



RF INSURANCE
BROKERS, INC.

RF Insurance Brokers Inc.

Unit 14B 14th Floor, Petron MegaPlaza Building,
358 Sen. Gil J. Puyat Ave., Makati City
Telephone Nos.: (02) 8646-0422
TIN: 634-563-945-00000

20 June 2025

ATTY. REYNALDO A. REGALADO

Insurance Commissioner

INSURANCE COMMISSION

1071 United Nations Avenue, Ermita,
Manila

Thru: **Anti-Money Laundering and Corporate Governance Division**

Re: **TRANSMITTAL LETTER**
Submission of MTPP Manual and Appointment of Compliance Officer of
RF Insurance Brokers Inc.


Dear Hon. Commissioner Regalado,

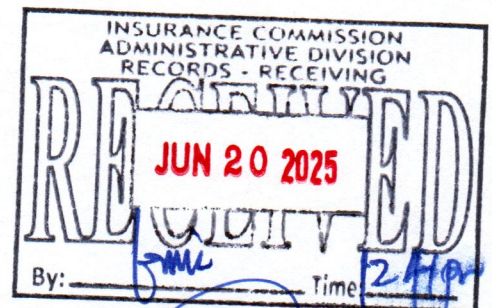
In compliance with IC Circulars, we hereby submit the following documents:

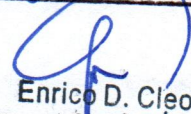
1. RFIBI's 2025 AMLA Operating Manual: Money Laundering and Terrorist Financing Program (MTPP)
2. Board Resolution on the Appointment of Compliance Officer/ Primary Designated Officer of RF Insurance Brokers Inc. ("RFIBI")

We hope that you find everything in order. Thank you very much!

Very truly yours,


ELJENE M. GOMINTONG
Corporate Secretary




Enrico D. Cleofas
Insurance Commission - Admin:
Records - Receiving

REPUBLIC OF THE PHILIPPINES)
CITY OF MAKATI) S.S.
METRO MANILA)

CORPORATE SECRETARY'S CERTIFICATE

I, **ELJENE M. GOMINTONG**, of legal age, Filipino, and with office address at Unit 14B, Petron Mega Plaza Building, 358 Sen. Gil J. Puyat Ave., Makati City, having been sworn according to law, hereby depose and state that:

1. I am the duly elected and qualified Corporate Secretary of **RF INSURANCE BROKERS INC.**, (doing business under the names and styles of "**Rampver Insure and RFIBI**"), a domestic corporation with principal office address at Unit No. 14B Petron Mega Plaza Building, 358 Sen. Gil J. Puyat Ave., Makati City.
2. During a special meeting of the members of the Board of Directors held on June 16, 2025 at the above stated office, following resolution was duly adopted:

"BOARD RESOLUTION"

WHEREAS, the Corporation **RF INSURANCE BROKERS INC.** is one of the Covered Institutions that is mandated to comply with the SEC Memorandum Circular No. 16, Series of 2018: "2018 Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for SEC Covered Institutions (AML/CTF)" and IC Circular Letter No. 2019-65, amending CL No. 2018-48 dated 14 September 2018 and CL No. 2018-60 dated 15 November 2018 by formulating an MTPP that is consistent with the AML and CTF Laws, IRRs, Guidelines and other applicable IC and AMLC issuances and by submitting an updated MTPP Manual, which shall be updated at least once every two (2) years or as necessary.

NOW THEREFORE, on motion made and duly seconded, the following resolutions are hereby adopted:

RESOLVED, that a new MTPP has been prepared, duly noted and approved by the Board of Directors of **RF INSURANCE BROKERS INC.**

RESOLVED, that the Company's 2025 AMLA Operating Manual: Money Laundering and Terrorist Financing Prevention Program (MTPP) establishes internal policies, procedures, and controls for the detection, prevention, and reporting of suspicious transactions, and sets of frameworks for ensuring compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations.

RESOLVED, that the Corporation, approves and confirms that the adoption of the Company's 2025 AMLA Operating Manual: Money Laundering and Terrorist Financing Prevention Program (MTPP) is in accordance with the guidelines and requirements set forth by the Anti-Money Laundering Council (AMLC) and other relevant regulatory bodies. The program has been reviewed and approved for implementation within the company.



Adopted this JUN 19 2025 of June 2025 in Makati City, Philippines by the affirmative vote of the undersigned members representing a majority of the directors of RF INSURANCE BROKERS INC.


REX MARIA A. MENDOZA
President


MARIA ANNA CONCEPCION G. MENDOZA
Director


JANICE MARIE P. FERNANDO
Director


ENRIQUE ROMEO G. MENDOZA
Director

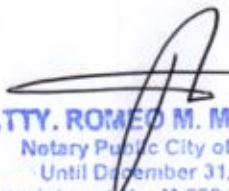
BERNARDO F. ABIS
Director

3. This certification is executed to attest to the truth of the foregoing and for whatever purpose this may serve.


ELJENE M. GOMINTONG
Corporate Secretary

SUBSCRIBED AND SWORN to before me this JUN 19 2025 day of 2025 at Makati City, after affiant exhibited to me and I confirmed the affiant's identity through her validly issued Philippine Passport with number P6103011B issued on 15 January 2021, by the Department of Foreign Affairs, Manila, and valid until 14 January 2031. Which Passport bears his photograph and signature.

Doc. No. 760
Page No. 63
Book No. 96
Series of 2025.


ATTY. ROMEO M. MONFORT
Notary Public City of Makati
Until December 31, 2025
Appointment No. M-032 (2024-2025)
PTR No. 10456008 Jan. 2, 2025/Makati City
IBP No. 306870 Dec. 27, 2024
MCLE NO.VII-0027570 Roll No. 27932
101 Urban Ave. Campos Rueda Bldg
Brgy. Pio Del Pilar, Makati City



RF INSURANCE
BROKERS, INC.

RF INSURANCE BROKERS INC.

**2025 AMLA Operating Manual:
Money Laundering and Terrorist Financing Prevention Program
(MTPP)**

TABLE OF CONTENTS

	Page no.
1. INTRODUCTION	5
1.1 Objectives of this Manual	5
1.2 Importance of Policies and Procedures	6
2. DEFINITION OF TERMS	6
3. DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM	12
3.1 Definition of Money Laundering	12
3.2 Stages of Money Laundering	13
4. BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING	14
4.1 Money Laundering and Terrorist Prevention Program	14
4.1.1 Detailed Procedures for AMLA compliance	14
1. Customer Identification Process	14
2. Record Keeping and Retention	14
3. Covered Transaction Reporting	14
4. Suspicious Transaction Reporting	14
5. Continuous AML/CFT Training Program	15
6. Screening and Recruitment Process	15
7. Internal Audit System	15
8. Independent Audit Program	15
9. Mechanism for correction	15
10. Cooperation with the AMLC	15
11. Designation of AML Compliance Officer	15
4.1.2 Policies and Procedures to control ML/TF Risks	15
5. CUSTOMER IDENTIFICATION	16
5.1 General Requirements	
5.1.1 Written Client Identification and Acceptance Policies	16
5.1.2 Continuing Due Diligence / KYC Measures	16
5.1.3 Customer Information and Identification Documents	17
5.1.4 Required Identity and Source of Income /Assets Determination	18
5.1.5 Additional or Further Verification Measures	20
5.1.6 Updating Client Information	21
5.1.7 Unusual Transactions	21
5.1.8 Acquisition of the Business of another Covered Institution...	21
5.1.9 If the True Identity of Customer cannot be established	21
5.1.10 Conduct of Face-to-Face Contact	21
5.1.11 Presentation of Original Identification Documents	22
5.1.12 Use of New or Developing Technologies.....	22
5.1.13 Third Party Reliance	22
5.1.14 Outsourcing the Conduct of Customer Identification	23
5.1.15 Prohibited Accounts	23
5.2 Risk Assessment/Risk Profiling of Customers	23
5.2.1 Standards and Procedures for Due Diligence	23
5.2.2 Reduced Due Diligence	25
5.2.3 Enhanced Due Diligence	26
5.2.4 Minimum Validation Procedures for EDD	27

5.2.5	Failure to Conduct/Complete EDD and Tipping Off	28
5.3	High Risk Customers	28
5.4	Politically Exposed Persons	29
5.5	Single Proprietorship, Corporations, Partnerships and Indirect Prospects	30
5.6	Shell Companies	32
5.7	Trust, Nominee and Fiduciary Accounts	33
5.8	Transactions Undertaken on Behalf of Account Holders or Non-Account Holders	33
5.9	Bearer Shares	33
5.10	Wire Transfers	34
6.	RECORD KEEPING	36
6.1	General Requirements for Record Keeping	36
6.2	Periods of Retention	37
6.3	Records Relating to Pending Case	38
6.4	Forms of Records	38
6.5	Digitization of Customer Records	38
6.6	Persons Responsible for Safekeeping of Records	38
7.	MONITORING AND REPORTING OF COVERED AND SUSPICIOUS TRANSACTIONS	38
7.1	Reporting System	38
7.2	Registration with AMLC	38
7.3	Covered Transaction Report (CTR)	38
7.4	Suspicious Transaction Reporting (STR)	38
7.5	Transaction Reporting	39
7.6	Transactions that are both Covered and Suspicious	39
7.7	Attempted Suspicious Transactions	39
7.8	Reporting of Customer's Unlawful Activities	40
7.9	Register of Suspicious and Covered Transactions	40
7.10	Confidentiality of CTR and STR	40
7.11	Safe Harbor Provision	41
7.12	Procedure for Reporting	41
7.13	Terminating Client Relationship	42
8.	COMPLIANCE	42
8.1	The Compliance Officer – Qualifications and Responsibilities	42
8.2	Adviser Regarding AML matter	43
8.3	Responsibility of Rampover Insure and its Board	43
9.	INTERNAL CONTROL AND PROCEDURES	44
9.1	General Requirements	44
9.2	Coverage of Internal Control Policies and Procedures	44
9.3	Written Internal Reporting Procedures	44
10.	INTERNAL AUDIT	45
10.1	Internal Audit Function and Reporting Line	45
10.2	Frequency and Scope of Internal Audit	45
10.3	Electronic AML/CFT Monitoring System	45
10.4	Reporting of Internal Audit Findings	45
10.5	Outsourcing of Internal Audit Functions/External Audit	45
11.	TRAINING	45
11.1	Education and Continuing Training	45
11.2	Outsourcing of Training Functions/External Training Providers	46
11.3	Recommended Training Programs	46

11.4	Regular Refresher Training	47
11.5	Training Program and Records of Trainings Conducted	47
11.6	Cascading of Updates and New Requirements	47
12.	Exhibit A – High Risk Businesses	48
13.	Exhibit B – Forms used by Rampver Insure	49

1. INTRODUCTION

RF Insurance Brokers Inc. (Rampver Insure or RFIBI or “Corporation”) is duly registered with the Securities and Exchange Commission (SEC). The primary purpose of the Corporation is to act as an insurance broker or representative for and in behalf of an insured other than himself and/or act in any manner in negotiating contracts of insurance or placing risk or affecting reinsurance for any insurance company, to sell medical, health maintenance and related services, pre-need products, as well as any and all types of securities (without acting as stock broker), extended warranties, and other similar products and services; to offer, market and/or sell any products or service which insurance companies may from time to time be authorized to offer, market and/or sell; to render risk management consulting and training services in relation to the marketing and selling of the aforementioned products and services; and generally to do and perform all acts or things which are necessary, proper and/or incidental to the purposes herein stated.

Rampver Insure is committed to preventing the misuse of its personnel and/or facilities by persons (including clients, prospective shareholders, counterparties and service providers) who seek to engage in money laundering. Rampver Insure hereby adopts these policies and procedures to prevent, detect and provide for the reporting of money laundering activities pursuant to Republic Act No. 9160, as amended by Republic Act No. 9194 (also known as “The Anti-Money Laundering Act of 2001”, An Act Defining the Crime of Money Laundering Providing Penalties therefore and for Other Purposes) and the Securities and Exchange Commission Anti-Money Laundering Operating Manual for Covered Institutions, and other pertinent laws, rules and regulations administered by the SEC taking into consideration the international best practices in the implementation and enforcement of the Anti-Money Laundering (AML) and the Combating the Financing of Terrorism (CFT) regimes. Rampver Insure is one of the Covered Institutions that is mandated to comply with the SEC Memorandum Circular No. 16, Series of 2018: “2018 Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for SEC Covered Institutions” by submitting an updated MLPP Manual, which shall be updated at least once every two (2) years or as necessary.

It is expected that Rampver Insure, its directors, officers, distributors, shareholders and employees will implement and strictly adhere to these policies and procedures as well as all laws and regulations pertaining to anti-money laundering. It is critical that each employee of Rampver Insure be knowledgeable of the procedures intended to ensure compliance with anti-money laundering laws and regulations such as detection, investigation and reporting of covered and suspicious transactions. In implementing these policies and procedures, the Funds may rely on the company’s personnel and resources.

1.1 Objectives of this Manual

- (1) To ensure that Rampver Insure is in compliance with Republic Act 9160, as amended by Republic Act No. 9194 (also known as “The Anti-Money Laundering Act of 2001”), the Securities and Exchange Commission Anti-Money Laundering Operating Manual for Covered Institutions and other anti-money laundering laws and regulations. This Amended AMLA

Manual is in compliance with the SEC 2018 Guidelines for AML/CFT (per SEC MC No. 16, Series of 2018.)

- (2) To protect Rampver Insure from tarnishing its good name and reputation and prevent the use of Rampver Insure as a vehicle for money laundering or other illegal activities.
- (3) To enable personnel to recognize suspicious or illegal activity before or during its occurrence and report such activity to the proper authorities.

1.2 Importance of Policies and Procedures

Rampver Insure must conduct business according to high ethical standards and in accordance with applicable regulations. It will be a violation of these policies and procedures and, potentially, applicable regulations if an employee knowingly provides assistance to persons who attempt to violate or circumvent anti-money laundering regulations. For this purpose, “knowledge” includes the concepts of “willful blindness” and “conscious avoidance of knowledge.” Thus, employees whose suspicions are aroused, but who then deliberately fail to make further inquiries, wishing to remain ignorant, may be considered under the policy to have the “knowledge” required for disciplinary action. Violations of money laundering regulations may subject employee(s) to a penalty of imprisonment and a fine under Republic Act 9160, as amended by Republic Act No. 9194, and the company to fines, customer dissatisfaction and a tarnished reputation.

2. DEFINITION OF TERMS

Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the Anti-Money Laundering Act, as amended.

Agent shall refer to SEC licensed mutual fund distributor (MFD) and Certified Investment Solicitor (CIS) authorized to sell mutual fund shares and units.

AML shall mean anti-money laundering.

AMLA or the “Act” refers to Republic Act No. 9160 known as the Anti-Money Laundering Act of 2001 and amendments thereto.

AMLC refers to Anti-Money Laundering Council, the Philippines’ central AML/CFT authority and financial intelligence unit, which is the government instrumentality mandated to implement the AMLA and Terrorist Financing Prevention and Suppression Act (TFPSA). It also refers to the official name of the Council, which is the governing body of the said government agency.

Bangko Sentral ng Pilipinas (“BSP”) is the central bank of the Republic of the Philippines. The BSP provides policy directions in the areas of money, banking, and credit. It supervises operations of banks and exercises regulatory powers over non-bank financial institutions with quasi-banking and/or trust functions.

Beneficial Owner refers to any natural person who (1) Ultimately owns or controls the customer and/or on whose behalf a transactions or activity is being conducted; or **(2)** Has ultimate effective control over customer that is a legal person or arrangement.

Legal Arrangements shall refer to express trusts or other similar legal arrangements.

Ultimate effective control refers to any situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control. This may be achieved through, but not limited to, any of the following situations:

- a) direct or indirect ownership of at least 25% of any category of voting shares or capital of a legal person, arrangement, understanding, relationship or otherwise has or shares voting power, which includes the power to vote, or to direct the voting of such security; and/or investment returns or power, which includes the power to dispose of, or to direct, the disposition of such security; *Provided*, that a person shall be deemed to have an indirect beneficial ownership interest in any security which is:
 - (i) held by members of his/her immediate family sharing the same household;
 - (ii) held by a partnership in which he/she is a general partner;
 - (iii) held by a corporation of which he/she is the controlling shareholder; or
 - (iv) subject to any contract, arrangement or understanding which gives him/her voting power or investment power with respect to such securities: *Provided, however*, that a person shall not be deemed to be a beneficial owner of securities held by him/her for the benefit of third parties or incustomer or fiduciary accounts in the ordinary course of business, so long as such shares were acquired by such person without the purpose or effect of changing or influencing control of the issuer.
- b) the ability to elect a majority of the board of directors, or any similar body, of a legal person or arrangement; or
- c) any situation in which:
 - (i) a person has the ability in fact to exert a dominant influence over the management or policies of a legal person or arrangement; or
 - (ii) a majority of the members of the board of directors of a such legal person or arrangement, or any equivalent body, are accustomed or under an obligation, whether formal or informal, to act in accordance with a given person's

directions, instructions or wishes in conducting the affairs of the legal person or arrangement.

In exceptional cases where no natural person is identifiable who ultimately owns or exerts control over the legal entity, Rampver Insure, having exhausted all other means of identification, and provided there are no grounds for suspicion, may consider the senior managing official/s to be the beneficial owner/s.

All securities of the same class beneficially owned by a person, regardless of the form such beneficial ownership takes, shall be aggregated in calculating the number of shares beneficially owned by such person.

A person shall be deemed to be the beneficial owner of a security if that person has the right to acquire beneficial ownership within thirty (30) days, including, but not limited to, any right to acquire, through the exercise of any option, warrant or right; through the conversion of any security; pursuant to the power to revoke a trust, discretionary account or similar arrangement; or pursuant to automatic termination of a trust, discretionary account or similar arrangement.

Beneficial Ownership Information refers to the identification documents and information of the beneficial owner of a customer

Beneficial Ownership Verification ("BOV") is the process of taking reasonable measures to identify and verify the beneficial owner, including the determination of the true nature of the beneficial owner's capacities and duties vis-à-vis his agent, nominee or trustee.

Beneficiary shall refer to any person for whose benefit a mutual fund account is created.

CFT means Countering Financing of Terrorism.

Client Due Diligence ("CDD") refers to the process of obtaining, verifying by reliable means, and recording the identity, representative capacity, domicile, legal capacity, occupation or business purpose of any natural or legal person, as well as other identifying information through the use of legal or private documents establishing or conducting business relations.

Covered Transaction is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (Php 500,000) within one (1) business day.

Covered Transaction Report ("CTR") refers to a report on a covered transaction, as defined herein, filed by ATRAM before the AMLC.

Customer or Client shall refer to any person or entity that keeps an account, or otherwise transacts business with a covered person. It includes the following: (1) any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions; (2) beneficiary of a trust, an investment fund or a pension fund; (3) a company or person whose assets are managed by an asset manager;

(4) a grantor of a trust; and (5) any insurance policy holder, whether actual or prospective.

Customer Due Diligence (“CDD”) refers to the procedure of identifying and verifying the true identity, of customers, and their agents and beneficial owners, including understanding and monitoring of their transactions and activities.

Reduced Due Diligence/Simplified Due Diligence (RDD/SDD) refers to the lowest level of customer due diligence.

Enhanced Due Diligence (EDD) refers to the enhanced level of scrutiny intended to provide a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate risks presented.

Customer Identification Process (“CIP”) refers to the process of determining the identity of the customer vis-à-vis the valid and acceptable identification document submitted to, and/or presented to a covered institution.

Customer Verification Process (“CVP”) refers to the process of validating the truthfulness of the information, and confirming the authenticity of the identification documents, presented, submitted and provided by the customer; or other ways of verifying the identity and assessing the risk profile of customers, and their agents and beneficial owners, through the use of reliable and independent sources, documents, data or information.

Demographic Data refers to a person’s full name, sex, date and place of birth, address, citizenship or nationality, and such other personal information from which the identity of a person can be ascertained.

Designated Persons refers to (a) any person or entity designated and/or identified as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations Security Council Resolution or by another jurisdiction or supranational jurisdiction; (b) any organization, association, or group of persons prescribed pursuant to the Human Security Act of 2007; or (c) any person, organization, association, or group of persons whose funds or property, based on probable cause are subject to seizure and sequestration under Section 39 of the Human Security Act of 2007.

Designated Non-Financial Businesses and Professions (“DNFBP”) refers to businesses and professions, which are not under the supervision or regulation of the BSP, SEC and IC, and designated as covered persons under the AMLA.

Freeze refers to the blocking or restraining of specific property or funds from being transacted, converted, concealed, moved or disposed without affecting the ownership thereof.

Freeze Order (“FO”) refers to a provisional remedy aimed at blocking or restraining monetary instruments or properties in a way related to an unlawful activity, as herein defined, from being transacted, withdrawn, deposited, transferred, removed, converted, concealed, or otherwise moved or disposed without affecting the ownership thereof.

Front-liner shall refer to the agent or person or employee who is the first contact of the clients. In Rampver Insure, front-liners are SEC licensed CIS employees who have direct interaction with the clients. They are also referred to as Sales or Marketing personnel or Agents.

Identification Information/Personal Information refers to the demographic data and biometric information of a natural person, or information about a juridical person or legal arrangement, from which the identity of a person is apparent or can be reasonably and directly ascertained by the person holding the information, or when put together with other information would directly and certainly identify a person.

Information and Communication Technology (ICT) refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present and disseminate information.

Institutional Risk Assessment refers to a comprehensive exercise to identify, assess and understand a covered person's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

Money Laundering/Terrorism Financing Prevention Program" (MLPP)" refers to a covered person's comprehensive, risk-based, and written internal policies, controls and procedures to implement the relevant laws, rules and regulations, and best practices to prevent and combat ML/TF and associated unlawful activities in the operational level.

Person/Entity refers to any natural or juridical person.

Politically Exposed Person ("PEP") refers to an individual who is or has been entrusted with the prominent public position in: (a) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (b) a foreign state, or (c) an international organization.

Proceeds refers to an amount derived or realized from any unlawful activity.

Relationship refers to business or professional relationship between the covered person and its customer.

Risk refers to risk of loss arising from ML/TF activities.

Risk-Based Approach ("RBA") refers to the process by which countries, competent authorities, and covered persons identify, assess, and understand the ML/TF risks to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. This includes prioritization and efficient allocation of resources by the relevant key players and stakeholders in applying AML/CFT measures in their operations in a way that ensures that they are commensurate with the risks involved.

Sectoral Risk Assessment refers to a comprehensive exercise to identify, assess and understand an industry's or business or professional sector's threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

Securities and Exchange Commission ("SEC") refers to the regulatory body that regulates the securities industry.

Shell Bank refers to a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. It can also be a bank that (a) does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorized to engage; (b) does not employ one or more individuals on a full-time basis at this fixed address; (c) does not maintain operating records at this address; and (d) is not subject to inspection by the authority that licensed it to conduct banking activities.

Shell Company refers to legal entities which have no business substance in their own right but through which financial transactions may be conducted.

Source of Fund refers to the origin of the funds or other monetary instrument that is the subject of the transaction or business or professional relationship between a covered person and its customer, such as cash on hand, safety deposit box with a covered person, and a particular bank or investment account.

Source of Wealth refers to the resource from which the customer's wealth, including all monetary instruments and properties, came, comes, or will come from, such as employment, business, investments, foreign remittance, inheritance and donation.

Supervising Authority ("SA") refers to the BSP, the SEC, the IC, or other government agencies designated by law to supervise or regulate a particular financial institution or DNFBP.

Suspicious Transaction refers to a transaction with a covered person, regardless of the amount involved that is, in any way, related to terrorism financing or terrorist acts. It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or group of persons.

Suspicious Transaction Report (STR) refers to a report on a suspicious transaction, as herein defined, filed by a covered person before the AMLC

Terrorist refers to any natural person who: (a) commits, or attempts, or conspires to commit terrorist acts by any means, directly or indirectly, unlawfully, and willfully; (b) participates, as a principal, or as an accomplice, in terrorist acts; (c) organizes or directs others to commit terrorist acts; or (d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

Terrorist Act refers to an act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

Terrorist Organization, Association or Group of Persons refers to any entity owned or controlled by any terrorist or group of terrorists that: (a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (b) participates as an accomplice in terrorist acts; (c) organizes or directs others to commit

terrorist acts; or (d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose of furthering the terrorist acts where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

Terrorist Financing (“TF”) refers to the financing of terrorist acts, and of the terrorists and terrorist organizations. Financing of terrorism is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial services or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (1) to carry out or facilitate the commission of any terrorist act; (2) by terrorist organization, association or group; or (3) by an individual terrorist.

Terrorism Financing Prevention and Suppression Act (“TFPSA”) refers to Republic Act No. 10168.

Transaction refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the covered person and its customer. It also includes any movement of funds, by any means, in the ordinary course of business of a covered person.

Unlawful activity refers to any act or omission or series or combination thereof involving or having direct relation to the activities as enumerated in the AMLA, as amended.

3. DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1. Definition of Money Laundering. - Money laundering is the processing of the proceeds of a crime to disguise their origin. It is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the AMLA, so that they appear to have originated from a legitimate source.

Money laundering is committed by:

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

- B. Any covered person who, knowing that a covered or suspicious transaction is required under the AMLA to be reported to the AMLC, fails to do so.

3.2. Stages of Money Laundering. - The process of money laundering generally comprises three (3) stages during which there may be numerous transactions that, could alert a covered institution to the money laundering activity:

- (1) *Placement* - the physical disposal of cash proceeds, derived from illegal activity.
- (2) *Layering* - separating the illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity or to obscure the source of the funds.
- (3) *Integration* - provides appearance of legitimacy to criminally- derived wealth. If the layering process has succeeded, the integration schemes place the laundered proceeds back into the economy in such way that they re-enter the financial system appearing to be normal business funds.

Because of the nature of the business relationships entered into and among clients and the covered institutions, which are no longer predominantly cash-based, they are less conducive to the initial placement of criminally derived funds other than financial industries such as banking. Most payments are made by way of checks from another financial institution; hence, it can be assumed that the first stage of money laundering has already been achieved. Nevertheless, the purchases by cash are not unknown and the risk of the business being used at the placement stage cannot be ignored. The businesses of these covered institutions are most likely to be used at the second stage of money laundering, i.e., the layering process, as they provide a potential avenue which may allow a dramatic alteration of the form of funds, from cash on hand to securities such as stock certificates, investment contracts, evidences of indebtedness, bearer and other negotiable instruments. Investment transactions incorporate an added attraction to the money launderer in that the alternative asset is normally highly liquid. The ability to liquidate investment portfolios containing both lawful and illicit proceeds, whilst concealing the criminal source of the latter, combined with the huge variety of investments available, and the ease of transfer between them, offers the sophisticated criminal launderer an ideal route to effective integration into the legitimate economy. Due diligence must, therefore, be exercised to prevent the use of these covered institutions as instruments for money laundering.

Financing of Terrorism, as defined under RA 10168, refers to a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part:

- (1) to carry out or facilitate the commission of any terrorist act;
- (2) by a terrorist organization, association or group; or
- (3) by an individual terrorist.

Financing of terrorism generally refers to the carrying out of transactions involving funds or property that may or may not be owned by terrorist, or which have been intended to be used or to assist the commission of terrorism. Terrorism financing is not necessarily

confined to funds derived from unlawful sources but may also involve funds, derived from legitimate sources or a combination of lawful and unlawful sources.

Due diligence must therefore be exercised to prevent the use of Rampver Insure as instrument for money laundering. To combat money laundering, AML laws prescribe covered persons to put in place internal policies on customer identification, reporting of covered and suspicious transactions, and record keeping and retention, among others.

4. BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

4.1 Money Laundering and Terrorist Prevention Program - Rampver Insure has adopted a comprehensive and risk-based Money Laundering and Terrorist Financing Prevention Program (MLPP) which is geared towards the promotion of high ethical and professional standards and the prevention of the covered institutions from being used, intentionally or unintentionally, for money laundering and terrorism financing.

The MLPP is consistent with the AMLA, as amended its RIRR and the provisions set forth in the SEC Guidelines and designed according to Rampver Insure's corporate structure and risk profile. In compliance with the regulations, the MLPP is in writing, and approved by the board of directors of Rampver Insure, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same.

The MLPP is readily available in user-friendly form, whether in hard or soft copy. Rampver Insure has put up a procedure to ensure an audit trail evidencing the dissemination process for new and amended policies and procedures.

Rampver Insure's anti-money laundering program embodies the following:

4.1.1 Detailed procedures of Rampver Insure's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, other applicable guidelines issued by the AMLC, to wit:

1. Customer identification process including acceptance policies and on-going monitoring process;
2. Record keeping and retention;
3. Covered transaction reporting; and
4. Suspicious Transactions (ST) reporting, including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregate amounts breach the threshold. The ST reporting shall include a reporting chain under which a ST will be processed and the designation of a board-level or approved committee who will ultimately decide whether or not Rampver Insure should file a report to the AMLC. Since the resources of Rampver Insure do not permit the designation of a committee, it has designated a Compliance Officer to perform this

function instead, provided that the board of directors has approved this decision in writing.

5. An effective and continuous AML/CFT training program for all directors and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under the SEC AMLA Guideline, the AMLA, as amended, its RIRR and Rampver Insure's internal policies and procedures as embodied in the MLPP. The training program also includes refresher trainings to remind these individuals of their obligations and responsibilities as well as update them of any changes in the MAL/CFT laws, rules, and internal policies and procedures.
6. An adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s or adverse circumstances in their background that would entail a risk of involvement in money laundering or terrorist financing are employed to assume sensitive functions within the covered institution'
7. An internal audit system in accordance with AML/CFT Guidelines;
8. An independent audit program with written scope of audit that will ensure the completeness and accuracy of the information and identification documents obtained from clients, the covered and suspicious transactions reports submitted to the AMLC, and the records retained in compliance with the SEC 2018 AML/CFT Guidelines as well as adequacy and effectiveness of the training program on the prevention of money laundering and terrorism financing;
9. A mechanism that ensures all deficiencies noted during the audit and/or SEC regular or special examination or other applicable regulator's examination are immediately corrected and acted upon;
10. Cooperation with the AMLC;
11. Designation of an AML Compliance Officer, who shall have at least a rank of senior vice president or equivalent position with adequate stature and authority in the corporation as the lead implementor of the program within an adequately staffed compliance office. The AML compliance officer should not be a member of the Board of Directors and should annually attend AML trainings. The AML Compliance Officer may also be the liaison between Rampver Insure, the SEC and the AMLC in matters relating to Rampver Insure's AML/CFT compliance. Since the resources of Rampver Insure do not permit the hiring of an AML Compliance Officer, the board of directors may provide that the Compliance Officer shall also assume the responsibility of the former.

4.1.2 Policies and control procedures and monitoring mechanism for prevention or migration of ML/TF risks. These General Policies are stated below:

1. No director, officer, distributor, shareholder or employee of Rampver Insure shall knowingly participate, engage in, or assist any other person or entity in engaging in any activity believed to be money laundering or any other suspicious or illegal activity.
2. No director, officer, distributor, shareholder or employee of Rampver Insure shall assist any client or prospect in tailoring financial transactions in order to circumvent laws and regulations contained under Republic Act 9160, as amended by Republic Act No. 9194.
3. No director, officer, distributor, shareholder or employee of Rampver Insure shall consciously decide to avoid uncovering the truth about any prospect's suspected illegal transactions or activities.
4. Any director, officer, distributor, shareholder or employee of Rampver Insure who fails to comply with the foregoing policies may be subject to penalties under Republic Act 9160, as amended by Republic Act No. 9194, as well as other penalties imposed by Rampver Insure.
5. Rampver Insure will, consistent with applicable laws and regulations cooperate fully with the concerned authorities in the enforcement of anti-money laundering laws and regulations in connection with transactions involving it.

5. CUSTOMER IDENTIFICATION

5.1 General Requirements

5.1.1 Written Client Identification and Acceptance Policies and Procedures. – Rampver Insure has developed clear written client identification and graduated acceptance policies and procedures including a set of criteria for customers that are likely to pose low, normal or high risk to its operations. Such policies and procedures have been designed to ensure that the financially or socially disadvantaged are not denied access to financial services, while at the same time prevent suspicious individuals or entities from opening an account or establishing a relationship.

The policies and procedures include procedures for providing customers with adequate notice that Rampver Insure is requesting information to verify their identities

5.1.2. Continuing Due Diligence / KYC Measures. – To prevent money laundering, it is important that the employees of Rampver Insure know the true identity of individuals and institutions who are, or seek to become shareholders of any of the Funds that the company distributes.

It is the responsibility of the Sales and Business Development people (“Frontline Employees”) to make the required KYC¹ determinations and to obtain sufficiently reliable information to support these determinations.

"Know your Customer (KYC)" measures of Rampver Insure includes conducting continuing due diligence on the business relationship to ensure that the transactions being conducted are consistent with Rampver Insure's knowledge of the customer and/or beneficial owner, their business profile, including, where necessary, the source of its funds.

5.1.3. Customer Information and Identification Documents. – Rampver Insure has established and maintains a system of verifying the true identify of its customers based on reliable, independent source documents, data and information. This system likewise include the procedures for verifying the legal existence and organizational structure of corporate clients, as well as the identification and authority of persons who act on their behalf. Rampver Insure complies with regulatory requirements such as the AMLA, RIRR and other AMLC issuances, and other relevant statutory regulations, for the purpose of verifying and recording the true and full identity of its customers.

Rampver Insure must obtain and record competent evidence of the true and full identity, representative capacity, domicile, legal capacity, occupation or business purposes of clients, as well as other identifying information on those clients, whether they be occasional or usual, through the use of documents such as, but not limited to:

- (1) Identity documents, such as passports, birth certificates, driver's licenses, and other similar identity documents, which are verifiable from the institution issuing the same.

The identifying documents should provide evidence of complete name or names used, residential address, date of birth, nationality, office address and contact details. They should include at least one (1) identifying document bearing the photograph and signature of the client. The identifying documents which are considered most reliable are official identity cards and passports. While identification documents that are easily obtained in any name e.g. medical cards, credit cards and student identification cards, may be used, they should not be accepted as the sole means of identification.

Clients engaging in transactions with Rampver Insure shall present one (1) original official identity card with photo and signature. For this purpose, the term "official identity card" shall refer to those issued by any of the following: the National Government of the Republic of the Philippines, its political subdivisions or instrumentalities, or government owned and controlled corporations.

Passports issued by foreign governments shall be considered as prima facie identification documents of persons engaging in transactions with Rampver Insure.

- (2) Incorporation and partnership papers, for corporate and partnership accounts. These documents should be certified as true copies from the issuing government agency.

¹ These KYC procedures and policies are for anti-money laundering policies only. KYC policies for other purposes (e.g. ensuring that investment management services are appropriate given a client's personal financial situation and objectives) may, in any one or more circumstances, require additional KYC steps to be taken by the Rampver Insure personnel.

- (3) Special authorizations for representatives, which must be duly notarized.

5.1.4 Required Identity and Source of Income/Assets Determinations

Before any funds can be accepted from a prospective customer, a Frontline Employee must determine the identity of the prospect (including the identity, authority and relationship to the prospect of any person who will be acting on its behalf)².

Under no circumstances can an investment be made under an anonymous or fictitious name.

Individual Prospects:

Whenever possible, individual prospects should be interviewed personally.³ The following information shall be obtained:

- (1) complete name and names used;
 - (2) present address;
 - (3) permanent address;
 - (4) mailing address;
 - (5) date and place of birth;
 - (6) nationality;
 - (7) contact details (avoid prepaid cellular phone numbers)
 - (8) nature of work, name of employer or nature of self-employment or business;
 - (9) Tax Identification Number (TIN), Social Security System (SSS) number or Government Service System (GSIS), and Insurance System number;
 - (10) Specimen signature or biometrics of the customer;;
 - (11) Sources of funds, when necessary
 - (12) Names of beneficial owner or beneficiaries, if applicable;
 - (13) Complete name, address and contact information of beneficial owner, if applicable
- (Based on SEC Memorandum Circular 2, Series of 2010).

Customers who engage in a transaction with Rampver Insure for the first time shall be required to present the original and submit a clear copy of at least one (1) official identification document.

Where the customer or authorized representative is a foreign national, Rampver Insure shall require said foreign national to present passport or Alien Certificate of Registration issued by the Bureau of Immigration.

² Rampver Insure may not permit a client to establish a “special name account” (i.e. an account using a pseudonym or number rather than the client’s actual name) unless its property developer maintains records containing the actual name and other identifying information regarding the beneficial owner of the account. For corporate accts., the use of trade or business names is allowable provided that the client submits a duly approved Business name from the Securities and Exchange Commission, and the name and signature of the client must appear on the agreement between Rampver Insure and the client.

³ Sec. 4.B.3(a) of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

Identity documents, such as but not limited to, passports, birth certificates, driver's licenses, employment identification cards, and other similar identity documents, which are verifiable from the institution issuing the same shall be used for this purpose. At least one of the documents must be pre-signed and bear a photograph of the prospect.

"The identifying documents, which are considered most reliable are official identity cards and passports. While identification documents that are easily obtained in any name, e.g., medical cards, credit cards and student identification cards may be used, they should not be accepted as the sole means of identification."⁴ For verification purposes, photocopies of identification or other documents are inadequate. Prospects must be requested to present original documents for comparison with the photocopies of identification cards.

Accounts opened without face-to-face contact, such as via the Internet, post or telephone or other such instances, should be dealt with in a stringent and careful manner and such prospects must be informed that identity verification procedures apply to them as well.

The following are a number of checks, which can be used to verify the identity of prospects where there is no face-to-face contact:

- Barangay certification;
- telephone contact with the applicant at an independently verified home or business number;
- subject to the applicant's consent, telephone confirmation of the prospect's employment with the employer's personnel department at a listed business number;
- income or salary details appearing on recent bank statements, income tax returns or any other document evidencing compensation;
- confirmation of the address through an exchange of correspondence or by other appropriate methods;
- an initial deposit check drawn on another financial institution regulated by the Bangko Sentral ng Pilipinas will provide additional assurance as to identity. (Based on SEC Memorandum Circular 2, Series of 2010).

Corporate/Institutional Prospects:

Before establishing a business relationship with corporate/institutional prospects, a company search and/or other commercial inquiries shall be made, to ensure that the corporate/institutional prospects customer has not been or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company/institution or its directors, or the business or its partners, a search or inquiry with the Securities and Exchange Commission or other relevant agency shall be made.⁵

The following relevant customer information and identification documents shall be obtained in respect of corporate/institutional prospects, which are regulated in the Philippines:

- Name of entity.
- Name of authorized signatory.
- Official address
- Contact number or information,

⁴ Sec. 4.A.1a of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

⁵ Sec.4.C.1of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

- Information about the nature of the business of the client, copies of identification documents of shareholders, directors, officers and all authorized signatories.⁶
- Specimen signatures or biometrics of the authorized signatory
- Copies of the Certificate of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation issued by the Securities and Exchange Commission (SEC) for corporations and partnerships.
- Secondary License or Certificate of Authority issued by the Supervising Authority or other government agency, if applicable.
- Articles of Incorporation or Certificate of Partnership, as appropriate, copies of the By-Laws
- Latest General Information Sheet, which lists the names of directors/partners and principal stockholders, and secondary licenses.
- Corporate/Partner's Secretary Certificate citing the pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity.
- Written confirmation or statement as to existence or non-existence of beneficial owners, and name of beneficial owner, if applicable.
- Appropriate directors' resolutions and signed application forms or account opening authority containing specimen signatures.

The originals or certified copies of any or all of the foregoing documents should be produced for verification.

For corporations, institutions, businesses or partnerships registered outside the Philippines, comparable documents are to be obtained, duly authenticated by the Philippine Consulate where said companies are located.

In the event that the corporation, institution, business or partnership subsequently undergoes significant changes in the company and ownership structure, the appropriate steps must be taken to verify the identity of the new owners.

Prospects Acting through a Trustee, Nominee or Agent:

When the prospect is acting through on behalf of another person as trustee, nominee or agent, evidence must be obtained of the true and full identity of both the beneficial owner and such agents and authorized signatories and the nature of their representative capacity and duties.

Where the account is opened by a firm of lawyers or accountants, Rampver Insure should make reasonable inquiries about transactions passing through the subject accounts that give cause for concern, or from reporting those transactions if any suspicion is aroused. (Based on SEC Memorandum Circular 2, Series of 2010).

5.1.5. Additional or Further Verification Measures. - Clients shall be made aware of Rampver Insure explicit policy that business transactions will not be conducted with applicants who fail to provide competent evidence of their identity, but without derogating from Rampver Insure's obligation to report suspicious transactions. Where initial verification fails to identify the applicant, or gives rise to suspicion/s that the information provided is false, additional verification measures shall be undertaken to determine whether to proceed with

⁶ Sec.4.C.2 of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

the business and/or make a suspicious transaction report if circumstances under Section 3(b-1) of the AMLA, as amended, would apply. Details of the additional verification are to be recorded in writing and be made available for inspection by the Commission or appropriate authorities.

Rampver Insure shall take further measures to verify the identity of the customer or the beneficial owner, as applicable, if during the business relationship, it has reason to doubt:

- (1) The accuracy of the information relating to the customer's identity;
- (2) That the customer is the beneficial owner; or
- (3) The customer's declaration of beneficial ownership.

5.1.6. Updating Client Information. - Rampver Insure shall ensure that they know their customers well, and accordingly, shall keep current and accurate all material information with respect to their customers by regularly conducting verification and an update thereof.

5.1.7. Unusual Transactions. - Rampver Insure shall pay special attention to all unusually large transactions or unusual patterns of transactions. This requirement applies both to the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities.

5.1.8. Acquisition of the Business of Another Covered Institution. - In case that Rampver Insure acquires the business of another covered institution, either in whole or as a product portfolio, it is not necessary for the identity of all existing customers to be re-identified, provided that:

- (1) All customer account records are acquired with the business; and
- (2) Due diligence inquiries do not raise any doubt as to whether the anti-money laundering procedures previously adopted by the acquired business have satisfied Philippine requirements.

5.1.9. If the True identity of Customer cannot be established. - Rampver Insure's policies and procedures include procedures for responding to circumstances in which Rampver Insure cannot form a reasonable belief that it knows the true identity of a customer or when Rampver Insure is unable to comply with Section 5.a.3 hereof. These procedures shall include, among others, the following:

- (1) When the covered institution should not open the account or commence business relations or perform the transaction;
- (2) The terms under which a customer may conduct transactions while the covered institution attempts to verify the customer's identity;
- (3) When the covered institution should close an account or terminate business relationship after attempts to verify customer's identity fail; and
- (4) Should consider filing a Suspicious Transaction Report with the AMLC.

5.1.10. Conduct of Face-to-Face Contact. - Frontline Employees of Rampver Insure conduct face-to-face contact on the commencement of the relationship, as reasonably practicable. The use of Information and Communication Technology in the conduct of face-to-face contact is allowed, provided that the Frontline Employee has verified the

identification documents submitted by the prospective customer and the entire procedure is documented.

5.1.11. Presentation of Original Identification Documents. – Rampver Insure shall request individual clients who present only photocopies of identification card and other documents to produce the original documents thereof for verification purposes.

5.1.12. Use of New or Developing Technologies. - Rampver Insure must pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

5.1.13. Third Party Reliance. - Rampver Insure may rely on a third party to perform customer identification, including face-to-face contact. The third party shall be:

- (1) A covered person; or
- (2) A financial institution or DNFB0 operating outside the Philippines that is covered by equivalent customer identification and face-to-face requirements. The intermediary or third party relied upon are considered as covered institution as defined under the AMLA Guidelines or any other guidelines or rules issued by the pertinent government agencies/institutions, or as defined and identified by foreign jurisdictions in so far as covered institutions in their respective jurisdictions are concerned.

The ultimate responsibility, however, for identifying the customer, remains with Rampver Insure who is relying on the third party. In case of high risk customers, Rampver Insure conducts enhanced due diligence procedures.

It is understood that the Commission reserves the right to disapprove arrangements of Rampver Insure with intermediaries or third parties when it has been proven to have been abused by Rampver Insure.

Where such reliance is permitted, the following criteria should be met:

- (1) Rampver Insure, relying on the intermediary or third party, should immediately take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the intermediaries and third parties upon request without delay. Rampver Insure should be satisfied with the quality of the due diligence undertaken by the intermediaries and third parties.
- (2) Rampver Insure should satisfy itself that the intermediaries and third parties are regulated and supervised, and have measures in place to comply with customer due diligence requirements.
- (3) The customer identification program of the third party intermediary is similar to or is equivalent to the customer identification program of Rampver Insure.
- (4) Ultimate responsibility for customer and/or beneficial owner identification

and verification remains with Rampver Insure relying on intermediaries or third parties.

In cases of high risk customers, Rampver Insure relying on the third person shall also conduct enhanced due diligence procedures.

5.1.14. Outsourcing the Conduct of Customer Identification. - Rampver Insure may outsource the conduct of customer identification, including face-to-face contact, to a counter-party, intermediary or agent. The outsource, counter-party or intermediary shall be regarded as agent of Rampver Insure - that is, the processes and documentation are those of Rampver Insure itself. The ultimate responsibility for identifying the customer and keeping the identification documents remains with the Rampver Insure.

In case that Rampver Insure shall outsource the conduct of customer identification, including face-to-face contact, it shall ensure that the employees or representatives of the counter-party, intermediary or agent undergo equivalent training program as that of Rampver Insure's own employees undertaking similar activity.

5.1.15. Prohibited Accounts. - Rampver Insure shall maintain customer accounts only in the name of the account holder. They shall not open or keep anonymous accounts, fictitious name accounts, incorrect name accounts, and similar accounts.

5.2 Risk-Assessment/Risk-Profiling of Customers

5.2.1. Standards and Procedures for Due Diligence - Rampver Insure has set the standards in applying reduced, normal and enhanced customer due diligence, which set the conditions for the denial of account opening of the customers. The customer due diligence to be applied depends on the following:

- (1) Reduced Diligence – where lower risks of money laundering and terrorist financing have been identified.
- (2) Enhanced Diligence – when the risks of money laundering are higher. Rampver Insure shall examine the background and purpose of the transactions, which appear to be suspicious and have no apparent economic or lawful purpose

Frontline Employees of Rampver Insure must assess the money laundering risks presented by each prospect and determine the corresponding level of supporting information that is required, depending on the applicable customer due diligence. Factors for Frontline Employees to consider and verify in making such risk assessments include:

- (1) The source(s) of the funds to be invested. If the source(s) of funds arise from or are in any way related to an unlawful activity, a Suspicious Transaction Report must be filed in accordance with the reportorial requirements set forth below.
- (2) The prospect's reputation and standing in the community (e.g., is the prospect a reputable, established business or business person?).

- (3) The nature of the prospect's business, including nature of customers, business partners and transactions and level of regulation to which the business is subject, (e.g., is the prospect's business well understood? Is it a "high risk Business" listed on Exhibit A).
- (4) The identity and reputation of the institutional prospect's chief executive officer and chief financial officer (or equivalent officers) and the identity, business reputation of any owner of a majority of the firm's outstanding equity or of any other third party known to control the institutional prospect (collectively, "controlling persons") which is not publicly listed.
- (5) Whether the individual prospect or the "Controlling Persons" (as defined above) of the institutional or any person acting on the prospect's behalf is a "public figure" or "related individual".⁷
- (6) Appropriate diligence must be performed to determine if Rampver Insure or any of its investment company principals has had an adverse business experience with or has previously declined the said prospect which would warrant that business with the said prospect be declined.

To help assure that due consideration is given to the money laundering risks presented by a prospect and that required determinations are made, the Frontline Employee must require each prospect to fill out a Client Information Sheet as prescribed by its investment company principals. A manager having supervisory responsibility over the particular Frontline Employee must review and, if necessary, discuss the completed Client Information Sheet/s with the Frontline Employee before an investment can be booked for the prospect. The identity of existing clients or beneficial shareholders should be renewed/updated at least every other year.

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

Enhanced due diligence shall be applied to customers that are assessed by Rampver Insure or under the SEC AMLA Guidelines as high risk for ML/TF.

For customers assessed to be of low risk such as small account balances and transactions, Rampver Insure shall apply reduced due diligence. Some entities may likewise be considered as low risk clients, e.g., banking institutions, trust entities and Qualified Buyers (QBs) authorized by the BSP to operate as such and publicly listed companies subject to regulatory disclosure requirements.

In designing a customer acceptance and risk profiling policy, the following criteria relating to the product or service, the customer, and geographical location, at a minimum, have been taken into account by Rampver Insure:

- (1) The nature of the service or product to be availed of by the customers;
- (2) The purpose of the account or transaction;

⁷

- (3) The amount of the funds to be deposited by the customer or the size of the transactions undertaken;
- (4) Source of funds/nature of business activities;
- (5) The regularity or duration of the transaction;
- (6) The fact that the customer came from a high risk jurisdiction,
- (7) The existence of suspicious transaction indicators
- (8) Public or high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;
- (9) Country of origin and residence of operations or the fact that a customer came from a high risk jurisdiction;
- (10) The existence of ST indicators;
- (11) Watch list of individuals and entities engaged in illegal activities or terrorist-related activities as circularized by the BSP, SEC, AMLC, and other international entities or organizations, such as the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List; and
- (12) Such other factors, e.g., the amount of the funds involved or the size of the transaction undertaken by a customer or the size of transactions, and regularity or duration of the transaction, as the covered institution may deem reasonable or necessary to consider in assessing the risk of a customer to ML/TF.

In assessing the risk profile of customers which are juridical entities, Rampver Insure must also consider the financial profile and other relevant information of the active authorized signatories.

Rampver Insure shall document the risk profiling results as well as how a specific customer was profiled and what standard of CDD (reduced, average or enhanced) was applied. Further, it shall regularly update its risk-assessment/risk-profiling of its clients.

Money Laundering Sensitivity Level

Frontline Employees must assess the money laundering risks presented by each prospect. The Compliance Officer must be consulted before Rampver Insure can open accounts for high-risk clients.

5.2.2. Reduced Due Diligence. - In general, the full range of customer due diligence measures should be applied. However, if the risk of money laundering or the financing of terrorism is lower based on Rampver Insure's assessment, and if information on the identity of the customer and the beneficial owner is publicly available, or adequate checks and controls exist elsewhere in national systems, it could be reasonable for Rampver Insure to apply simplified or reduced customer due diligence measures when identifying and verifying the identity of the customer, the beneficial owner and other parties to the business relationship. Examples of customers where simplified or reduced customer due diligence measures could apply are:

- (1) Financial institutions where they are subject to requirements to combat money laundering and the financing of terrorism consistent with the Financial Action Task Force (FATF) Recommendations and are supervised for compliance with those controls.
- (2) Public companies that are subject to regulatory disclosure requirements.
- (3) Government institutions and its instrumentalities.

Reduced due diligence shall not be applied if there is suspicion of ML/TF.

5.2.3. Enhanced Due Diligence (EDD). - Rampver Insure shall examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions and/or unusual patterns of transactions which, have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Where the risks of ML/TF are higher, covered persons are required to conduct enhanced CDD measures consistent with the risks identified.

Whenever EOD is applied as required by the AMLA guidelines, or by Rampver Insure's customer acceptance policy, or where the risk of ML/TF are higher, the covered institution shall do all of the following, in addition to profiling of customers and monitoring of their transactions:

- (1) Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of normal due diligence.
 - (a) In case of individual customers-
 - (i) Supporting information on the intended nature of the business relationship/source of funds/source of wealth (such as financial profile, ITR, etc.);
 - (ii) reasons for intended or performed transactions;
 - (iii) list of companies where he/she is a stockholder, beneficial owner, director, officer, or authorized signatory;
 - (iv) other relevant information available through public databases or internet; and
 - (v) a list of banks where the individual has maintained or is maintaining an account.
 - (b) In case of entities -
 - (i) prior or existing bank references;
 - (ii) the name, present address, nationality, date of birth, nature of

work, contact number and source of funds of each of the primary officers (e.g., President, Treasurer);

- (iii) volume of assets, other information available through public databases or internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial Statements, etc.); and

- (iv) reasons for intended or performed transactions.

- (2) Conduct validation procedures on any or all of the information provided;
- (3) Secure senior management approval to commence or continue business relationship/transacting with the customer;
- (4) Conduct enhanced ongoing monitoring of the business relationship, by, among others, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- (5) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and
- (6) Perform such other measures as the covered institution may deem reasonable or necessary.

5.2.4. Minimum Validation Procedures for EDD. - The procedures performed must enable Rampver Insure to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

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

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

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

- (1) Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
- (2) In the case of an entity that is subject to supervision by a financial regulatory/supervisory body, inquiring from the supervising authority the status of the entity;
- (3) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
- (4) Contacting the entity by phone or e-mail.

5.2.5. Failure to Conduct/Complete EDD and Tipping Off. - Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, Rampver Insure shall decline to establish the relationship with the customer, or to execute the requested transaction, without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

Where the covered person fails to satisfactorily complete EDD and reasonably believes that conducting EDD will tip off the customer, it shall file an STR and closely monitor the account and review the business relationship.

If Rampver Insure forms a suspicion that transactions relate to ML/TF, it should take into account the risk of tipping off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip off the customer or potential customer, it may choose not to pursue that process, and should file an STR. Institutions should ensure that their employees are aware of, and sensitive to, these issues when conducting the CDD.

5.3 High Risk Customers

5.3.1. Rampver Insure should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which:

- (1) Are subject to financial sanctions, embargoes or similar measures by the United Nations or other public international organizations;
- (2) Have been identified by credible sources as:
 - (a) having deficient AML/CFT regimes;
 - (b) having significant amounts of corruption or other criminal activity, including in particular illegal drug production, distribution or trafficking, money laundering, or human trafficking;
 - (c) providing financing or supporting terrorism or terrorist activities, or having terrorist organizations operating within their territory;
 - (d) being tax havens;
 - (e) experiencing significant civil unrest.

Credible sources include the FATF, FATF Style Regional Bodies (FSRB) such as the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities such as the Office of Foreign Assets Control of the U.S. Department of the Treasury, or other reliable third parties such as regulatory authorities, international standard setting bodies such as the IOSCO, the Basel Committee, the IAIS, or securities or commodities exchanges.

The background and purpose of these transactions should, as far as possible, be examined, and the findings established in writing. Whenever this examination reveals that these transactions have no apparent economic or visible lawful purpose, Rampver

Insure should decline to proceed with the transaction or to establish the business relationship, or terminate the existing relationship, and should consider filing an STR with the AMLC.

5.3.2. Rampver Insure should ensure that the principles applicable to covered institutions are also applied to branches, offices, affiliates and subsidiaries located abroad, if any, especially in countries which do not or insufficiently apply the anti-money laundering measures implemented in the Philippines, to the extent that local applicable laws and regulations permit.

Whenever Rampver Insure's branch, office, subsidiary or affiliate based outside the Philippines is prohibited from implementing the SEC AMLA Guidelines or any of the provisions of the AMLA, as amended, or its RIRR, by reason of local laws, regulations or a supervisory directive, Rampver Insure shall:

- (1) formally notify the Commission of this situation;
- (2) furnish a copy of the applicable laws and/or regulations or the supervising authority's directive, as the case may be;
- (3) advise the Commission of what measures or mitigating controls it intends to adopt to manage the money laundering (ML) and terrorist financing (TF) risks in such branches, offices, subsidiaries, or affiliates to the extent feasible;
- (4) keep the Commission apprised of its efforts in this area, including any updates to the measures or controls referred to in point 3 above;
- (5) at the direction of the Commission, close any branch or office, or divest itself of its interest in any subsidiary or affiliate, as the case may be, if the Commission determines that Rampver Insure cannot effectively manage the ML and/or TF risks arising from its relationship with such ranch, office, subsidiary, or affiliate.

5.3.3. Customers from countries referred to in Section 5.3.1 above are considered higher risk customers. Rampver Insure is required to establish the source of wealth of higher risk customers. Decisions on business relations with higher risk customers must be taken by its senior management.

5.4 Politically Exposed Persons

5.4.1. Rampver Insure shall establish and record the true and full identity of PEPs, as well as their immediate family members and entities related to them.

Before Rampver Insure can accept a prospect as customer, a Frontline Employee must determine whether the prospect is a public figure, a related individual (each as defined in footnote 7), or a firm that is controlled by a public figure or related individual.

⁷ A "public figure" is any individual who occupies, has recently occupied, is actively seeking, or is being considered for, a senior position in a government or political party of a country, state, or municipality or any department (including the military), agency, or instrumentality (e.g., a government-owned corporation thereof). A "related individual" is any person who is (i) a senior adviser who is closely associated with a public figure, or (ii) a member of a public figure's immediate family (i.e. spouse, parent, sibling, or child).

Once an individual prospect has been identified as a public figure, a related individual or an institutional prospect controlled by a public figure or related individual, the Business Development Manager should be informed of the determination. The Business Development Manager should then determine the reputational and other risks that would be posed to Rampver Insure if it provided investment advisory services to the individual or institutional prospect. In determining the magnitude of these risks, the Business Development Manager must consider information on the prospect's reputation. Depending on the risk level determined through proper evaluation of these factors, the Business Development Manager may determine that it is appropriate to take any one or more of the following steps in order to determine whether to accept the account:

- (1) Review available published articles regarding the prospect.
- (2) Obtain the authorization of the prospect under the law to ensure that any account information or other relevant information may be disclosed as necessary to conduct appropriate inquiries and obtain appropriate approvals.

In case of domestic PEPs or persons who have been entrusted with a prominent function by an international organization, or their immediate family members or close associates, in addition to performing the applicable due diligence measures, Rampver Insure shall:

- (1) Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
- (2) In cases when there is a higher risk business relationship, adopt measures under Section 5.3.3 and Section 5.3.4 hereof on Enhanced Due Diligence relative to individual customers.

In relation to foreign PEPs or their immediate family members or close associates, in addition to performing the applicable customer due diligence measures, covered persons shall:

- (1) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
- (2) Adopt measures under Section 5.3.3 and Section 5.3.4 hereof on Enhanced Due Diligence relative to individual customers.

5.5 Single Proprietorships, Corporations, Partnerships and indirect Prospects

5.5.1. Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant 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 veracity of the corporation or identity of its directors and/or officers, or of the business or its partners, a search or inquiry with the Commission or the relevant Supervising Authority/Regulatory Agency shall be made.

5.5.2. The following relevant documents shall be obtained in respect of corporate/other business applicants that are regulated in the Philippines (Please refer also to Section 5.1.4 for the list of documentary requirements for individuals and corporate prospects):

- (1) Copies of the Certificate of Registration issued by the Department of Trade and Industry, for single proprietors, or by the SEC, for corporations and partnerships, including the Articles of Incorporation or Certificate of Partnership, as

appropriate; copies of the By-Laws of the corporation; the latest General Information Sheet, which lists the names of directors/trustees/partners and principal stockholders; and secondary licenses, if any; and other documents such as but not limited to clearance/certification from the Commission that the company is active and compliant with the reportorial requirements.

The original or certified true copies of any or all the foregoing documents, where required, should be produced for comparison and verification.

- (2) Corporate/Partners' Secretary Certificate citing the pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity;
- (3) Where necessary and reasonable, Rampver Insure may also require additional information about the nature of the business of clients, copies of identification documents of shareholders, directors, officers and all authorized signatories; and
- (4) In the case of a corporate/business applicant that is owned or controlled indirectly or through a chain of entities, a detailed organizational chart or organogram clearly showing the respective ownership and/or control structure, including identification of all beneficial owners.

The type of measures that would normally be needed to satisfactorily perform identification of beneficial owners would require identifying the natural persons with a controlling interest and identifying the natural persons who comprise the management of the legal person or arrangement. Where the customer or owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder of that company.

5.5.3 For companies, businesses or partnerships registered outside the Philippines, if any, comparable documents are to be obtained, duly authenticated by a senior officer of Rampver Insure assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

5.5.4. If significant changes to the company structure or ownership occur subsequently, or suspicions arise as a result of a change in the payment profile as reflected in a company account, further checks are to be made on the identities of the new owners.

5.5.5. It is not necessary for Rampver Insure to routinely verify the details of the intermediate companies in the ownership structure of a company. However, Rampver Insure must always use its best efforts to determine who actually controls the customer. Complex ownership structures (e.g. structures involving multiple layers, cross-ownership, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk. In these cases, further steps may be necessary to ensure that the institution is satisfied on reasonable grounds as to the identity of the beneficial owners.

The need to verify the intermediate corporate layers of the ownership structure of a company will therefore necessarily depend upon Rampver Insure's overall

understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for Rampver Insure to consider if it has taken adequate measures to identify the beneficial owners.

It is a good business practice for Rampver Insure to have each legal entity account holder complete and sign a "beneficial owner declaration form" for each account, and to obtain an organizational chart clearly showing the companies in the group, the relationship of the companies to each other, the ownership of each company, and the ultimate beneficial owner(s) of the customer.

5.5.6 Indirect Prospects

If a prospect has an existing business relationship with any of its registered investment company principals, then Rampver Insure may rely upon the latter's KYC analysis of the prospect in accordance with that business' own anti-money laundering policy procedures, but only if the following requirements are satisfied:

- (1) Rampver Insure must document or receive confirmation that the other investment companies have (a) a legitimate business relationship with the prospect, and (b) has complied with its own anti-money laundering policies and procedures.
- (2) The Client Relations/Admin Officer must evaluate the type of KYC information required and obtained by the other investment companies for the type of prospect in question. Additionally, the said Officer must determine if such information would sufficiently satisfy the KYC determinations that Rampver Insure is required to make for the same type of Indirect Prospect. If, in the Client Relations/Admin Officer's judgement, the KYC information required by the other investment companies for the type of prospect would not satisfy Rampver Insure's KYC determinations, then, before Rampver Insure can accept such indirect prospects as clients, it must obtain additional KYC information that will satisfy its own KYC requirements.
- (3) Rampver Insure must be able to obtain, upon request, from the other investment companies the documentation that was obtained and relied upon by them to determine the identity of the Indirect Prospect. Rampver Insure must maintain for its own records all the documentation relating to the said Indirect Prospect.

5.6 Shell Companies

5.6.1. Shell companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted. Rampver Insure should note that shell companies may be abused by money launderers and therefore be cautious in their dealings with them.

5.6.2. In addition to the requirement under Section 5.6.2, Rampver Insure should also obtain a Board of Directors' Certification as to the purposes of the owners/stockholders in acquiring the shell company. There must likewise be satisfactory evidence of the identities of the beneficial owners, bearing in mind the "Know-Your-Customer" principle.

5.7 Trust, Nominee and Fiduciary Accounts

5.7.1. Rampver Insure shall establish whether the applicant for business relationship is acting on behalf of another person as a trustee, nominee or agent. Covered institutions should obtain competent evidence of the identity of such agents and authorized signatories, and the nature of their trustee or nominee capacity and duties.

5.7.2. Where Rampver Insure entertains doubts as to whether the trustee, nominee or agent is being used as a dummy in circumvention of existing laws, it shall immediately make further inquiries to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, Rampver Insure shall consider whether to proceed with the business, bearing in mind the "Know-Your- Customer" principle. If Rampver Insure decide to proceed, it shall record any misgivings and give extra attention to monitoring the account in question.

5.7.3. Where the account is opened by a firm of lawyers or accountants, Rampver Insure should make reasonable inquiries about transactions passing through the subject accounts that give cause for concern, or from reporting those transactions if any suspicion is aroused. If a money laundering Suspicious Transaction Report is made to the AMLC in respect of such client's accounts, the Council will seek information directly from the lawyers or accountants as to the identity of its client and the nature of the relevant transaction, in accordance with the powers granted to it under the AMLA, as amended, and other pertinent laws.

5.8 Transactions Undertaken on Behalf of Account Holders or Non-Account Holders

5.8.1. Transactions Undertaken on Behalf of Account Holders or Non-Account Holders. - Where transactions are undertaken on behalf of account holders of Rampver Insure, particular care shall be taken to ensure that the person giving instructions is authorized to do so by the account holder.

Transactions undertaken for non-account holders demand special care and vigilance. Where the transaction involves significant amounts, the customer should be asked to produce competent evidence of identity including nationality, especially in cases where the client is not a Filipino, the purposes of the transaction, and the sources of the funds.

5.9 Bearer Shares

5.9.1. Bearer shares are equity securities that are wholly owned by whoever holds the physical stock certificate. The issuing company does not register the owner of the stock or track transfers of ownership. Transferring the ownership of the stock involves only delivering the physical document. Bearer shares therefore lack the regulation and control of common shares because ownership is never recorded. Due to the higher ML/TF risks associated with bearer shares, the FATF standards require countries that allow companies to issue bearer shares to take appropriate measures to ensure that they are not misused for money laundering.

Philippine legislation prohibits domestic companies from issuing bearer shares. However, some foreign jurisdictions do permit companies to issue such shares, and there is a possibility that Philippine securities firms may encounter such firms as customers. Thus, institutions

dealing with companies that issue such shares need to be particularly diligent, as it is often difficult to identify the beneficial owner(s). Rampver Insure has adopted procedures to establish the identities of the holders and beneficial owners of such shares and ensure that they are notified whenever there is a change of holder or beneficial owner.

If Rampver Insure shall deal with bearer share entities, it shall conduct enhanced due diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account. These entities shall be subject to ongoing monitoring at all times and the list of stockholders and/or beneficial owners shall be updated within thirty (30) days after every transfer of ownership and the appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

Specifically, Rampver Insure should obtain declarations prior to account opening, and annually thereafter, from each beneficial owner holding at least five percent (5%). Rampver Insure should also require the customer to notify it immediately of any changes in the ownership of the shares.

5.10 Wire Transfers

5.10.1. Because of the risk associated with dealing with fund/ wire transfers, where Rampver Insure may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, it has established policies and procedures designed to prevent it from being utilized for that purpose which shall include, but not limited to, the following:

- (1) A beneficiary institution shall not accept instructions to pay-out fund transfers to non-customer beneficiary, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said beneficiary. Should the originator and beneficiary be the same person, the beneficiary institution may rely on the customer due diligence conducted by the originating institution provided the rules on third party reliance under Section 5.1.12 are met, treating the originating institution as third party as therein defined;
- (2) An originating institution shall not accept instructions to fund/wire transfer from a non-customer originator, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said originator;
- (3) In cross border transfers, if the originator is a high risk customer as herein described, the beneficiary institution shall conduct enhanced due diligence on the beneficiary and the originator. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant;
- (4) Whenever possible, manually initiated funds transfer (MIFT) instructions should not be the primary delivery method. Every effort shall be made to provide client with an electronic solution. Where MIFT is utilized, the following validation procedures shall apply:
 - a) Prior to Rampver Insure accepting from a customer a manually initiated funds transfer request, the customer must execute and sign an agreement which preferably is part of the account opening documentation, wherein are

outlined the manual instruction procedures with related security procedures including customer agreement to accept responsibility for fraudulent or erroneous instructions provided Rampver Insure has complied with the stated security procedures.

- b) It is mandatory that written MIFT instructions are signature verified. In addition, one of the following primary security procedures must be applied:
 - (i) a recorded callback to the customer to confirm the transaction instructions, or
 - (ii) test word arrangement/verification, provided that this procedure may be substituted by any of the following validity checks:
 - use of a controlled PIN or other pre-established code;
 - sequential numbering control of messages;
 - pre-established verifiable forms;
 - same as prior transmissions;
 - standing/pre-defined instructions; or value for value transactions.
 - c) It is mandatory that MIFT instructions are signature verified and the device be located in a secured environment with limited and controlled staff access which permits visual monitoring. If monitoring is not possible, the device must be secured or programmed to receive messages into a password protected memory.
 - d) MIFT transactions below a certain threshold [approved by the [branch manager/country manager] (for branches of foreign covered institutions) or Business Risk Manager in accordance with policies and procedures approved by Rampver Insure's board of directors), may be processed with the mandatory procedure described above and an enhanced security procedure such as any or all of the following:
 - e) Telephone callback numbers and contacts must be securely controlled. The confirmation callback is to be recorded and made to the signatory/(ies) of the customer's individual account(s). For commercial and company accounts, the callback will be made to the signatory/(ies) of the account or, if so authorized, another person designated by the customer in the MIFT agreement. The party called is to be documented on the instructions. The callback must be made by someone other than the person receiving the original instructions and effecting the signature verification.
- (5) Cross border and domestic fund/wire transfers and related message not exceeding P50,000.00 or its equivalent in foreign currency, shall include accurate and meaningful originator and beneficiary information. The following information shall remain with the transfer or related message through the payment chain:
- (a) Name of the originator;
 - (b) Name of the beneficiary; and
 - (c) Account number of the originator and beneficiary, or in its absence, a unique reference number.

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

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

- (7) Should any wire/fund transfer amounting to P50,000.00 or more or its equivalent be unaccompanied by the required originator information, the beneficiary institution shall exert all efforts to establish the true and full identity and existence of the originator by requiring additional information from the originating institution or intermediary institution. It shall likewise apply enhanced due diligence to establish the true and full identity and existence of the beneficiary. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of an ST to the AMLC when circumstances warrant.

6. RECORD KEEPING

6.1 General Requirements for Record Keeping - Rampver Insure's policies and procedures as described in Section 5 hereof, shall include procedures for making and maintaining a record of all customer relationships and transactions, including customer identification and verification, such that:

- (1) Requirements of the AMLA, as amended, are fully met;
- (2) Any transaction effected via the covered institution can be reconstructed and from which the AMLC, and/or the courts will be able to compile an audit trail for suspected money laundering, when such report is made to it;
- (3) The covered institution can satisfy within a reasonable time any inquiry or order from the AMLC as to disclosure of information, including without limitation, whether a particular person is the customer or beneficial owner of transactions conducted through the covered institutions.

6.2. Periods of Retention. - Rampver Insure must keep the documents set forth below for at least five (5) years from the date of the establishment of the business relationship or the date on which the document was obtained, prepared or updated, whichever is late.

- (1) Records of all transactions, including but not limited to, completed and signed Client Profile Forms and all documentation obtained in support of required identity, source-of-income/assets and other determinations shall be maintained and safely secured in an easily accessible place. (Responsible Party: Frontline Employee assigned to client).
- (2) Reports filed with AMLC and the SEC as well as other government authorities with respect to an investment company client or prospective investment company client and all documentation obtained by the involved Rampver Insure employee supporting these reports (Responsible Party: Business Development Manager involved in alerting the Reporting Officer as to facts requiring filing of the report by the Compliance Officer).
- (3) Records relating to anti-money laundering training, including the names of attendees and the dates and locations of the training sessions (Responsible party: General Manager).
- (4) With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least five (5) years from the dates when they were closed (Responsible party: General Manager).
- (5) Any other documents required by applicable anti-money laundering regulations. (Responsible party: Business Development Manager)
- (6) SRC Rule 52.1.1 (Books and Records Keeping Rule) and Rule 52.1.2 (Records Retention Rule) of the 2015 Implementing Rules and Regulations of the SRC continue to be in full force and effect.

Notwithstanding the foregoing, for closed accounts, the records on customer identification, account files and business correspondence shall be preserved and stored for at least five (5) years from the dates when they were closed. If the records relate to on-going investigations or transactions that have been subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed.⁸ Transaction documents may be retained as originals or copies, on microfilm

⁸ Sec.5.4 of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

or in electronic form, provided such are admissible in court, pursuant to the Revised Rules of Court and the E-Commerce Act and its implementing guidelines.⁹

6.3. Records Relating to Pending Case. - Notwithstanding Section 6.2 hereof, if the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.

6.4. Forms of Records. - Transaction documents may be retained as originals or copies, on microfilm, provided that such forms are admissible in court, pursuant to the Revised Rules of Court and the E-commerce Act and its Implementing Rules and Regulations.

6.5. Digitization of Customer Records. - Covered institutions shall comply with the Guidelines on Digitization of Customer Records as promulgated by the AMLC in accordance with the terms thereof, as may be applicable.

6.6. Persons Responsible for Safekeeping of Records. - Rampver Insure has designated at least two (2) persons responsible in the safekeeping of all records and report to the Commission any change in the person/s responsible.

7. MONITORING AND REPORTING OF COVERED AND SUSPICIOUS TRANSACTIONS

7.1. Reporting System. - Rampver Insure has instituted a system for the mandatory reporting of covered transactions and suspicious transactions. Rampver Insure employees are responsible for monitoring transactions directed by its clients in order to detect covered and suspicious transactions that suggest attempted or actual money laundering.

7.2. Registration with AMLC. - Rampver Insure, being a covered person, has registered with the AMLC's electronic reporting system.

7.3. Covered Transaction Report (CTR). - Rampver Insure shall file a Covered Transaction Report ("CTR") with the AMLC involving any transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (Php500,000.00) within one (1) banking day;

7.4. Suspicious Transaction Report (STR). - Rampver Insure shall file Suspicious Transaction Reports ("STR") with the AMLC for transactions, regardless of the amount of the transaction, where any of the following circumstances exists:

- (1) There is no underlying legal or trade obligation, purpose or economic justification;
- (2) The client is not properly identified;
- (3) The amount involved is not commensurate with the business or financial capacity of the client;
- (4) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA;
- (5) Any circumstance relating to the transaction which is observed to deviate from the file of the client and/or the client's past transactions with the covered institution;

⁹ Sec.5.3 of the SEC Anti-Money Laundering Operating Manual for Covered Institutions

- (6) The transaction is in any way related to an unlawful activity or offense under the AMLA that is about to be, is being, or has been committed; or
- (7) Any transaction that is similar or analogous to any of the foregoing.

Circumstances may suggest that money laundering activity is taking place. In such circumstances, the economic background and purpose of any transaction or business relationship should be clarified and scrutinized carefully. Examples of Suspicious Circumstances are as follows:

- (1) If in combination with other factors suggesting actual or attempted money laundering, a client insists that cash deposits be accepted, despite being informed of Rampver Insure's policy discouraging cash deposits.
- (2) A client whose identity cannot or is unusually difficult or expensive to verify.
- (3) Clients who are reluctant to provide normal information when establishing a business relationship or who provide fictitious or conflicting information.
- (4) Clients who avoid contacts with Rampver Insure staff/employees.
- (5) Clients with no discernable reason for using Rampver Insure's services.
- (6) Clients who are reluctant to provide complete information regarding their purpose, prior asset management relationships, officers or directors, or location of their business.
- (7) Client who are reluctant to reveal details about their activities, or to provide financial statements, or whose financial statements are noticeably different from those of similar businesses.
- (8) Any dealing with an agent where the identity of the principal is undisclosed, contrary to normal procedures for the type of business or transaction concerned.
- (9) Use of an address which is not the client's apparent address.

In this regard, Rampver Insure should exercise due diligence by implementing adequate systems for identifying and detecting suspicious transactions.

Suspicious transactions are likely to involve a number of factors which together raise a suspicion in the mind of Rampver Insure that the transaction may be connected with any unlawful activity.

7.5. Transaction Reporting. - Rampver Insure shall report to the AMLC all covered transactions and suspicious transactions within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

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

7.6. Transactions that are both Covered and Suspicious. - Should a transaction be determined to be both a covered and a suspicious transaction, Rampver Insure shall report the same as a suspicious transaction.

7.7. Attempted Suspicious Transactions. - Rampver Insure shall likewise file STR for suspicious attempted transactions. An ***attempted transaction*** is one that a client

intended to conduct and made overt acts to do so. Such overt acts include entering into negotiations or discussions to conduct the transaction and involves definite measures to be undertaken by Rampver Insure or the client. In order for an attempted transaction to be reported as an *attempted suspicious transaction*, there must be reasonable grounds to suspect that said attempted transaction is related to money laundering or terrorist financing or when any of the circumstances enumerated in Section 7.4 hereof exists.

7.8. Reporting of Customer's Unlawful Activities. - Where any employee or personnel, director or officer of Rampver Insure knows that the client has engaged in any of the unlawful activities under the AMLA, the matter must be promptly reported to its Compliance Officer who, in turn, must immediately report the details to the AMLC.

If there is reasonable ground to suspect that the customer has engaged in an unlawful activity, the Compliance Officer, on receiving such a report, must promptly evaluate whether there are reasonable grounds for such belief and must then immediately report the case to the AMLC, unless he considers, and records an opinion, that such reasonable grounds do not exist.

7.9. Register of Suspicious and Covered Transactions. - Rampver Insure shall maintain a register of all suspicious transactions that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the AMLC.

Rampver Insure shall likewise maintain a register of all covered transactions which are not reported to the AMLC pursuant to AMLC Resolution No. 292, Series of 2003.

The registers shall contain details of the date on which the report is made, the person who made the report to its Compliance Officer, and information sufficient to identify the relevant papers related to said reports.

7.10. Confidentiality of CTR and STR. - Rampver Insure, its directors, officers and employees, shall not warn their customers that information relating to them has been reported or is in the process of being reported to the AMLC, or communicate, directly or indirectly, such information to any person other than the AMLC. Any violation of this confidentiality provision shall render them liable for criminal, civil and administrative sanctions under the AMLA.

When reporting CTs and STs to the AMLC, Rampver Insure, 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 report was made, the contents thereof, or any other information in relation thereto. Any information about such reporting shall not be published or aired, in any manner or form, by the mass media, or through electronic mail, or other similar devices.

In case of violation thereof, the concerned officer and employee of Rampver Insure shall be criminally liable in accordance with the provision of the AMLA, as amended.

Rampver Insure, its directors, officers and employees, shall not notify their customers that information relating to them has been flagged internally with a view toward making a determination as to whether to file a ST, or communicate, directly or indirectly, such information to any person other than the AMLC.

7.11 Safe Harbor Provision. - No administrative, criminal or civil proceedings shall lie against any person for having made a suspicious or covered transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other Philippine law. Covered institutions, its directors and employees shall likewise not be liable for any loss arising out of such disclosure, or any act or omission, in relation to the fund, property or investment in consequence of the disclosure, where such is made in good faith and in the regular performance of their duties under the Act.

7.12 Procedure for Reporting:

Rampver Insure employees must promptly report to the Business Development Manager any client-directed transaction or series of transactions conducted, or attempted to be conducted, at or through Rampver Insure if the employee knows, suspects or has reason to suspect that the transaction or series of transactions:

- (1) involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including but not limited to the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any money laundering regulation;
- (2) is designed to evade a money laundering regulation; or
- (3) has no business or apparent lawful purpose or is not the sort of transaction(s) in which the client would normally be expected to engage and, after examining available facts including the background and possible purpose of the transaction, no reasonable explanation for the transaction(s) is known.¹⁰

Once notified of a suspicious client-directed transaction (including series of transactions), the Business Development Manager must document the reason for the transaction and determine whether the transaction is suspicious according to the foregoing standard. The Business Development Manager must create and maintain a written record of these determinations (see Section VI Record Keeping).

In addition, if the Business Development Manager determines that the transaction constitutes a suspicious transaction, he or she must promptly report the matter to the Reporting Officer.

The Reporting Officer must in turn validate the case it meets the criteria for possible suspicious transactions. If it does, the Reporting Officer must forward the report to the Compliance Officer.

The Compliance Officer must present the case to the Senior Management of Rampver Insure for consultation. The Compliance Officer must then promptly evaluate whether there are reasonable grounds that the customer has engaged in an unlawful activity and

¹⁰ Generally, a client-directed transaction or series of transactions suggests attempted or actual money laundering if it lacks a reasonable economic basis or is unnecessarily complex. Examples of such transactions are where a client directs matching buy and sell orders (creating the illusion of trading) or transactions that appear to be structured to avoid legal reporting requirements. Also, client requests to clear transactions in ways that are inconsistent with normal practice may suggest money laundering.

will then take the appropriate action, including the completion and filing of the Suspicious Transaction Report with the AMLC, unless he considers, and records an opinion, that such reasonable grounds do not exist.

The Business Development Manager must maintain a register of all suspicious transactions of Rampver Insure that have been brought to the attention of its Compliance Officer, including transactions that are not reported to the Council.

The said register must contain details of the date on which the report is made, the person who made the report to the Business Development Manager, and information sufficient to identify the relevant papers related to said reports.

Under no circumstances shall it be disclosed to any existing shareholder or prospective shareholder or any of its representatives that any information regarding themselves or their transactions are being reported to the AMLC. Neither shall it be disclosed directly or indirectly to any other person other than the AMLC.

7.13 Terminating Client Relationship

Rampver Insure may decide to terminate an existing client relationship because suspicious activity in the client's account or concerns or doubts about the true identity of the client, the source of the client's income or assets or whether the client is involved in illegal activities. The Business Development Manager should consult with the Reporting Officer who will endorse the matter to the Compliance Officer. The Compliance Officer shall promptly determine whether it is appropriate to notify governmental authorities in these circumstances and, if so, the most appropriate method of notification. Appropriate precautions must be taken to ensure that clients are not prematurely notified of termination or Rampver Insure's intent to terminate in these circumstances. Also, where appropriate, legal counsel should be involved in Rampver Insure's decision to terminate a client relationship.

8. COMPLIANCE

8.1. The Compliance Officer – Qualifications and Responsibilities. - Rampver Insure has appointed a senior officer as the Compliance Officer who is in charge of the implementation of its Operating Manual and the application of the internal programs and procedures, including customer identification policies and procedures, proper maintenance of records, reporting of covered and suspicious transactions to the AMLC, and training of employees.

The Compliance Officer shall be:

- (1) A senior officer with relevant qualifications and experience to enable him to respond sufficiently well to inquiries relating to the relevant person and the conduct of its business;
- (2) Responsible for establishing and maintaining a manual of compliance procedures in relation to the business of Rampver Insure;
- (3) Responsible for ensuring compliance by the staff of Rampver Insure with the provisions of the AMLA, as amended, its Implementing Rules and Regulations, and Rampver Insure's manual of compliance Procedures;
- (4) Responsible for disseminating to its board, officers and all employees memorandum

- circulars, resolutions, instructions, and policies issued by the AMLC and by the Commission in all matters relating to the prevention of money laundering;
- (5) The liaison between covered institution and the AMLC in matters relating to compliance with the provisions of the AMLA and its Implementing Rules and Regulations;
 - (6) Responsible for the preparation and submission to the AMLC written reports on the covered institutions' compliance with the provisions of the AMLA and its Implementing Rules and Regulations, in such form as the AMLC may determine, and within such period as the Commission may allow in accordance with the AMLA, as amended;
 - (7) Responsible for organizing training sessions for the staff on issues related to AML/CFT compliance, including providing guidance to the staff on how to avoid "tipping off" if any ST is filed or if any transaction or set of circumstances is flagged internally as potentially suspicious;
 - (8) Responsible for analyzing transactions to determine whether any are subject to reporting according to the indicators of suspicious transactions mentioned in the AMLA, relevant SEC regulations and this Guideline, and undertaking closer investigation of transactions when necessary;
 - (9) Responsible for reviewing all internal reports of potentially suspicious transactions for their completeness and accuracy;
 - (10) Responsible for preparing STRs and ensuring their timely filing with the AMLC;
 - (11) Responsible for keeping records of internally and externally reported suspicious transactions;
 - (12) Responsible for remaining informed of the national and international issues and developments on money laundering and terrorist financing and making suggestions to the board of directors and management for upgrading the institution's policies and procedures in light of these developments; and
 - (13) Responsible for periodically reporting information on the institution's efforts to combat money laundering and terrorist financing to the board, and recommending changes in the institution's policies or procedures when deemed necessary.

The Compliance Officer should not simply be a passive recipient of ad hoc reports of suspicious transactions, but should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. To fulfill these functions, Rampver Insure must ensure that the Compliance Officer receives full cooperation from all staff and full access to all relevant documentation.

8.2. Adviser Regarding AML matters. - Rampver Insure shall appoint one or more senior officers, or an appropriate unit, to advise its management and staff on the issuance and enforcement of in-house instructions to promote adherence to the AMLA, as amended, the RIRR, its MLPP, including personnel training, reporting of covered and suspicious transactions, and generally, all matters relating to the prevention of money laundering.

8.3. Responsibility of Rampver Insure and its Board. - Notwithstanding the duties of the Compliance Officer, the ultimate responsibility for proper supervision, reporting and compliance under the AMLA, as amended, its RIRR shall rest with Rampver Insure and its board of directors.

9. INTERNAL CONTROL AND PROCEDURES

9.1. General Requirements. - Rampver Insure is required to establish and implement internal control and procedures aimed at preventing and impeding money laundering. Such procedures shall, among other things, ensure that such covered institutions and their employees are aware of the provisions of the AMLA, its implementing rules and regulations, as well as all reportorial and compliance control and procedures that shall be established by the AMLC, the Supervising Authority and each covered institution.

Rampver Insure shall see to it that its policies and procedures for dealing with money laundering, reflecting the requirements under the AMLA and its implementing rules and regulations, are clearly set out and reflected in their Operating Manual.

9.2. Coverage of Internal Control Policies and Procedures. - Policies and procedures should cover, among others:

- (1) Communications of firm policies relating to money laundering, including timely disclosure of information and internal audits to ensure compliance with policies, procedures and controls relating to money laundering;
- (2) Account opening and customer identification, including requirements for proper identification;
- (3) Maintenance of records;
- (4) Compliance with the requirement of the AMLA, as amended, its Revised Implementing Rules and Regulations, and all Circulars issued by the Commission and the AMLC;
- (5) Cooperation with the Commission and other relevant Authorities.

9.3. Written Internal Reporting Procedures. - Rampver Insure has established written internal reporting procedures which shall:

- (1) Enable all its directors, officers, employees, and all key staff to know to whom they should report any knowledge or suspicion of money laundering activity;
- (2) Ensure that there is a clear reporting chain under which suspicions of money laundering activity will be passed to the Compliance Officer, in accordance with the reporting procedures of Rampver Insure
- (3) Require the Compliance Officer to consider any report in the light of all relevant information available for the purpose of determining whether or not it gives rise to a knowledge or suspicion of money laundering;
- (4) Ensure that the Compliance Officer has reasonable access to any other information which may be of assistance in the determination as to whether or not a suspicious transaction report is to be filed;
- (5) Require that, upon determination of the suspicious nature of the report, the information contained therein is disclosed promptly to the AMLC;

- (6) Maintain a register of all reports filed pursuant to Sections 7.7, 7.8 and Section 7.9 above.

10. INTERNAL AUDIT

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

10.2. Frequency and Scope of Internal Audit. - The internal audit shall be responsible for the periodic (not less frequently than once every 2 years) and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, CT and ST reporting and record keeping and retention, as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

10.3. Electronic AML/CFT Monitoring System. - For Rampver Insure with electronic AML/CFT transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities.

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

10.5. Outsourcing of Internal Audit Functions/External Audit. - Rampver Insure may, due to the scale and nature of their operations, assign the internal audit function to another person (e.g. professional association, parent company or external auditors) under terms of reference approved by Rampver Insure's board of directors designed to ensure the effectiveness of the internal audit function. Where Rampver Insure delegates its responsibilities for internal audit, due diligence is to be exercised to ensure that the persons appointed are able to perform these functions effectively and the fact of such appointment must be relayed in writing to the Commission and to AMLC. Notwithstanding that the internal audit function may be outsourced, Rampver Insure's board of directors remains responsible for its effective operation.

11. TRAINING

11.1. Education and Continuing Training. - In order to recognize attempts to use Rampver Insure as a vehicle for money laundering activities, Rampver Insure personnel must be fully aware of their personal obligations and responsibilities in combating money

laundering. They must have sufficient knowledge about their clients and the types of transactions the client is likely to be engaged in.

Rampver Insure shall create and maintain a training program to ensure that all Rampver Insure staff and personnel, including directors and officers, will be fully knowledgeable of all aspects of prevention, detection and reporting of any suspicious activities that may constitute money laundering. New staff must develop a general appreciation of the background of money laundering, the importance of identifying covered and suspicious transactions and reporting such transactions to the appropriate authorities. On the other hand, a higher level of instruction covering all aspects of money laundering procedures should be provided to supervisors and managers, while personnel who deal directly with clients (such as Business Development Officers and advisory staff) should be trained to identify suspicious transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. Frontline employees should be made aware of Rampver Insure's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in cases under suspicious circumstances. (Based on SEC Memorandum Circular 2, Series of 2010)

This training program should be attended by all employees in the business development and client relations area and those who have access to shareholder transactions. Refresher courses and re-training programs shall be arranged once a year to remind key staff of their responsibilities and to make them aware of the changes in the law, rules and regulations relating to money laundering.

Rampver Insure shall provide education and continuing training for all its staff and personnel, including directors and officers, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and to be familiar with its system for reporting and investigating suspicious matters.

11.2. Outsourcing of Training Functions/External Training Providers. - Rampver Insure may, due to the scale and nature of their operations, assign the training functions to another person (e.g. professional association, parent company or external training provider). Where Rampver Insure delegates its responsibilities for training, due diligence is to be exercised to ensure that the persons appointed are able to perform these functions effectively and the fact of such appointment must be relayed in writing to the Commission and to AMLC.

Notwithstanding that the training function may be outsourced, Rampver Insure's board of directors remains responsible for the effective operation of the training program.

11.3. Recommended Training Programs. - Timing and content of training for various sectors of staff will need to be adapted by Rampver Insure to its own needs. The following training programs are recommended:

(1) New Staff

A general appreciation of the background to money laundering, the need to be able to identify suspicious transactions and report such transactions to the appropriate designated point within Rampver Insure. This training shall be provided to all new employees, regardless of level of seniority.

(2) Cashiers/Dealers' Representatives/Frontliners/Advisory Staff

Personnel who deal directly with the clients are the first point of contact with potential money launderers. Their efforts are therefore vital to the covered institutions' reporting system for such transactions. They should be trained to identify suspicious transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. "Front Line" staff should be made aware of Rampver Insure's policy for dealing with non-regular customers particularly where large cash transactions are involved, and the need for extra vigilance in cases under suspicious circumstances.

(3) Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to supervisors and managers. This will include the offences and penalties arising from the AMLA, procedures relating to service of production and restraint orders, internal reporting procedures, and the requirements for verification of identity and the retention of records.

11.4. Regular Refresher Training. - Rampver Insure shall, at least once a year, make arrangements for refresher training to remind key staff of their responsibilities and to make them aware of any changes in the laws and rules relating to money laundering, as well as the internal procedures of Rampver Insure.

11.5. Training Program and Records of Trainings Conducted. - Rampver Insure's annual AML training program and records of all AML seminars and trainings conducted by Rampver Insure and/or attended by its personnel (internal or external), including copies of AML seminar/training materials, shall be appropriately kept by the Compliance Officer/unit/department, and made available during periodic or special SEC examinations and to self-regulatory organizations (SROs) of Rampver Insure, if applicable.

11.6. Cascading of Updates and New Requirements. - Rampver Insure shall ensure that all relevant personnel are informed in a timely manner of any new provisions, updates or changes in laws, as well as new, amended or updated Commission rules, regulations, guidelines and circulars relating to money laundering and/or terrorist financing, and the internal procedures of Rampver Insure based on any of the foregoing. Training on any such new provisions, amendments, updates or changes shall be provided as necessary.

Exhibit A

High Risk Businesses

- (1) Non-bank financial institutions (e.g. money transmitters, foreign exchange changers, remittance services, check cashiers)
- (2) Travel agencies
- (3) Casinos
- (4) Import/Export companies (e.g. trading companies)
- (5) Jewel/gem/precious metal dealers
- (6) Car/boat/plane dealerships
- (7) "Small" or foreign broker dealers
- (8) Any cash-intensive businesses
- (9) Art and antique dealers

Exhibit B

FORMS USED BY RAMPVER INSURE

INSURANCE APPLICATION FORMS,

CLIENT INFORMATION SHEET

AND

INVESTOR SUITABILITY QUESTIONNAIRE