trustee, nominee, agent, or intermediary, applying CDD not only on the latter but also on the trustors or principals?

Yes. The company shall verify the validity of the sub-agent or intermediary. It shall determine the true nature of the parties' capacities. A certified document is required from the sub-agent or intermediary stipulating his/her role in the conduct of his business with the Insured. The same standards for assessing the risk profile and determining the standard of CDD is to be applied.

v. The entity has doubts about the veracity of previously obtained customer identification document or data?

The company shall apply enhanced due diligence on the customer/client if in doubt about the veracity of customers/clients.

- d. Does your entity undertake customer due diligence (CDD) measures on the beneficiary(ies) of life insurance and other investment related insurance policies? Please describe in detail the COD process and the specific provision in the MTPP that apply.

Non applicable.

- e. Explain the COD requirements applicable to potential individual customers stating the minimum information to be obtained, IDs acceptable and its classification based on reliability, if any, and policy in updating identification information citing the specific internal policy provisions.

The company requires customers/individual the true and full identity.

1.) Identification Information:

- Full name;
- Date & place of birth;
- Sex;
- Citizenship or nationality;
- Address;
- Contact number or information;
- Source of fund;
- Specimen signature and,
-Name, address, date and place of birth, contact number or information, sex and citizenship or nationality of beneficiary and/or beneficial owner, whenever applicable.

2.) Identification Document:

- Phil. ID; or
- Other identification documents as herein defined.

- f. Explain the CDD requirements applicable to potential customers that are juridical entities and the persons acting on their behalf such as but not limited to the President and the authorized signatory/ies stating the minimum information to be obtained, IDs acceptable and its classification based on reliability, if any, measures to prevent the unlawful use of legal persons in relation

to money laundering and terrorist financing and policy in updating identification information citing the specific internal policy provisions.

The company shall obtain from their customer that are juridical person the following minimum identification information and documents before or during the course of establishing business relationships:

1.) Identification Information:

- Full name;
- Name of authorized representative, transactor, signer;
- Current office address;
- Contact number or information;
- Nature of business;
- Company website
- Source of fund;
- Specimen signature or biometrics of the authorized representative, transactor, signer; and,
- Name, address, date and place of birth, contact number or information, sex and citizenship or nationality of beneficiary and/or beneficial owner, if applicable.

2.) Identification Documents:

- Certificates of Registration issued by the BIR, DTI, SEC, BSP, and by AMLC for covered person;
- Articles of Incorporation/Partnership;
- Registration Data Sheet/Latest GIS;
- Sec. Cert. citing pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity; and,
- For entities registered outside of the Philippines, similar documents and/or information duly authenticated by a senior officer of the covered person assigned in the country of registration; in the absence of the said officer, the documents shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

- g. Does your entity identify the beneficial owner of juridical entities dealing with your entity and verify the information acquired? If yes, please describe in detail including the specific internal policy provisions.

Yes. The company shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner through the information:

- a. The identity of natural persons, if any, who ultimately have controlling ownership interest in a juridical person;

- b. To the extent that there is doubt as to whether the persons with controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural persons, if any, exercising control over the juridical person through other means; and,
 - c. Where no natural is identified under item (a) & (b) above, the identity of the relevant natural person who hold senior management positions.
Any information gathered shall be verified from trustworthy parties such as banks, reputable law firms'/accounting firms or accessing public or private databases or official sources. Verification of information
- h. Does your entity verify the true identity of customers, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data, or information? If yes, please describe in detail including the specific internal policy provisions.

One of the CDD Standards of the company is to identify and verify the true identity of a customer using reliable independent source documents and data information. CDD Minimum Requirements/Internal Policy Procedures includes but are not limited to the following:

- a) Confirming the place and date of birth from a duly authenticated official document;
- b) Verifying the address through utility bills, bank or credit card statement, or other documents showing address or through on-site visitation;
- c) Contacting the customer by phone or email;
- d) Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means; and
- e) Determining the veracity of the declared source of funds.

Satisfactory evidence of the true and full identity, legal capacity, occupation or business purposes and other reliable data or sources of information shall be strictly obtained.

- i. Does your entity verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person? If yes, please describe in detail including the specific internal policy provisions

The company shall verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person. It is the policy of the entity where transactions are undertaken on behalf of account holders, particular care shall be taken to ensure that the person giving such instruction is authorized to do so by the account holder.

The company shall establish and record the true and full identity and existence of both the customer and the authorized person.

- j. Does your entity 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 entity is satisfied that it knows who the beneficial owner is? If yes, please describe in detail including the specific internal policy provisions.

Yes. The company, to the best of its ability should have a system to identify the beneficial owner and take reasonable measure to verify the identity of its ownership and control structure. In case of beneficial owners, or persons on whose behalf the account are being opened where the account may be attributable to beneficial owner,. The company at the minimum, needs to 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.

The company shall keep records of the action taken in order to identify the beneficial owner.

Customer shall be made aware of the company's explicit policy that transactions will not be conducted in the event of failure to complete verification of any relevant information or to obtain information/data from reliable sources.

- k. Does your entity understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business relationship with its customers? If yes, please describe in detail including the specific internal policy provisions.

Yes. The company shall determine and understands as appropriate, obtain information, the purpose, and intended nature of the account, transaction, or business relationship with its' customers.

- l. Does your entity, on the basis of materiality and risk, conduct ongoing

due diligence on the business relationship of existing customers? If yes, please describe the extent/scope of this obligation and indicate the specific internal policy provisions.

The entity conducts ongoing monitoring by establishing a system that will enable them to understand the normal and reasonable account or business activity of customers, and scrutinize transactions undertaken through the course of business relationship to ensure that customer's accounts, including transactions being conducted are consistent with ICRE's knowledge of its customer, their business and risk profile, including, where necessary, the source of funds. Further, by undertaking reviews and updating of existing records, document the action taken, and accordingly update customer's risk profile.

- m. Does your entity perform enhanced due diligence for higher risk categories of customer, business relationship or transaction and does it apply to existing customers? If yes, please explain Including reference to the list of customers considered as high-risk, criteria and factors considered in applying EDD, types of measures required, control mechanisms for managing the risks associated with dealing with these customers, validation procedures and the specific internal policy provisions. Also, provide number of high-risk customers per category.

Yes. Whenever enhance due diligence is required or where the risk are higher, the company shall perform the following:

- A.) Gather documents to support the: (i) Source of wealth and fund; (ii) Nature of occupation and/or business; (iii) Reason for intended/[performed transaction; and, (iv) other identification information which the company/ICRE deems it necessary.
- B.) Conduct additional validation procedure, such as: (i) Verifying volume of assets; (ii) Verifying declared residence and conducting face-to-face contact with customer, their agents and beneficial owners; and, other modes of validation which the company deems it necessary.
- C.) Secure approval of senior management to commence or continue transacting with the customer;
- D.) Conduct enhance ongoing monitoring, frequent or regular updating of identification and information documents;
- E.) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standard; and,
- F.) Such other measure as the company deems reasonable or necessary

- n. Does your entity apply reduced due diligence where there is low risk of ML or TF? If yes, please explain providing details of any applicable conditions/standards and specific internal policy provisions. Is this permitted with regard to customers that are resident in another country? If yes, please explain further.

Simplified or Reduced Due Diligence (RDD). Where lower risks of ML/TF have been identified through adequate analysis by the company/ICRE and based on the result of the institutional risks assessment, simplified or reduced customer due diligence measure may be applied. However, simplified or reduced customer due diligence measures are not acceptable whenever there is suspicion of ML/TF, or where specific higher risk scenarios apply.

Reduced Due Diligence for Low Risk Customer

- I. For individual customers, the company may allow an account under the true and full name of the account owner/s upon presentation of acceptable identification card or official document.
- II. For corporate, partnership, and sole proprietorship entities, and other entities such as banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such, publicly listed companies subject to regulatory disclosure requirements, government agencies, The company may open an account under the official name of these entities with the minimum information/documents and Board Resolution duly certified by the Corporate Secretary authorizing the signatory to sign on behalf on the entity, obtained at the time of account opening.

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

- o. What does your entity do in cases where it is unable to satisfactorily complete the COD measures required by existing internal rules or under CL 2018-48, as amended, the AMLA, as amended, and its IRR? Please indicate the specific internal policy provisions that apply.

When the company is unable to satisfactorily complete the CDD measures, it shall consider making a suspicious transaction report (STR) and shall terminate the business relationship with the customer.

The company shall also: a.) refuse to open an account, commence business relationships, or perform the transaction; or, terminate business relationships; and, b.) file an STR in relation to the customer, if circumstances warrants.

It is the policy of the company/ICRE that, where information gathered like reports on critical customer data in line with the CDD measures not obtained/disclosed despite diligent effort and follow up, or such reports on customers with unusual activities that may lead to suspicious transactions, shall be provided to the Compliance Officer will analyze and effectively monitor high risk customer accounts. Any adverse findings hereof shall be advised to the Senior Management and immediately report to the AMLC for appropriate action.

- p. What are your obligations with regard to establishing business relationships with a politically exposed person, his/her immediate family relative, his/her close relationship/associates, entities related to them? Please describe the existing policies governing these arrangements, including the standard of due diligence that apply to them on account opening, control mechanisms to address the risks associated with dealing with them, and updating of identification information with references to specific internal policy provisions.

The company/ICRE shall establish and record the true and full identities of Politically Exposed Persons (PEP), their family members, close relationships/associates and entities related to them. Carefully consider a PEP position and the position's attendant risks with respect to the money laundering and terrorist financing in determining what standard of due diligence shall apply to them.

- A. Domestic and International Organization PEP. In addition to performing the applicable CDD measures, the entity shall:
1. Take reasonable measure to determine whether a customer, and his agent, and beneficial owner are PEPs; and,
 2. In cases where there is a higher risk business relationship, adopt the following measures:
 - a.) Obtain senior management approval before establishing or, for existing customers, continuing, such business relationships;
 - b.) Take reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as PEPs; and,
 - c.) Conduct enhanced ongoing monitoring on that relationship.

- B. Foreign PEP. In addition to performing the applicable CDD measures, the entity shall:
1. Put in place risk management system to determine whether a customer or beneficial owner is a PEP;
 2. Obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;
 3. Take a reasonable measures to establish the source of wealth and source of funds; and,
 4. Conduct enhanced ongoing monitoring on that relationship.

The Company, in addition to performing applicable CDD measures, adheres the same with the provision of the AMLA which shall not be construed or implemented in a manner that will discriminate against certain customer types, such as politically-exposed persons, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny these persons' access to the services provided by the covered persons.

- q. Does your entity allow non-face-to-face transactions (transactions with trustee, nominee, agent or intermediary accounts including account opening)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

As a general rule, no transactions or new accounts shall be opened and created without face-to-face contact and personal interview between the company/ICRE duly authorized personnel and the potential customer. However, the use of Information and Communication Technology (ICT) in the conduct of personal face-to-face contact and interview is allowed, provided, that the designated company/ICRE personnel is in possession of and has verified the identification documents submitted by the prospective client *prior* to the interview and the *entire procedure is documented*.

- r. Do any of your businesses make use of third parties, referral by brokers, intermediaries, fiduciaries, affiliates, subsidiaries and the like (Collectively called as third parties)? If Yes, please identify the third-parties and the due diligence undertaken on the third parties. Please also identify the business areas which make use of third parties, the approval process for introducing customers/clients, the type of relationship, and whether or not such third parties perform the COO

process that would usually be undertaken by the entity;

In some business instances, the company/ICRE may resort to third parties referred by agents but it must ensure that the latter is a covered person defined under Sec. 3 (a) of the AMLA as amended and is covered by customer identification face-to-face requirements.

The company/ICRE using third parties shall also conduct its own EDD procedures under the following circumstances:

- 1.) Where the business relationships and transactions with persons including companies and financial institutions from other countries do not insufficiently apply FATF Recommendations; or,
- 2.) When establishing source of wealth of high risk customers.

The senior management shall undertake decisions on business relations with high risk customers.

- s. Do you rely on third parties to perform some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

The company/ICRE may rely on a third party provided the same must be a covered person defined under the AMLA and the ICRE shall obtain from the third party a written sworn certification containing the following:

- 1.) The third party conducted the prescribed customer identification procedures including the face-to-face contact requirement to establish the existence of the customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and,
- 2.) Reliance by the company/ICRE shall have the ability to obtain identification documents from the third party upon request without delay.

The company/ICRE may also rely on a third party that is part of the same financial, business, or professional group under the following circumstances:

- 1.) The group applies CDD and record-keeping requirements, in line with the AMLA and TF, their respective IRR, and other AMLC issuances; and the MTPP in accordance with the rules hereof;
- 2.) The implementation of CDD and record-keeping requirements, and the MTPP is supervised at a group level by SA; and,
- 3.) Any higher country risk is adequately mitigated by the group's AML/CTF policies.

Notwithstanding the foregoing, the ultimate responsibility and accountability for identifying the customer and conducting CDD remains with the company/ICRE relying on the third party. Provided that, in cases of high-risk customers, the ICRE shall also conduct enhance due diligence procedure.

- t. Are there instances where you outsource some of the elements of the CDD process (face-to-face or gathering of the minimum information)? If yes, please explain the existing policies governing these arrangements as well as the control mechanisms to address the risks associated with this type of business relationships or transactions with references to specific internal policy provisions.

No.

- u. What are your obligations with regard to business relationships and transactions with persons (including legal persons and other financial institutions) who are nationals or citizens of foreign jurisdiction or geographical location which do not or insufficiently apply internationally accepted AML and CTF standards, as determined by relevant domestic or international bodies? Please provide the internal policy provisions, which serve as basis for these obligations.

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

It is the internal policy of the company/ICRE not to enter into business relationship with customers including persons (including legal persons and other financial institutions) who are nationals or citizens of foreign jurisdiction who refuse to produce the required identification papers and failed to submit customer identification documents.

- v. Are there measures in place to ensure that your entity is advised of concerns about weaknesses in the AML/CTF systems of other countries? If yes, please describe these measures and how these concerns are incorporated into the entity's Program.

The company/ICRE shall apply enhance due diligence, limit businesses relationships or financial transactions with the identified country or persons in that country,

proportionate to the risk when called upon to do so by the FATF, or independently of any call by the FATF to do so, when warranted.

- w. Are there measures in place to ensure that funds collected by or transferred through non-profit organizations are not diverted to support the activities of terrorists or terrorist organizations? If so, please specify what these measures are and indicate the specific policy provisions.

Yes. There are measures in ensuring that funds collected by or transferred through non-profit organizations are not diverted to support unlawful activities. The company shall determine the veracity of the declared source of funds. Validate the source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc. The Company may require additional identification documents to further vouch the identity of the clients.

- x. What are your obligations with regard to relevant United Nations Security Council Resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing? Please provide the internal policy provisions, which serve as basis for these obligations.

The company/ICRE shall secure the consent of all their customers to be bound by obligations set out in the relevant United Nations Security Council Resolutions (UNSECR's) relating to the prevention and suppression of proliferation financing weapons of mass destruction, including the freezing and unfreezing action as well as mechanism to comply prohibitions from conducting transactions with designated persons and entities.

2. Record Keeping and Retention Process

- a. Please describe the record-keeping obligation including the type of records and information that should be maintained. Please indicate the specific internal policy provisions.

Under the guidelines on digitization of customer records, the company/ICRE shall retain all transaction records in original forms and filed in the filing cabinet.

- b. Do you maintain all necessary records on transactions, both domestic and international and, if so, for how long following completion of the transaction? Who are the designated custodians that shall be accountable and responsible for

safekeeping these documents?

Yes, the company maintain, preserve, and safely store for at least five (2) years following the completion of transactions, all records of customer identification and transaction documents, or as long as the business relationship exists.

- c. Do you maintain records of the identification information and documents and data, account files and business correspondence and, if so, for how long following the termination of an account or business relationship

Yes, the company also maintain, preserve, and safely store for at least five (2) years following the termination of account or transaction, all records of customer identification and transaction documents both domestic and international, account files and business correspondence

- d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the designated custodian that shall be accountable and responsible for safekeeping and making these records available with references to specific internal policy provisions

Yes. The company/ICRE ensures that all CDD information and transaction records are available swiftly to the IC, AMLC and other domestic competent authorities in the exercise in their official functions or upon order by a competent authority.

3. Covered and Suspicious Transactions Reporting

- a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

None yet. The company is using manual procedure.

- b. If no, please describe how you manually perform the functionalities mentioned above.

The company/ICRE manually perform the functionalities of covered and suspicious transactions by implementing procedures classifying them into suspicious and non-suspicious ones. Gathering of information, documents and making preliminary analysis from the compliance officer in case suspicious transactions arises. A Manual Procedure that requires the management and its employees to be compliant

therewith. Keeping a database of customer accounts and their transactions with the use of computer and or through the original documents and papers submitted. Maintain a register of all ST's that have been brought to the attention to the Compliance Officer whether or not the same was reported to the AMLC.

- c. Do you pay special attention to unusual transactions? If yes, how do you define unusual transactions? And what type of special measures do you implement in managing them? Please indicate the specific internal policy provisions for this requirement.

Yes. Unusual transactions of customers that may put the Company at risk shall be reported to the Compliance Officer. The Company shall apply enhanced due diligence on its customer with unusual transaction.

- d. Are you required to report to the AMLC a suspicious transaction report (STR), when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the entity (whether or not to file an STR) with references to the specific internal policy provisions that mandate reporting.

Yes. The company is required to report any suspicious transaction report (STR) to AMLC which is related to funds that are proceeds of criminal activity, shall ensure the accuracy and completeness of covered and suspicious transaction report. If there is reasonable ground to that the client/customer has engaged in an unlawful activity, the compliance officer, upon receiving such report shall promptly evaluate whether the suspicion is valid. If valid, The case shall be immediately reported to the AMLC.

- e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the entity (whether or not to file an STR) with reference to the specific internal policy provisions that mandate reporting.

Yes. Should a transaction be determined to be a covered and a suspicious transaction of terrorism, it shall be reported for the proper filing and or reporting of STR in accordance with the AMLC Registration and Reporting Guidelines and any amendments thereto.

- f. Other than the 6 specified circumstances for filing an STR, what other

instances do you report an STR or an alert has been tagged using the last item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

The company/ICRE has its own procedures in combatting money laundering and terrorist financing. Hereunder are the instances where the company/ICRE considered when reporting STR or when alert has been tagged:

- 1.) Client is not properly identified
- 2.) Request to keep client details unknown
- 3.) Large and unusual premium payment in cash received.
- 4.) Excessive overpayment of premium with request for refund
- 5.) Unnecessary routing of funds through third party accounts;
- 6.) Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;
- 7.) Substitution, during the life of an insurance contract of the ultimate beneficiary with a person without any apparent connection with the policy holder;
- 8.) Unusual transactions without an apparently profitable motive; and,
- 9.) Any other or similar indicators as may be detected by the ICRE from time to time.

- g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report? Please describe, by reference to the specific internal policy provisions, the scope of the protection in terms of who would benefit from it and the types of liability against which it is available.

The entity/ICRE has legal protection with its officers and staff who report their suspicion in accordance with obligation to report and are only effectively discharging their obligations to prevent money laundering and terrorist financing in the company.

- h. Do you prohibit your officers and staff from disclosing ("tipping off") to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC? If they are, please describe the scope of this prohibition by reference to the specific internal policy provisions.

When reporting covered (CTR) or suspicious transactions (STR), The company and its 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 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 any other similar devices. In case of violation thereof, the concerned director, officer and employee of the ICRE and media shall be held criminally liable.

In the event that urgent disclosure is required, particularly when the account concerned is part of an ongoing investigation, the Compliance Officer shall notify in writing the BOD.

4. Employment and Training Program

a. Please indicate the standards that apply when hiring new staff to the Compliance Office, the Internal Audit and the entity as a whole?

i. The company/ICRE shall apply the following standards when hiring new staff to the Compliance Office:

- i- The applicant for compliance office must have clear and demonstrable good corporate skills and knowledge in combating money laundering and financing terrorism together with assigning a specialized team to help the officer in this task;
- ii- Has strong determination and compliance as a center of best practice in insurance industry in areas of combating money laundering and terrorism financing;
- iii- Has adequate knowledge in procedures in addressing obligations of independent audit function to test compliance with the procedures, policies and controls;
- iv- Shall perform a periodic review of the implementation of the policies and procedures indicated on the Anti-Money Laundering Manual to determine compliance with existing laws and regulations, evaluate adequacy and measure effectiveness.
- v- Has independent will to report and advised the company through the company's officers or Compliance Coordinator, when suspects any suspicious, and unusual findings so that it shall be forwarded to the AMLCC for appropriate action.

b. Please describe the entity's AML training and refresher program with specific references to the level of training and focus on the

participant, the Office tasked to implement the program, the financial, human and technical support that that Office has been given and frequency of offering.

The company provides for refresher trainings to review updates to compliance measures as they arise from new legislation, IC or AMLC issuances and discoveries in ML/TF trends and detection techniques. The employees training are conducted annually.

The scope of training includes but not limited to the following:

1. Provision of AMLA and its IRR;
2. The company's Corp. Governance Manual, and ML/TFPP Program;
3. Participation of Directors, Officers, and Staffs in ML prevention;
4. Risk Management (Customer Identification Process; Record Keeping; Covered & Suspicious Transactions Reporting);
5. Preventive Measures;
6. Cooperation and Reporting to I.C. and AMLC.

- c. Are the staffs of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices? Please give details.

Yes. Generally, all employees shall be provided with adequate training on anti-money laundering law, rules and regulations as well as the policies and procedures established by the Company to ensure awareness and compliance. Whereas, training with staffs of Compliance Office specifically includes the application of CDD and EDD, determination of CTR and STR, monitoring of ML/TF, and the process and reporting procedure to the Compliance Office.

Training on anti-money-laundering shall be on a regular basis to create awareness in new rules and regulations and to update on the latest trends and techniques applied by money launderers to make them more effective in preventing money laundering activities.

- d. Do you have an on-going employee training on AML and CTF? if yes, please indicate the last employee training on AML and CTF and the schedule for the year as well as the specific policy provisions for this requirement.

Yes. The company policy is to provide the employees training/seminar about Anti-Money Laundering (AML) once hired to be aware of their obligation as an employee of the company.

C. INTERNAL CONTROLS AND AUDIT

1. What is the structure of the Internal Audit Office including the financial, human and technical resources, delegated authorities, reporting and communication line, duties and responsibilities of the Office as a whole and of individual officers and staff together with their qualification and experiences as well as standards in hiring new staff, and control mechanisms of the Office in ensuring that the pre-set objectives are adhered by responsible officers and staff in the different Department, Groups, Units and/or Branches?

The company has no internal audit office yet but has internal control to prevent the ML/TF.

2. Do you establish and maintain internal procedures, policies and controls to prevent ML and TF? How do you communicate these to the officer, staff and employees? Please provide details with reference to the applicable policy provisions

The company maintains internal procedures, policies and controls to prevent ML and TF. These measures are enforceable to keep abreast of AML laws and also for the purposes of company assessment in setting internal policies. The company requires appropriate compliance management arrangements, such as compliance of officers at the management level in reporting STR transactions to senior management and to the board.

The internal procedures, policies, and controls to prevent ML/TF are disseminated to the in the forms of email letters to the officers, staffs and/or employees. This compliance with the requirements of the AMLA, as amended, its IRRs and all Circulars issued by the Insurance Commission and the Anti-Money Laundering Council.

3. Do you maintain an adequately resourced and independent audit function that tests compliance with these procedures, policies and controls? If yes, please indicate the available resources, financial, human, and technical and the specific policy

provisions for this requirement.

The Company/ICRE maintain an adequately resourced and independent audit function to test compliance with the law, decisions, and other enforcement measures to prevent ML and TF.

The external audit department has the responsibility in monitoring compliance with the procedures, policies and controls. Financial transactions are regularly examined. Documents related to acceptance of business are check if the required information are submitted and complied with. Any observations are relayed immediately to the management in order that necessary requirements are complied.

D. IMPLEMENTATION

1. Covered and Suspicious Transaction Reporting Policies and Procedures

- a. Do you have an electronic money laundering transaction monitoring system in place? If yes, is it internally developed or purchased from a vendor, and does it have the following automated functionalities?

None yet. The company is presently using manual procedure.

- b. If no, please describe how you manually perform the functionalities mentioned above

The company has the means of complying manually with the AML regulations, its internal policies and manual compliance system (Monitoring and Reporting Tools). Manual functionalities are performed in the implementation of:

- i. Manual monitoring system by monitoring the list of Customer Due Diligence that provides risk scoring for all clients, and Suspicious Activity Monitoring that provides red flag/alerts for suspicious transactions, particularly, cash transactions;
- ii. Manual adaptation of risk-based approach for the customer identification and verification process in which such are assessed through a comprehensive company's framework with the guidance from AML provisions which enables them not to be used as a median to unlawful transactions linked with money laundering and terrorist financing;
- iii. Manually perform the functionalities of covered and suspicious transactions by implementing procedures, classifying them into suspicious and non-suspicious ones.

Gathering of information, documents and making preliminary analysis by the compliance officer in case suspicious transactions arises; and

iv Manual database is established which stores information from the date the company became operational are still monitored, classified and stored and such is maintained for combating money laundering and terrorism financing references.

- c. Do you pay special attention to unusual transactions? What type of special measures do you implement in managing them?

Yes. Unusual transaction of customers shall be reported to the AMLC Committee. The Company shall apply enhance due diligence on its customer if it acquires information in the course of its account transaction monitoring.

- d. Are you required to report to the AMLC a suspicious transaction report (STR) when you suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity? Please describe the scope of the obligation, the decision process and the decision maker within the entity (whether or not to file an STR).

Yes. The company is required to submit reports suspicious transaction report (STR) to AMLC. Shall ensure the accuracy and completeness of covered and suspicious transaction report. The source of wealth or income, including how the funds were acquired, to assess whether the actual transaction pattern is consistent with the expected transaction pattern and whether this constitutes any grounds for suspicion on money laundering.

- e. Does the obligation to make an STR also apply when you suspect or have reasonable grounds to suspect that funds are related to terrorism? If yes please describe the scope of this obligation, the decision process and the decision maker within the entity.

Yes. Should a transaction be determined to be a covered and a suspicious transaction of terrorism, it shall be reported for the proper filing and or reporting of STR in accordance with the AMLC Registration and Reporting Guidelines and any amendments thereto. The company's obligation therewith is to assure that the information acquired are based on its internal investigation and the requirements submitted by the suspect such as financial statement, including attempted transactions, when the company suspects or has reasonable grounds to suspect, or to believe, that the funds are proceeds from criminal activity, or are related or linked to terrorist financing, terrorist acts or terrorist organizations or those who finance terrorism.

- f. Other than the 6 specified circumstances for filing an STR, what other instances do you report an STR or an alert has been tagged using the last Item- any transaction that is similar or analogous to any of the foregoing, i.e. tax evasion, malversation of public funds, bribery, etc?

The company has implemented its procedures in combatting money laundering and terrorist financing. Hereunder are the instances where the company/ICRE considered when reporting STR or when alert has been tagged:

1. Client is not properly identified
2. Request to keep client details unknown
3. Large and unusual premium payment in cash received.
4. Excessive overpayment of premium with request for refund
5. Unnecessary routing of funds through third party accounts;
6. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;
7. Substitution, during the life of an insurance contract of the ultimate beneficiary with a person without any apparent connection with the policy holder;
8. Unusual transactions without an apparently profitable motive; and,
9. Any other or similar indicators as may be detected by the ICRE from time to time.

- g. What is the legal protection against potential liability available to your officers and/or staff who report their suspicion in accordance with the legal obligation to report?

The entity/ICRE has legal protection with its officers and staff who report their suspicion in accordance with obligation to report and are only effectively discharging their obligations to prevent money laundering and terrorist financing in the company.

- h. Does the Compliance Office keep annual statistics on red flags systems alerts, ML investigations, CT reports, ST reports broken down as to the nature? Please provide copies of the statistics.

The entity/ICRE has no such red flag systems alert, ML investigations, CT reports and ST reports being recorded yet.

- i. Does the Compliance Office keep track dispositions of red flag systems alerts? Please provide copies of the tracking report.

There is no such red flag systems alert being recorded yet.

- j. Do you prohibit your officers and staff from disclosing ("tipping off") to any person the fact that an STR, CTR or related information is being reported or provided to the AMLC?

When reporting covered (CTR) or suspicious transactions (STR), The company and its 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 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 any other similar devices. In case of violation thereof, the concerned director, officer and employee of the ICRE and media shall be held criminally liable.

2. Risk Based and Tiered Customer Acceptance, Identification, Verification and Ongoing Monitoring Policies and Procedures

- a. Does your entity undertake customer due diligence (COD) measures when:

establishing business relations?

- i. Yes, The company shall obtain from the customers/clients the minimum identification, information and documents before or during the course of establishing a business relationship with corporate clients/investors, a company search and/or other commercial inquiries shall be made to ensure that the prospective client has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In case of doubt as to the identity of the company, its directors or the business in general, a search or inquiry with the Department of Trade and Industry (DTI), or Securities and Exchange Commission (SEC) and shall be made.

carrying out transactions with non-clients?

- ii. Satisfactory evidence of new customer's or non-client's identity shall be obtained. Moreover, effective procedures for verifying the bona fides of new customers shall be implemented. In this regard, the Board of Directors and Senior Management shall ensure that the Company is not used to facilitate in money laundering. The Company shall direct all employees to exercise utmost diligence to ensure that adequate measures are implemented to prevent the Company from being unwittingly involved in such a criminal activity.

carrying out occasional transactions?

- iii. Evidence of the true and full identity, representative capacity, domicile, legal capacity, occupation or business purpose/s of the clients, as well as other identifying information on those clients, whether they be occasional or usual, shall be strictly obtained.

dealing with trustee, nominee, agent, or intermediary, applying COD not only on the latter but also on the trustors or principals?

- iv. In case of doubt as to whether the trustee, nominee or agent is being used as dummy in circumvention of existing laws, further inquiries shall immediately be made to verify the status of the business relationship between the parties. When satisfactory evidence of the beneficial owners cannot be obtained, The Company shall apply the "Know Your Customer" principle in deciding whether or not to proceed with the business.

dealing with juridical entities that have no business substance in their own right but through which financial transactions may be conducted, applying COD on the entities' beneficial owner?

- v. The company develops a systematic procedure for identifying customer/clients that are corporate, partnership, and sole proprietorship entities as well their partners, stockholders, owners, directors, and authorized signatories.

the entity has doubts about the veracity of previously obtained customer identification document or data?

- vi. If during the business relationship, when there is a reason to doubt the accuracy of the information on the client's identity, the following measures shall be taken to verify the identity of the client or the beneficial owner, whichever is applicable: (a) it shall be classified as high risk account subject to continuous monitoring and (b) disciplinary history and disclosure of past relevant sanctions shall be reviewed.

- b. Does your entity undertake customer due diligence (COD) measures on the beneficiary(ies) of life insurance and other investment related insurance policies?

Non applicable

- c. Does your entity identify the beneficial owner of juridical entities dealing with the entity and verify the information acquired?

Yes

- d. Does your entity verify the true identity of customers, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data, or information?

Yes

- e. Does your entity verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person?

Yes, company/ICRE shall verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person.

- f. Does your entity identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable sources, such that the entity is satisfied that it knows who the beneficial owner is?

Yes

- g. Does your entity understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business relationship with its customers?

Yes

- h. Does your entity, on the basis of materiality and risk, conduct ongoing due diligence on the business relationship of existing customers?

Yes

- i. Does your entity perform enhanced due diligence for higher risk

categories of customer, business relationship or transaction and does it apply to existing customers?

Yes

- j. Does your entity apply reduced due diligence where there is low risk of ML or TF? What does your entity do in cases where it is unable to complete the COD measures required by existing internal rules or under CL 2018-48, as amended, the AMLA, as amended, and its IRR?

Yes, the company shall, on a risk-sensitive basis, apply enhanced due diligence measures.

- k. What does your entity do in cases where it is unable to complete the COD measures required by existing internal rules or under the CL 2018-48, as amended, the AMLA, as amended, and its IRR?

Where lower risks of ML/TF have been identified through an adequate analysis of risk by ICRE and based on the result of the institutional risk assessment, simplified or reduced customer due diligence measure may be applied.

- l. In case of non-face-to-face services, does the entity ensure that control measures to address risks associated with this type of business relationships or transactions are implemented?

Information on critical customer data in line with the CDD measures not obtained/disclosed despite diligent efforts which may lead to suspicious transactions, the same shall be reported to the Compliance Officer for appropriate action as follows:

Where ICRE/company is unable to comply/complete with the relevant CDD measures, it shall:

1. Refuse to open an account, commence business relations or perform the transactions; or shall terminate business relationships; and,
2. File an STR in relation to the customer, if circumstances warrant

3. Record Keeping and Retention Policies and Procedures

- a. What are the type of records and information that your entity maintains?

CDD information and transaction records of customers, account files and business correspondence are in original forms

- b. Do you maintain all necessary records on transactions and, if so, for how long following completion of the transaction? Who is/are the designated custodian that shall be accountable and responsible for safekeeping these documents?

Yes, the company maintain records for at least five (5) years from the date of transactions. For STR, as long as the business relationship, or the case if any, exists. A designated custodian is responsible for the safekeeping of records.

- c. Do you maintain records of the identification documents and information, account files and business correspondence and, if so, for how long following the termination of an account or business relationship?

Yes, the company maintains records of customer identification documents and information, account files and business correspondence for at least five (5) years from the dates of transactions. Records obtained through CDD, at least five (5) years following the termination/terminations of account.

- d. Do you ensure that all customer and transaction records and information are available on a timely basis to competent authorities? If yes, please indicate the designated custodian that shall be accountable and responsible for safekeeping and making these records available

Yes, the company shall ensure that all CDD information and transaction records are available swiftly to IC, AMLC and other domestic competent authorities in the exercise of their official functions or upon order by competent authority. Mr. Noel Tolete, our Finance Head is the designated custodian who is responsible for safekeeping of said records.

- e. Do you conduct compliance testing to ensure that all units and/or branches maintain and safely store KYC and transaction records?

Yes.

- f. Does the Internal Audit cover an assessment of compliance of the record-keeping and retention process?

No. The company does not have an Internal Audit group.

4. Continuing Education and Training Program

- a. Are newly hired employees required to attend AML and CTF training?

Yes. Training shall be conducted to all new employees, regardless of level of seniority, which includes the general appreciation of the background of money laundering, the need to be able to identify suspicious transaction and to report such transactions to the appropriate designated compliance Officer.

- b. Is there an existing training and refresher program for all responsible directors, officers and staff? Please provide a copy of the program.

None.

- c. Are the staffs of the Compliance Office and Internal Audit Office provided with training for combating money laundering and terrorist financing that is different from the staff of other offices?

Yes.

- d. Do you have an on-going director and employee training on ML and TF prevention? If yes, please indicate the last training and the schedule for the year.

None.

- e. Do you conduct a regular post-test on directors and employees to gauge their understanding of AMLA, as amended, its IRR, CL 2018-48, as amended, and other IC and AMLC relevant regulations?

None

- f. Provide statistics on education and training provided to responsible directors, officers and employees covering the immediately preceding year.

None

E. ICRE DATA/ INFORMATION

1. Provide information on the total asset of the entity as of 31 December of the immediately preceding year.

Total assets as of December 31, 2019 per Audited F.S. = P42,956,951.00

2. Provide a list of all products being offered/sold according to classification by the ICRE.

Motor Car Insurance; Bonds; Marine Insurance; Personal Accident Insurance; Fire Insurance; HMO; Engineering Insurance; and, Miscellaneous.

3. Provide data/information on products covering the immediately preceding year.

Product Classification	Total Premium(net of all taxes)/ Contract Price/ Membership Fees Received	Number of Issued or Sold Policies/Pre-Need Plans/HMO Agreements	Number of Outstanding Policies/Pre-Need Plans/HMO Agreements	Number of Policies/Pre-Need Plans/HMO Agreements/Surrendered/Cancelled
Motor Car	Ps 11,866,512.90	620	87	
Fire	20,148,721.90	263	36	
Bonds	9,030,346.70	225	10	
Marine	17,956.80	46	12	
PA/Health/HMO	37,641,898.11	259	59	
Engineering	451,049.85	19	1	
Miscellaneous	1,021,526.84	125	6	
Total	Ps 80,178,013.10	1557	211	

4. Provide number of suspicious and covered transactions reported to AMLC covering the immediately preceding year.

Type of Report	Number of Reports Submitted
Suspicious Transaction Reports	None
Covered Transaction Reports	None


CERTIFICATION

The undersigned President and AML and CTF Compliance Officer of the company certify that the responses and explanations set forth in the above AML and CTF Compliance Questionnaire are true, complete and correct of our own personal knowledge and/or based on authentic records.

Signed in the City of MAKATI 21 JUL 2021 on ___ day of July 2021.


CHONA M. JACINTO
President


CHONA M. JACINTO
AML and CTF Compliance Officer



JESUS D. GOMEZ
AML and CTF Asst. Compliance Officer
(Technical Head)

SUBSCRIBED AND SWORN to before me this 21 JUL 2021 day of July 2021, by the following who are all personally known to me and who exhibited to me their respective identification document as follows:

<u>Name:</u>	<u>ID No./Proof of Identity:</u>
Chona M. Jacinto	TIN: 115-795-676; Driver's Lic. No. N11-83-003529
Jesus D. Gomez	TIN: 100-891-713; Driver's Lic. No. N08-81-004180

Doc. No. 40
Page No. 09
Book No. 175
Series of 2021.

Page 40 of 40


ATTY. RAYMOND A. RAMOS
COMMISSION NO. M-239
NOTARY PUBLIC FOR MAKATI CITY
UNTIL DECEMBER 31, 2021 per B.M. No. 3795
11 KALAYAAN AVENUE EXTENSION,
BARANGAY WEST REMBO, MAKATI CITY
SC Roll No. 62179/04-26-2013
IBP NO. 137312/01-04-2021/Pasig City
PTR NO. MKT 8531022/01-04-2021/Makati City
MCLE Compliance No. VI-0007878/04-06-2018