ANSWER TO
AML AND CTF COMPLIANCE QUESTIONNAIRE

COMMONWEALTH INSURANCE COMPANY
NAME OF ICRE

March 30, 2022
Date Accomplished

A. BOARD OF DIRECTOR AND SENIOR MANAGEMENT OVERSIGHT

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

a. Yes. CIC shall develop sound risk management strategic and operational plans that ensures risk associated with money-laundering such as counterparty, reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of these regulations, to the end that CIC shall not be used as a vehicle to ML and TF conduit thus legitimizes proceeds of unlawful activity or to facilitate of finance terrorism.

The following are the details CIC's BOD and SM Oversight which ultimately responsible for effective management of the company in relation to AML/CTF risks:

i. The Board of Director's responsibility is to comply with the provisions and rules of AMLA, as amended and its RIRR.
ii. Ensure and oversight on the institution's compliance adequate management.
iii. Senior Management shall oversee the day to day management of the covered persons and entities;
iv. Ensure effective implementation of the AML/CFT policies approved by the Board and alignment of activities with the strategic objectives and risk profile;
v. Corporate values set by the aforementioned officers.
vi. Senior Management shall establish a management structure that promotes accountability and transparency and upholds checks and balances for the company to be safe from ML and TF risks;
vii. Ensure the implementation and effectiveness of the AML/CTF Risk management system and issue instructions for the corrective measures in pursuant to AML/CTF guidelines.
viii. Awareness and updating of the Sanction List released by AMLA and other government agencies in connection with money laundering activities;
ix. Dissemination of relevant information to all officers and staffs in all branches of CIC, who are obligated given their position to implement compliance measures; and

x. Compliance by all senior management, responsible officers, and employees with the Guidelines the AML and CFT laws, their respective implementing rules and regulations, other directives, guidance and issuances from the IC and AMLC and its own MLTFPP.

b. The policies and objectives of CIC are attained and done though periodic conduct of compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of AML and CFT transaction monitoring system and record retention system through sample testing and review of audit or checking reports. Under CIC's policy on KYC guidelines, client dealings shall be in accordance thereof, CDD and risk management is are also highly observed.

c. CIC shall promote high ethical and professional standards in the prevention of and not be used as a vehicle to Money Laundering and Terrorist Financing conduit thus legitimizes proceeds of unlawful activity or to facilitate of finance terrorism intentionally or unintentionally. Moreover, CIC regularly submits its compliances to Insurance Commission, particularly its STR and CTR, which is one of the monitoring tools that identifies if there is any suspicious and covered transactions in the company's clientele, which as todate, no such kind of transactions being encountered.

Board of Director (BOD) – shall approve a comprehensive, risk based ML/TFPP geared towards the promotion of high ethical and professional standards and the prevention of ML and TF. It receives plans and policies for their approval.

Senior Management (SM) – shall be responsible for compliance, as well as accountable for installing and maintaining systems and controls that ensure compliance with all relevant laws and regulations of the CIC.

Compliance Office – shall be responsible for the management of the implementation of CIC's Money Laundering and Terrorist Financing Prevention Program (MLTFPP) whose primary task of the Compliance and Administrative Division and the designated Compliance Officer/Coordinator.

Internal Audit – 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.

d. **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 ML/TF risk. An effective counter on the ML/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. Yes. The Compliance Office/Officer shall report directly to the BOD through the AMLC Committee on all matters related to AML and Terrorist Financing compliance and their insurance risk management. However, compliance office need not to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors. Thus, the Compliance Office/Officer must first report to the BOD before the senior management.

f. The following are the authorities delegated by the BOD to the Compliance Office and the

AML and CTF Compliance Officer in relation to ML and TF prevention:

1. Ensures compliance by the officers and employees with the provisions of the anti-money laundering law as amended, implementing rules and regulations thereto; conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system through sample testing and review of audit or examination reports; and report to the AMLCC any compliance findings;

2. Alerts senior management, the BOD or CIC AMLC Committee if it believes that the covered person is failing to appropriately address AML/CTF issues; and

3. Prepares and submits to the AMLC written reports on the Company's compliance with the provisions of anti-money laundering law, rules and regulations, in such form and submitted at such time as the Council may determine.

4. Responsible in reporting regularly in accordance with the existing guidelines of reporting suspicious transactions, may it be cash or electronic transaction or document related transaction.

g. The BOD and Senior Management adopts and ensure attainment of the entity's plans and objectives in a comprehensive and risk-based MLPP geared toward the promotion of high ethical and professional standards in the prevention of the Company 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. Yes. It is done through identifying, assessing and understanding its ML and TF risks in relation to its existing customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk based approach, including risk assessment in both quantitative and qualitative factors.

b. 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. The risk-based assessment of its clients and their transactions must be first determine by the Company as well as the appropriate level of enhanced due diligence necessary for those categories of clients and transactions that the Insurance Company has reason to believe pose a heightened risk of illicit activities at or through the Insurance Company. 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 and Compliance System Manual (Monitoring and Reporting Tools).

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

a. Yes, CIC conducted an over-all assessment of the entity's compliance through periodic review. The periodic updating, review of customer's KYC information, annual reports, typologies, and trends of ML/TF facilitates ongoing monitoring of the company. CIC's assessment against its fraud prevention program requires a conduct of periodic review once every two (2) years to verify that any of its branch or subsidiary operation is in compliance with the obligations imposed under the AMLC, its provisions and regulations.

b. Eighty Five (85%) to Ninety (90%) percent, more or less.

c. 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. Yes. Below is the summarized key findings and/or recommendation undertaken by the Company, however, the same yield negative result.

KEY FINDINGS	RECOMMENDED ACTIONS	Progress/ Development
Risk Assessment	Take appropriate steps to identify, asses and understand the risk in relation to customers, geographical exposures and documents its risk-based approach.	The BOD hereby appoints the SVP (Adviser) for Internal Audit to advise the compliance team on issuing and enforcement of in-house instructions to promote adherence to these rules.

e. N.A. The Company/ICRE has a centralized internal audit team.

KEY FINDINGS	RECOMMENDED ACTIONS	Progress/ Development
None	Not Applicable	Not Applicable

4. Management Information System

a. 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. Further, CIC has management information system which all relevant data of the company’s clients are recorded, in which it can also be cross-checked, verify and investigate the business transaction, if there exists any suspicious transaction.

b. 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 conclusions are made after thorough continuous monitoring conducted by the monitoring team in which thereafter submitted and reported to the designated regulating body, the BOD and SM for their verification and approval of the results. Reporting of the aforementioned transactions must be made immediately by the Compliance Officer's Team while the reporting of STR and CTR are made in accordance with the rules and requirements imposed by the AMLC.

c. Yes, the office of the Compliance Team and Corporate Secretary are both the designated custodians, 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. Yes, the office of the Compliance Officer as one of the 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. Names and contact details are as follows:

ROMEO C. DIOLATA
Compliance Officer
87500538
rcdiolata@cic.com.ph

GARY D. MORIONES
Primary Designated Officer
88187626 loc. 1264
gdmoriones@cic.com.ph

MARLON S. ESPINEDA
Associated Person
88187626 loc. 1268
marlon.espenida@cic.com.ph

LOURDES M. CORCELLES
SVP/Corp. Secretary
88187626 loc. 1010
lmc@cic.com.ph

b. The CIC Compliance Division formulates a non-life annual insurance training program aimed to provide efficient, adequate and continuous education program for all CIC 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.

Further the company ensures that any of its officers, employees or agents that may be found to have committed, conspired, abetted or aided in the commission of anti-money laundering or financing terrorists shall be meted out by appropriate disciplinary measures, not to mention the criminal and civil actions which may be filed against them in court.

c. Through a comprehensive company's framework and patterned with the guidance from AML provisions which enables the authorities to monitor and combat all transactions linked with money laundering. Further, assessment is done by an on-site visit to the company's branches, evaluation method of compliance with AML, continuous monitoring and management compliance, and internal communication of its policies, systems and controls to prevent and detect money laundering and terrorist financing. The directors, senior management, department heads, units, groups, branches and staffs are keeping known and inform of such, for their awareness and compliance with legal requirements with AML measures.

d. 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. 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. Yes. "The company strengthens the implementation of strict recruitment policies in hiring its company employees especially its marketing staffs, insurance adjusters, agents and other related personnel. It also regularly conducts mandatory trainings/seminars to continuously educate its marketing staffs and insurance agents for them to be updated on the current trends of the market". (Capter-3, E of AML Manual).

g. 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. The Directors are all elected every year by the stockholders during the annual stockholders meeting, to hold their office until their successors are appointed and qualified, unless removed earlier from office for cause or as may be provided for by law.

   He must possess the necessary expertise, experience and skills in terms of insurance industry. (Chapter-III, A Manual of Corp. Governance).

h. No. The company has no such foreign branches and/or subsidiaries.

i. No, since the company has no foreign branches and/or subsidiaries.

j. Money Laundering and Terrorist Financing Prevention Program (MTPP) provisions are disseminated through training programs consisting of conferences, and seminars. Further, these are also disseminated through soft copies via electronic mail to directors and staffs for their awareness of such policies, rules and procedures to prevent ML and TF. To test compliance with legal requirements thereof, the provisions of documentary materials for staff that has responsibility to apply AML measures.

k. The Compliance Office/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. Moreover, regular monitoring undertaken by the Compliance Officer to different departments ensuring proper compliance to the company's ML and TF prevention program is also strictly observed.

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

a. After submission of our company's AML/TFPP, there is no checking and findings recommended.

KEY FINDINGS	RECOMMENDED ACTIONS	Progress/ Development
None	Not Applicable	Not Applicable

b. The pre-set guidelines as well as deficiencies and weaknesses during internal and external audits are noted and corrected by:
   1. By identifying the matters of deviation to be corrected;
   2. CIC's AML regulations shall establish an internal and external reporting requirements addressing unusual and suspicious transactions;
   3. When there is an internal report on unusual or suspicious transaction, investigation shall follow in relation to which report was made;
   4. When there is an external suspicious transaction report, the steps shall be documented for investigation in relation to which the unusual transaction report is made;
   5. All relevant details of any internal and external suspicious transaction report must be kept for at least five (5) years from the date on which the report was made.
   6. 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. None yet.

b. No.

KEY FINDINGS	RECOMMENDED ACTIONS	Progress/ Development
NONE	NOT APPLICABLE	NOT APPLICABLE

c. The company/ICRE will take appropriate preventive measures to be conducted assess and determine in sectoral and national risk assessment before determining what is 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. Authorities' intervention may also be considered when greater weight and exposure to ML/TF risks on proper identification and assessment of sectoral and institutional risks.

B. MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM

1. Customer Identification, Verification and Ongoing Monitoring Process

a. 1.) In accordance with CIC's nature of business by providing insurance services to its clients, its CDD manual requires 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
iii. Periodically update the CDD information that it holds and adjust the risk assessment it has made accordingly;
iv. CIC shall not enter or entertain business proposals with a customer whose identity matches with any person or entity known to have links with terrorists or terrorist organization as well as those who are under the sanctions list of AMLA, AMLC, UNSC Consolidated List, UNSCR, among others.

3.) CIC'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. CIC 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. More so, CIC also prohibits untrue financial transactions or execution of such transactions with fictitious persons.

c. i. For new individual customer/client. The company/ICRE, shall develop a systematic procedure for establishing the true and full identity of the new individual customer/client, and shall open and maintain the account/relationship only in the true and full name of its owner/s. Unless otherwise stated in this Guidelines, average customer due diligence requires that ICRE shall gather from individual customer/client before or during the course of establishment business relationship.

For new juridical persons-customer/client. The company/ICRE shall develop a systematic procedure for identifying customer/client that are corporate, partnership and sole proprietorship entities, as well as their directors, officers, partners, owners and representatives. It shall open and maintain accounts only in the true and full name of the identity. Unless otherwise stated in this Guidelines, average due diligence requires that the ICRE shall obtain from their customer/client that are juridical persons the minimum identification documents before or during the course of establishing business relationships. The ICRE shall understand the nature of the customer's business, its ownership and control structure.

For legal arrangement (Trust or Similar Arrangement). When performing due diligence measure, the ICRE shall identify and verify the identity of the customer, understand the nature of business, and its ownership and control structure. Unless otherwise stated in this Guidelines, average due diligence requires that ICRE shall obtain from their customer/client under legal arrangement the minimum identification information and documents before or during the course of establishing business relationships.

ii. Yes. Satisfactory evidence of new customer's or non-client's identity shall be obtained. Where applicable, transactions undertaken for non-clients or non-account holders demand special care and vigilance. Where the transaction involves significant amount, the customer should be required to produce positive evidence of identity. Moreover, effective procedures for verifying the bona fides of this kind of customers shall be implemented. In this regard, the Board of Directors and Senior Management shall ensure that the Company is not used to facilitate money laundering. It is the policy of the entity/ICRE 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. In sum, CDD must be applied.

iii. Yes. Where an account is occasional transaction in excess of the threshold is conducted, evidence of the true and full identity, occupation or business purpose/s of the clients, as well as other identifying information when carrying out occasional transactions shall be strictly obtained. ICRE 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. Yes. ICRE shall verify the validity of the authority of trustee, nominee, agent or intermediary. It shall determine the true nature of the beneficial owner's capacities and duties vis-a-vis his agent by obtaining a copy of written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of CDD to be applied to both. However, in case it entertains doubt as to whether the account holder or person purporting to act on behalf of the customer is being used as a dummy in circumvention of existing laws, it shall apply EDD and file an STR, if warranted.

v. Yes. The ICRE shall identify and take reasonable measure to verify the identity of beneficial owners who ultimately have a controlling ownership-interest in a juridical person; in case of doubt whether the person with controlling interest-ownership are the beneficial owners **or** where no natural person exerts control through ownership-interests, the identity of the natural person, if any, exercising control over the juridical person through other means; and, where no natural person identified, the identity of relevant natural person who holds senior management position.

vi. The ICRE should employ EDD if it acquire information that: A. raises doubt as to the accuracy of any information or document provided by the customer or ownership of the entity (Sec. 29, A of CL No.2018-48); and, The ICRE shall apply EDD on the customer/client if it acquires information in the course of its customer account or transaction monitoring that: 1. Raises doubt as to the accuracy of any information or document provided or the ownership of the juridical person or legal arrangement (Sec. 35, B-1 of CL No.2018-48).

d. For life or other investment-related insurance business, the CIC/ICRE, in addition to the CDD measures required for customer and the beneficial owner, conduct the following as soon as beneficiary/ies are identified/designated;

a. For beneficiaries that are identified as specially named natural or legal persons or legal arrangements - by taking the name of the person;
b. For beneficiaries that are designated by characteristics, by class or by other means – by obtaining sufficient information concerning the beneficiary to satisfy the ICRE that it will be able to establish the identity of the beneficiary at the time of payout.

Information collected should be recorded and maintained in accordance with the provisions under Title VI of this Guidelines. Where the ICRE is unable to comply with the forgoing, it should consider making a suspicious transaction report.

e. Individual Minimum Information. The ICRE shall develop a systematic procedure for establishing the true and full identity individual customer, and shall open maintain full name of the account owners. Unless otherwise stated in the guidelines, average customer due diligence requires that the ICRE shall gather from individual customer, before or during the course of establishing business relationship, the following minimum information and identification document:

1.) Identification Information:
-Full name;
-Date & place of birth;
-Sex;
-Citizenship or nationality;
-Address;
-Contact number or information;
-Source of fund;
-Specimen signature or biometric information; 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. Juridical Entities Minimum Information. The ICRE shall develop a systematic procedure for identifying customer that are corporate, partnership, sole proprietorship entities, as well as their stockholders, partners, owners, directors, officers, and authorized signatories. Unless otherwise stated in this guidelines, average due diligence requires that the ICRE 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;
-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 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.

The ICRE shall understand the nature of the customer's business, its ownership and control structure.

g. 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. 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. The 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. 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.

    CIC shall establish and record the true and full identity and existence of both the: (a) agent (trustee/nominee); and,
    (b) principal (trustor/beneficial owner) or person on whose behalf the account is being opened. CIC shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same criteria for assessing the risk profile.

j. Yes. The company/ICRE, 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, CIC, 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.

CIC/ICRE 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. Yes. The company/ICRE shall determine and understands as appropriate, obtain information, the purpose, and intended nature of the account, transaction, or business relationship with its' customers. Upon or at the time of account opening, all the minimum information and confirmation of this information with the valid identification documents hereof from individual customers shall be secured and recorded, the same with the authorized signatory/ies of corporate and juridical entities. CIC with the gathering of such information adheres to the company's KYC principle and the same is also protected under the Data Privacy and Protection Act. Such information given by the client is solely for the purposes of business transaction and shall not be allowed for any purposes other than the intended one, unless, otherwise, there exists a suspicious transaction, the same shall be turned over to the lawful authorities subject to the lawful directives of the court.

l. CIC 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.

The company scrutinizes and an ongoing monitoring is conducted in relation to all business relationships and transactions, but the extent of monitoring should be based on risk as identified in the company's risk assessment and its own CDD

efforts. Enhanced monitoring should be adopted and undertaken for higher risk-customer transactions.

It is the policy of the company/ICRE to carry out cross-sectional product/service monitoring in order to identify and mitigate the emerging risk patterns. A risk-and-materially based ongoing monitoring of customer's account and transactions is part of CDD.

m. Yes. Whenever EDD is required or where the risk are higher, the ICRE 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 ICRE 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 ICRE deems reasonable or necessary

   The company/ICRE shall at all times apply a–risk-sensitive approach in determining the nature and extent of EDD. It shall develop a clear, written and graduated customer acceptance and identification policies and procedures, which shall include sanctions screening. Enhanced Due Diligence for High Risk customers is applied as required by the customer identification policy in addition to the KYC identification requirements, as follows:

   A.) Obtain additional information other than the minimum information and/or documents required for the conduct of average due diligence;

      (a) In cases of individual customers, i. supporting information on the intended nature of the business relationship/source of funds/source of wealth, ii. Reasons for the intended or performed transactions, iii. list of companies where he is a director, officer or stockholder, iv. list of banks where the individual has maintained or is maintaining an account, and

v. other relevant information available through public databases or internet.

(b) For entities assessed as high risk customers, such as shell companies; i. prior or existing bank references, ii. the name, present address, nationality, date of birth, nature of work, contact number, and source of funds of each of the primary officers (President, Treasurer and authorized signatory/ies), stockholders owning at least 20% of the voting stock, and directors/trustees/partners as well as their respective identification documents; iii. volume of assets, other information available through public databases or internet; iv. supporting information on the intended nature of the business relationship, source of funds or source of wealth; and v. reasons for the intended or performed transactions.

B.) Conduct validation procedures on any or all of the information provided

C.) Secure senior management approval or the AML Compliance Committee approval to commence business relationship.

D.) Conduct enhanced ongoing monitoring of the business relationship

E.) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In Preparing the risk assessment, the entity shall take into account of all relevant risks and shall consider, in particular, the relevance of the following:

1.) Customer risk;
2.) Product risk;
3.) Delivery risk; and,
4.) Country risk.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, CIC shall deny business relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when so warranted.

n.

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. It shall be commensurate with the lower risk factors. Examples of possible measures are:

A.) Verifying the identity of the customer and beneficial ownership after the establishment of business relationships;

B.) Reducing the frequency of identification updates;

C.) Reducing the degree of ongoing monitoring and scrutinizing transactions based on reasonable monetary threshold;

D.) Avoid collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

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.

The Sales and Marketing Group and Operations Department shall comply with the following guidelines for establishing the true and full identity of the customers:

Reduced Due Diligence for Low Risk Customer

I. For individual customers, CIC may allow an account under the true and full name of the account owner/s upon presentation of acceptable identification card or official document as defined in this Manual or other reliable, independent source documents, data or information.

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 including GOCCs, CIC 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.

In certain exemption, Reduced Due Diligence may be permitted for customers that are resident of another country. The entity may issue guidelines allowing certain exemptions on

CDD measures, taking into account the nature of the product, type of business and risk involved, provided that ML/TF are effectively managed. (Ex. Foreign regulated person, the securities of which are listed on a recognized exchange).

o.

Where 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. (Sec. 45, CL 2018-48).

It is the policy of the entity/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.

The ICRE shall establish and record the true and full identities of PEPs, their family members, close relationships/associates and entities related to them. Carefully consider a PEPs 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 PEPs. 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 PEPs. 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 PEPs;
    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.

As a general rule, no transactions or new accounts shall be opened and created without face-to-face contact and personal interview between CIC's/ICRE's 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 CIC/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*. It must be noted, that incomplete documents after having provided the list for required documents but still the same is incomplete, shall not be entertained by the company.

The entity shall also apply the following measures when it is applying due diligence measure to non-face-to-face customers:

a.) perform at least one additional check designed to mitigate the risk of identity fraud; and,
b.) apply such additional enhance CDD Measures or undertake enhance ongoing monitoring as it considers appropriate.

r.

In some business instances, the company/ICRE may resort to third party referred by brokers or intermediaries 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 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.

The entity/ICRE may rely on a third party provided the same must be a covered person defined under the AMLA, its RIRR, 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 in accordance with this part and its own ML/TFPP, including the face-to-face contact requirement to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and,
2.) Reliance by ICRE shall have the ability to obtain identification documents from the third party upon request without delay.

The entity/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 TFPSA, 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 CIC/ICRE relying on the third party. Provided that, in cases of high-risk customers, the ICRE shall also conduct enhance due diligence procedure.

t.

The company/ICRE may outsource the conduct of customer identification and due diligence, including face-to-face contact through counterparty or intermediary. The identification and due diligence performed shall be equally regarded as those of the ICRE's itself. The ultimate responsibility and accountability for identifying the customer and keeping of documents remains with the ICRE.

The ICRE and counterparty or intermediary shall enter into an arrangement clearly specifying the following minimum responsibilities of the latter, to wit:

1.) Can obtain immediately the necessary information concerning CDD as required under the Guidelines;
2.) Has an adequate CDD processes;
3.) Has measures in place for record keeping requirements; and,
4.) Can provide the CDD information and provide copies of relevant documentation immediately upon request.

The counterparty or intermediary performing the conduct of customer identification and due diligence, as a minimum, must comply with the requirements provided under AML and TFPP, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances.

u.

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 CIC 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. As well as, where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, CIC shall deny business relationship with the said customer without prejudice to the reporting of a suspicious transaction to the AMLC when so warranted.

v.

The entity/ICRE shall apply countermeasures, conduct 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.

Yes. There are measures in ensuring that funds collected by or transferred through non-profit organizations are not diverted to support unlawful activities. CIC 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. Anyone who conducts a financial transaction with knowledge that the funds are proceeds of an unlawful activity is generally considered to be laundering money. The Company may require additional identification documents to further vouch the identity of the clients.

x.

The entity/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.

CIC as a legitimate insurance company regulated by the Insurance Commission has the obligation to coordinate with lawful authorities relevant to United Nations Security Council Resolutions (UNSCR) in charge of AML/CFT investigations for the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing in accordance with the AMLC guidance of standards and procedures. The company has the obligations, all duties, functions and powers relating to monitoring, supervision and investigation, enforcement in respect of the regulations enacted by the government in relation to the prevention and detection of money laundering (including responsibility for overseeing compliance by persons to whom such Regulations apply). Information on applicable laws and regulations regarding the prevention of money laundering should be obtained. CIC considers appropriate to cooperate with and provide assistance to overseas regulators in the exercise of their functions or in connection with the prevention or detection of financial crime. CIC is fully aware that noncompliance with the obligations as stated in the requirements set out in the AML Law Regulations may be sanctioned by the AMLC Regulatory and may also be discipline by other related authority.

2. Record Keeping and Retention Process

a.

Under the guidelines on digitization of customer records, ICRE/CIC shall retain all transaction records either in:

a.) original forms; or,
b.) such other forms sufficient to permit reconstruction of individual transactions so as to provide admissible evidence in court. (Sec. 20, CL 2019-65).

For low risk customers, ICRE maintains and stores in whatever form, (microfilm, or electronic form) a record or information data and transactions, sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Further, E-Commerce Act, and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court, said records shall be maintained in an organized and confidential manner pursuant to the application of Customer Diligence Measures or information that enables a copy of such records obtained, which allows the IC, AMLC, other competent authorities and the courts to establish an audit trail for money laundering and terrorist financing. Further, the company ensures that all CDD information and transaction records are available and readily accessible to CIC, IC, AMLC and upon order of other competent authorities.

b.

Yes, CIC shall maintain, preserve, and safely store for at least five (5) years following the completion of transactions, all records of customer identification and transaction documents, or as long as the business relationship exists. If a case has been filed in court involving the account and/or transaction, records must be retained, preserved and safely kept even beyond the five (5) year periods, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality. The Compliance Office Team is the designated custodian authorized by the company to safe keep all documents in relation to anti-money laundering and terrorist financing, as well as accountable and responsible in the preservation, storage and maintenance thereof.

c.

Yes, CIC shall also maintain, preserve, and safely store for at least five (5) 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. The company shall likewise keep the electronic copies of all covered and suspicious transaction reports for at least five (5) years from the dates of submission to the AMLC.

However, if the case has been filed in court involving the account and or transaction, records must be retained, preserved, and safely kept even beyond the five (5) year period until it is officially confirmed by the AMLC Secretariat that the case have been resolved, decided, or terminated with finality notwithstanding the above mentioned periods,

d.

Yes. The entity/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.

CIC ensures that all customer information and transaction records are available and readily accessible in the company's systems and controls in which those are maintained to prevent money laundering and terrorist financing. The Compliance Office/Team is the designated custodian that shall be accountable and responsible for safekeeping and making the records available as well as enables the supervisory authority, internal and external auditors and other competent authorities satisfy upon demand by any regulatory enquiry or court order to disclose information.

3. Covered and Suspicious Transactions Reporting

a.

None yet. The company is using manual procedure but there is plan to have the same be installed and programmed electronically.

b.

CIC manually perform the functionalities of covered and suspicious transactions by implementing stage procedures classifying them into suspicious and non-suspicious ones. Gathering of information, documents and making preliminary analysis for the compliance officer and his team's reference in case suspicious transactions arises. A Manual

Procedure that requires the management, branches and its employees to be compliant therewith. Keeping an integral database of customer accounts and their transactions with the use of computer and or through the original documents and papers submitted. Setting a program for upgrading customer identities, papers and documents as well as a quick and direct mechanism to notify or report suspicious operations.

The ultimate test is, that the entity/ICRE ensures the means of flagging and monitoring the transactions capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risk, and to regularly apprised the board of directors and senior management on AML/CTF compliance. Maintain a register of all ST's that have been brought to the attention of senior management whether or not the same was reported to the AMLC. Further, CIC regularly submits it STR and CTR in compliance with Insurance Commission's mandate in monitoring any suspicious or unscrupulous transactions.

c.

Yes. Unusual transaction are those that are outside the normal course of business for the company or person, or that otherwise appear to be unusual due to their timing, amount involve, size, nature of business transactions. Unusual activities of customers that may put the Company at risk shall be reported to the AMLC Committee. Unusually large transactions and all unusual patterns of transactions which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious are still be strictly monitored. To this extent, the Company shall apply enhanced due diligence on its customer if it acquires information in the course of its customer account or transaction monitoring.

d.

Yes. CIC, before reporting 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. 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.

If there is reasonable ground to suspect that the client has engaged in an unlawful activity, the AML Compliance Committee, upon receiving such report shall promptly evaluate whether the suspicion is valid. The case shall be immediately reported to the AMLC unless the Committee considers that such reasonable grounds do not exist. However, those unreported suspicion including transactions that are not reported to the AMLC shall be properly recorded.

That after internal and external investigation of the company and had gathered satisfactory evidence and information to believe that such transaction must be reported as suspicious transactions shall be reported and filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.

e.

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. CIC'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.

If there is reasonable ground to suspect that the client has engaged in an unlawful activity, the AML Compliance Committee, upon receiving such report shall promptly evaluate whether the suspicion is valid. This case shall be immediately reported to the AMLC unless the Committee considers that such reasonable grounds do not exist. However, those unreported suspicion including transactions that are not reported to the AMLC shall be properly recorded.

f.

CIC has implemented its own standard and procedures in combatting money laundering and terrorist financing. Such guidelines are in accordance with the rules promulgated by the implementing authorities like AMLA, AMLC, and IC. Hereunder are the instances where CIC/ICRE considered when reporting STR or when alert has been tagged:

1.) When there business transactions have no apparent purpose and which make no obvious economic sense;
2.) When during transaction a customer requested without reasonable explanation, which are out of the ordinary range of services requested or are outside the experience of the handling person;
3.) When the amount or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged;
4.) When a customer refuses to provide the information requested without valid reason;

5.) When an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;
6.) Unnecessary routing of funds through third party accounts;
7.) Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;
8.) Substitution, during the life of an insurance contract of the ultimate beneficiary with a person without any apparent connection with the policy holder;
9.) Unusual transactions without an apparently profitable motive; and,
10.) Any other or similar indicators as may be detected by the ICRE from time to time.

g.

The entity/ICRE assures no administrative, criminal or civil proceedings shall lie against any person for having made a covered transaction or suspicious transaction report in the regular performance of his/her duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any Philippine law.

CIC has the legal protection with its officers and or staffs who report their suspicion in accordance with legal obligation to report and are only effectively discharging their obligations to prevent money laundering and terrorist financing in the company.

h.

When reporting covered (CTR) or suspicious transactions (STR), CIC 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/Coordinator shall notify in writing the AMLC Committee.

However, in cases where the ICRE's form a suspicion of ML/TF and associated unlawful activities, and it is reasonably believe that performing the CDD process will tip-off the customer, they (entity/ICRE) need not pursue the CDD process, but instead, should file an STR, closely monitor the account, and review the business relationship.

4. Employment and Training Program

a.

Commonwealth Insurance Company shall apply the following standards when hiring new staff to the Compliance Office, the Internal Audit and the Company in general:

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.

CIC shall provide education and training for its entire staff and personnel particularly newly hired ones, to ensure that they are fully aware of their personal obligation and responsibilities in combating money laundering and the terrorist financing and to be familiar with the standard and procedures when reporting, and investigating suspicious matters. CIC ensures that the potential employee before hiring has adequately screened, including conducting criminal background checks, and verifications from previous employers.

b.

The company/CIC 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 refresher training shall be conducted, at least once a year to remind key personnel of their responsibilities and to make them aware of changes in the law, rules and regulations relating to money laundering as well as the internal policies and procedures.

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. Group Discussion and Interaction;
7. Freeze Compliance, Bank Inquiry, and Asset Preservation; and,
8. Cooperation and Reporting to I.C. and AMLC.

c.

Yes. In General, 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 and Internal Audit 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.

Yes. The last training was held on December 07, 2021, in Makati City.

Once every year preferably summer or December.

In the modern competitiveness environment, it is the policy of the company/ICRE to provide education and training to all employees and officers for they need to replenish their knowledge and acquire new skills to do their jobs in combating money laundering and be familiar with the system of investigating and reporting suspicious transaction. The Company

wants them to feel confident about improving efficiency and productivity as well as finding ways towards personal development and success.

C. INTERNAL CONTROLS AND AUDIT

1. CIC's Internal Audit Office has the utmost support of the top management and the Board. The Office as a whole is very much acquainted with the culture and business environment of the Company. In order to maintain the independence of the Internal Audit Department, it reports directly to the Audit Committee of the Board of Directors.

   The internal audit department is established by the Board of Directors, Audit Committee, or highest level of governing body (hereafter referred to as the Board). The internal audit department's responsibilities are defined by the Board as part of oversight role.

   The department has governed itself by adherence to The Institute of Internal Auditor's mandatory guidance for the Professional Practice of Internal Auditing (Standards).

   The duties and responsibilities of the Internal Audit are as follows:

   a.) Evaluating risk exposure relating to achievement of the organization's strategic objectives;
   b.) Evaluating the reliability and integrity of information and the means used to identify measure, classify, and report such information;
   c.) Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws and regulations which could have a significant impact on the organization;
   d.) Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets;
   e.) Evaluating the effectiveness and efficiency with which resources are employed. Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned;
   f.) Monitoring and evaluating governance processes;
   g.) Monitoring and evaluating the effectiveness of the organization's risk management process;
   h.) Evaluating the quality of performance of external auditors and the degree of coordination with internal audit;

i.) Performing consulting and advisory services related to governance, risk management and control as appropriate for the organization;
j.) Reporting periodically on the internal audit's purpose, authority, responsibility, and performance relative to its plan;
k.) Reporting significance risk exposure and control issues, including fraud risk, governance issues, and other matters needed or requested by the Board; and,
l.) Evaluating specific operations at the request of Board or management, as appropriate.

2. CIC 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. CIC also measures if these officer, staff and employees are effectively discharging their functions and regulatory obligations to prevent money laundering, terrorist financing in compliance with senior management's instructions and company's guidelines.

   The internal procedures, policies, and controls to prevent ML/TF are disseminated to the in the forms of memorandum and email letters to the concern 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. The Company/ICRE requires its Audit Department to 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 internal 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 concerned department in order that necessary requirements are complied.

D. IMPLEMENTATION

1. Covered and Suspicious Transaction Reporting Policies and Procedures

a.

None yet. The company is presently using manual procedure but there is plan to have the same be installed and programmed electronically.

b.

CIC has the means of complying manually with the AML regulations, its internal policies and Compliance System Manual (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 dubious transactions, particularly, cash or electronic 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 stage procedures, classifying them into suspicious and non-suspicious ones. Gathering of information, documents and making preliminary analysis for the compliance officer and his team's reference 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.

Yes. Unusual transactions are those outside the normal course of business for the company or person, or that otherwise appear to be unusual due to their timing, amount size shall be made immediately. Unusual activities of these types of customers shall be reported to the AMLC Committee. Unusually large transactions and all unusual patterns of which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious are still be strictly monitored. To this extent, the Company shall apply enhance due diligence on its customer if it acquires information in the course of its account transaction monitoring.

d.

Yes. CIC, before reporting 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. 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.

If there is reasonable ground to suspect that the client has engaged in an unlawful activity, the AML Compliance Committee, upon receiving such report shall promptly evaluate whether the suspicion is valid. The case shall be immediately reported to the AMLC unless the Committee considers that such reasonable grounds do not exist. However, those unreported suspicion including transactions that are not reported to the AMLC shall be properly recorded.

That after internal and external investigation of the company and had gathered satisfactory evidence and information to believe that such transaction must be reported as suspicious transactions shall be reported and filed in the forms prescribed by the AMLC and submitted in a secured manner to the AMLC in electronic form.

e.

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. CIC'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.

If there is reasonable ground to suspect that the client has engaged in an unlawful activity, the AML Compliance Committee, upon receiving such report shall promptly evaluate whether the suspicion is valid. This case shall be immediately reported to the AMLC unless the Committee considers that such reasonable grounds do not exist. However, those unreported suspicion including transactions that are not reported to the AMLC shall be properly recorded.

f.

CIC has implemented its own standard and procedures in combatting money laundering and terrorist financing. Such guidelines are in accordance with the rules promulgated by the implementing authorities like AMLA, AMLC, and IC. Hereunder are the instances where CIC/ICRE considered when reporting STR or when alert has been tagged:

1.) When there business transactions have no apparent purpose and which make no obvious economic sense;
2.) When during transaction a customer requested without reasonable explanation, which are out of the ordinary range of services requested or are outside the experience of the handling person;
3.) When the amount or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged;
4.) When a customer refuses to provide the information requested without valid reason;
5.) When an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;
6.) Unnecessary routing of funds through third party accounts;
7.) Insurance premiums have been paid in one currency and requests for claims to be paid in another currency;
8.) Substitution, during the life of an insurance contract of the ultimate beneficiary with a person without any apparent connection with the policy holder;
9.) Unusual transactions without an apparently profitable motive; and,
10.) Any other or similar indicators as may be detected by the ICRE from time to time.

g.

The entity/ICRE assures no administrative, criminal or civil proceedings shall lie against any person for having made a covered transaction or suspicious transaction report in the regular performance of his/her duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any Philippine law.

CIC has the legal protection with its officers and or staffs who report their suspicion in accordance with legal obligation to report and are only effectively discharging their obligations to prevent money laundering and terrorist financing in the company.

h.

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

i.

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

j.

Yes. When reporting covered (CTR) or suspicious transactions (STR), CIC 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 or employee 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/Coordinator shall notify in writing the AMLC Committee.

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

a.

i

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.

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. CIC 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.

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.

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, CIC shall apply the "Know Your Customer" principle in deciding whether or not to proceed with the business.

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.

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.

In assessing the risk profile of the parties, the covered person shall also consider the financial profile and other relevant information of the active signatories.

b. No. Because the company/CIC belongs to non-life insurance and surety industry.

c. Yes.

d. Yes.

e. Yes. CIC/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.

In case of doubt as to whether, the agent, trustee or nominee is being used as a dummy in circumvention of existing laws, further inquiries shall be immediately made to verify the status of the business relationship between the parties. If 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.

f. Yes.

g. Yes.

h. Yes.

i. Yes.

j. Yes. CIC shall, on a risk-sensitive basis, apply enhanced due diligence measures and undertake enhanced Ongoing Monitoring to insure compliance under CL 2018-48, as amended, the AMLA, as amended, and its IRR.

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

a.) Verifying the identity after the establishment of the business relationships;
b.) Reducing the frequency of customer identification updates;
c.) Reducing the degree of on-going monitoring; and,
d.) Not collecting specific information, but inferring the purpose and nature from the type of transactions or business established.

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

a.) Refuse to open an account, commence business relations or perform the transactions; or shall terminate business relationships; and,

b.) File an STR in relation to the customer, if circumstances warrant.

l. 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:

a. Refuse to open an account, commence business relations or perform the transactions;
or shall terminate business relationships; and,

b. File an STR in relation to the customer, if circumstances warrant.

m. Yes.

3. Record Keeping and Retention Policies and Procedures

a. CDD information and transaction records both natural and juridical person, account files and business correspondence. It shall retain all records either:

a.) In their original forms; or,

b.) Such other form sufficient to permit reconstruction of individual transactions so as to provide admissible evidence in court.

For low risk customer, the ICRE/company shall maintain and store in whatever form, a record of information data and transactions, sufficient to permit reconstruction of individual transaction so as to provide, if necessary, evidence for prosecution of criminal activity.

b. Yes, CIC 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. The Compliance Office/Team, is the designated custodian and who is also responsible for the safekeeping.

c. 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. CIC shall likewise keep the electronic copies of all covered and suspicious transaction reports for at least five (5) years from the dates of submission to the AMLC.

d. 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.

e. Yes.

f. Yes. Internal Audit group perform periodic review and assessment to determine compliance of existing laws and regulations including record keeping and retention process. (Chapter 5, D. of ML/TFPP).

4. Continuing Education and Training Program

a. 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. Yes. Please see attached Training and Refresher Program. The company provides for refresher trainings to review updates to compliance measures as they arise form new legislation, IC and/or AMLC issuances, internal audit findings and discoveries in ML/TF trends and detection techniques at least every two (2) years.

c. Yes.

d. Yes. December 07, 2021, at Makati City - Head Office.

e. Yes. By developing and creating opportunities for continuing education and training programs for its directors, officers, and employees to promote AML/CTF awareness and strong compliance culture.

f.

Classification (e.g. new employees; board of	Total Number per Classification	Number of Training Hours	Date of Training	Number of directors, officers and employees

directors; agents; officers; etc.)				who completed the training
Directors; &, Officers	9 16	Four (4) hrs. Four (4) hrs.	Dec. 07,2021 (8:30a.m.-12n.n. and 1:30p.m.-5:00p.m.)	9 Directors; 16 Officers;

E. ICRE DATA/ INFORMATION

1. Tentative Total assets as of December 31, 2021 per Audited F.S. = P4,091,125,821.67

2. Tentative Non-Life Insurance: Motor Car Insurance; Bonds; Marine Insurance; Personal Accident Insurance; Fire Insurance; Engineering Insurance; Special Risks; and, Miscellaneous.

3.

Product Classification	Total Premium/ 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	P 1,188,311,202.53	55,855	22,318	1,115
Motor Car-CTPL	148,305,487.29	381,934	-	-
Fire	25,645,516.92	3,977	664	12
Bonds	479,733,495.41	38,155	8,034	133
Personal Accident	5,235,962.70	292	-	7
Engineering	105,267,177.62	3,652	690	50
Miscellaneous	8,482,957.01	1,051	72	24
Marine	12,031,585.79	531	113	10
Equipment Floater	101,426,254.92	1,178	284	39
Total	**P2,074,439,640.19**	**486,625**	**32,175**	**1,390**

4.

Type of Report	Number of Reports Submitted
Suspicious Transaction Reports	4 Reports electronically submitted quarterly (monthly report covering Jan-Dec 2021)
Covered Transaction Reports	4 Reports electronically submitted quarterly (monthly report covering Jan-Dec 2021)

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 on 30th day of March, 2022.

MARIO A. NOCHE
President

ROMEO C. DIOLATA
AML and CTF Compliance Officer

SUBSCRIBED AND SWORN to before me this 30th day of March, 2022, by the following who are all personally known to me and who exhibited to me their respective identification document as follows:

Name:	ID No./Proof of Identity:
Mario A. Noche	TIN: 123-271-559; SSS No. 03-5196074-7
Romeo C. Diolata	VIN: 5905-0297A-L1764RCD1000; TIN-183-132-322

ATTY. JUAN JAIME D. NOLASCO
Notary Public
Until June 30, 2022
PTR No. 4863719
Mand. City / - 1/3/2022
IBP No.171577 – 1/3/2022
Roll No. 60888
MCLE No.VI-0020547-04/14/2022

Doc. No. 09;
Page No. 02;
Book No. 32;
Series of 2022.