SERVIAMUS MUTUAL BENEFIT ASSOCIATION

(AML/MTPP MANUAL)

MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM

4th Floor, Diocesan Centrum Bldg.
Lluch St., Iligan City,
Lanao del Norte
TIN: 008-534-242-000
Telephone No. (063) 228-4354/223-2493 | Fax No. (063)221-5327
E-mail: serviamus_mba@yahoo.com

YEAR 2020

TABLE OF CONTENTS

I. INTRODUCTION

For more than two decades, the Diocese of Iligan has been actively addressing the malnutrition problem in its area of jurisdiction. However, a deeper realization has evolved from years of experience; that to be able to effectively combat this problem, poverty, the root cause of malnutrition, should relevantly respond to another approach or a methodology must be adopted. Thus, credit scheme came into being. The loaning project further grew with the support from Food Transition Strategy (FTS) of the Catholic Relief Services (CRS) through the implementation of the Small Enterprise Development Program. This aimed to be established at the Diocesan level, a credit program which has potential of sustainability and impact, at the same time, support viable and sustainable income generating projects at the barangay level which served as continuing source of income for the supported families. The Small Enterprise Development Program (SEDP) continued providing loan assistance to individual micro-entrepreneur. Two years later, problems cropped up one after another as repayment rate dropped significantly and more clients were incurring arrears and bad debts. Nevertheless, the program was determined to move ahead. It was during this time that Catholic Relief Services (CRS) was vent on the instruction of the Grameen Banking technology for all its partners. Given all the opportunities and commitment/enthusiasm of all the staff, Grameen Bank replication was fully implemented on June 1997. As the program geared towards growth in terms of outreach and quality, it also transformed from being church-based to Non-Government Organization (NGO). On the 19th of October 1998, SERVIAMUS FOUNDATION INC.(SFI) legally entered into mainstream of development institutions. Serviamus Foundation Incorporated is governed by Republic Act No. 10693 known as the "Microfinance NGOs Act". SFI is also a member of the Microfinance Council of the Philippines.

As SFI continued to provide loan assistance, they also provided financial assistance in times of loss (death of member and dependents) thru Mutual Aid Fund (MAF). The members pay a weekly contribution of five pesos and receive maximum of Five Thousand Pesos (PhP5,000) as financial assistance. In 2007, the management and Board decided that MAF must be enhanced by providing bigger benefits and bigger premium to its members. The Enhanced Mutual Aid Fund (EMAF) program gives a beneficial impact to the members as well as to the community, yet the risk became higher because the premium and benefits did not undergo actuarial study. Last 2013, the SFI Board of Trustees and management decided to create a Mutual Benefit Association. It was registered in Securities and Exchange Commission (SEC) last May 24, 2013 and got a license from the Insurance Commission last January 27, 2014 with the License No. 2013-32-O. Serviamus Mutual Benefit Association Inc. (MBAI) is a member of the Microinsurance MBA Association in the Philippines Inc. (MiMAP) also known as RIMANSI Organization.

Pursuant to the power of the Insurance Commission (IC) under Rule 18 (A), of the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001 (AMLA), As Amended", and Rule 27 of the Implementing Rules and Regulations (IRR) of

Republic Act No. 10168, otherwise known as "The Terrorism Financing Prevention and Suppression Act", Serviamus Mutual Benefit Association, hereby submits this Money Laundering & Terrorist Financing Prevention Program (MTPP) manual based on the revised guidelines provided therein.

This manual is designed to ensure that it shall comply with the AML and CTF requirements and obligations set out in Philippine legislation, rules, regulations, government regulatory bodies and agencies' guidance, and that adequate systems and controls are in place to mitigate the AML risks and that the association is not used to facilitate financial crime.

II. DEFINITION of TERMS

a. "**Act**" shall refer to Republic Act 9160 (as amended by Republic Act No. 9194) entitled, "An Act Defining the Crime of Money-Laundering, Providing Penalties therefor and for Other Purposes:

b. "**Anti-Money Laundering Act**" (AMLA) refers to Republic Act No. 9160, as amended by Republic Act Nos. 9194, 10167, 10365, and 10927.

c. "**Anti-Money Laundering Council**" (AMLC) refers to the financial intelligence unit of the Philippines which is the government agency tasks to implement the AMLA and the Terrorism Financing Prevention and Suppression Act (TFPSA).

d. "**Beneficial Owner**" refers to any natural person who:
   1. Ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or
   2. Has ultimate effective control over a legal person or legal arrangement;
   3. Owns the same percentage prescribed in the Guidelines on Identifying Beneficial Ownership and 2018 IRR, and its succeeding future amendments
   4. Control includes whether the control is exerted by means of trusts, agreements, arrangements, understandings, or practices, and whether or not the individual can exercise control through making decisions about financial and operating policies.

e. "**Close Relationship/Associates of PEPs**" refer to persons who are widely and publicly known, socially or professionally, to maintain a particularly close relationship with the PEP, and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

f. "**Competent Authorities**" refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the AMLC; the authorities that have the function of investigating and/or prosecuting money laundering, unlawful activities and terrorist financing, and seizing/freezing and confiscating any monetary

g. instrument or property that is in anyway related to an unlawful activity; authorities receiving reports on cross-border transportation of currency & bearer negotiable instruments (BNls); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements.

h. **"Covered transaction"** refers to:
   1. A transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (Php500'000 00) or its equivalent in any other currency; or
   2. A transaction, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), where the total premiums/fees paid for a policy, plan or agreement for the entire year exceeds Five Hundred Thousand Pesos (Php500,000.00) or its equivalent in any other currency.

i. "**Customer/Member -Client**" refers to any person who keeps an account, or otherwise transacts business with an ICRE. lt includes the following:
   1. Beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained or a transaction is conducted;
   2. Transactors, agents and other authorized representatives of beneficial owners;
   3. Beneficiaries of insurance policies;
   4. A company or person whose assets are managed by an asset manager;
   5. Trustors/grantors/settlors of a trust; and
   6. Insurance policy holder/owner, insured, whether actual or prospective.

j. "**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.

k. "**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 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: (i) to carry out or facilitate the commission of any terrorist act; (ii) by a terrorist organization, association or group; or (iii) by an individual terrorist.

l. "**Identification Document**" (ID) refers to any of the following evidence of identity:

   1. For Filipino citizens: Those issued by any of the following official authorities:
      a. PhilID;

b. Other identification issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and Instrumentalities; and
c. Other identification documents that can be verified using reliable, Independent source documents, data or information.

2. For foreign nationals:
   a. PhilID, for resident aliens;
   b. Passport;
   c. Alien Certificate of Registration; and
   d. Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, and instrumentalities.
3. For Filipino students:
   a. PhilID;
   b. School ID signed by the school principal or head of the educational institution; and
   c. Birth Certificate issued by the Philippine Statistics Authority; and
4. For low risk customers: Any document or information reduced in writing which the ICRE deems sufficient to establish the customer's identity.

m. "**Immediate Family Member of PEPs**" refers to individuals related to the PEP within the second degree of consanguinity or affinity.

n. "**Materially-linked Accounts**" shall include the following:
1. All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;
2. All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;
3. All "In Trust For" accounts where the trustee pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
4. All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
5. All accounts of juridical persons or legal arrangements that are owned, controlled or ultimately effectively controlled by the natural person whose monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control; and
6. All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing.

o. "**Monetary Instruments**" shall include, but is not limited to the following:

1. Coins or currency of legal tender of the Philippines, or of any other country;

2. Credit instruments, including bank deposits' financial interest, royalties, commissions, and other intangible property;
3. Drafts, checks, and notes;
4. Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, Instrument, whether written or electronic in character, including those enumerated in Section 3 of the Securities Regulation Code;
5. A participation or interest in any non-stock, non-profit corporation;
6. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts, or deposit substitute instruments, trading orders, transaction tickets, and confirmations of sale or investments and money market instruments;
7. Contracts or policies of insurance, life or non-life, contracts of surety ship, pre-need plans, and member certificates issued by mutual benefit association; and Other similar instruments where title thereto passes to another by endorsement, assignment, or delivery.

p. "**Monetary Instrument or Property Related to an Unlawful Activity**" refers to:
   1. All proceeds of an unlawful activity;
   2. All monetary, financial or economic means, devices, accounts, documents, papers, items, or things used in or having any relation to any unlawful activity;
   3. All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds, and other similar items for the financing, operations, and maintenance of any unlawful activity; and
   4. For purposes of freeze order and bank inquiry: related and materially-Linked accounts.

q. "**Money Laundering**" is committed by 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 (a), (b), or (c) above.

Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required to be reported to the Anti-Money Laundering Council (AMLC) under any of the provisions of

the AMLA, as amended, its RIRR, or this Part, fails to do so.

r. "**Offender"** refers to any person who commits a money laundering offense.

s. "**Official Document**" refers to any of the following identification documents:

1. For Filipino citizens: Those issued by any of the following official authorities:
   a. Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
   b. Government-Owned or -Controlled Corporations (GOCCs);
   c. Covered persons registered with and supervised or regulated by the BSP, SEC or lC;
2. For foreign nationals:
   a. Passport or
   b. Alien Certificate of Registration;
3. For Filipino students: School ID signed by the school principal or head of the educational institution; and
4. For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the customer's identity.

t. "**Person**" refers to any natural or juridical person.

u. "**Politically Exposed Person**" (PEP) refers to an individual who is or has been entrusted with prominent public position in (1) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (2) a foreign State; or (3) an international organization.

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

w. "**Property**" refers to anything or item of value, real or personal, tangible or intangible, or any interest therein, or any benefit, privilege, claim, or right with respect thereto, including:

1. Personal property, including proceeds derived therefrom, or traceable to any unlawful activity, such as, but not limited to:
   a. Cash;
   b. Jewelry, precious metals and stones, and other similar items;
   c. Works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;
   d. Perishable goods; and
   e. Vehicles, vessels, aircraft, or any other similar conveyance.
2. Personal property, used as instrumentalities in the commission of any unlawful activity, such as:
   a. Computers, servers, and other electronic information and

Communication systems; and

b. Any conveyance, including any vehicle, vessel, and aircraft.

3. Real estate, improvements constructed or crops growing thereon, or any interest therein, standing upon the record of the registry of deeds in the name of the party against whom the freeze order or asset preservation order is issued, or not appearing at all upon such records, or belonging to the party against whom the asset preservation order is issued and held by any other person, or standing on the records of the registry of deeds in the name of any other person, which are: derived from, or traceable to, any unlawful activity; or used as an instrumentality in the commission of any unlawful activity.

x. "**Related Accounts**" refers to those accounts, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.

y. "**Suspicious Transaction**" refers to a transaction, regardless of amount, where any of the following circumstances exists:

1. There is no underlying legal or trade obligation, purpose or economic Justification;
2. The customer is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the customer;
4. Taking into account all known circumstances, it may be perceived that the customer'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 profile of the customer and/or the customer's past transactions with the covered person;
6. The transaction is in any way related to an unlawful activity or any Money laundering activity or offense that is about to be committed, is being or has been committed; or
7. Any transaction that is similar, analogous or identical to any of the foregoing.

Any unsuccessful attempt to transact with an ICRE, the denial of which is based on any of the foregoing circumstances' shall likewise be considered as suspicious transaction

z. "**Transaction**" refers to any act establishing any right or obligation, or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person.

aa. "**Unlawful Activity**" refers to any act or omission, or series or combination thereof, involving or having direct relation, to the following:

1. "Kidnapping for Ransom" under Article 267 of Act No 3815, otherwise Known as the Revised Penal Code, as amended;
2. Sections 4, 5, 6, 8, 9, 10, 11, 12,13, 14,15 and 16 of Republic Act No. 9165, otherwise known as the "Comprehensive Dangerous Drugs Act of 2002";
3. Section 3 paragraphs b, c, e, g, h and i of Republic Act No. 3019, as amended, otherwise known as the "Anti-Graft and Corrupt PracticesAct";
4. "Plunder" under Republic Act No. 7080, as amended;
5. "Robbery" and "Extortion" under Articles 294, 295, 296, 299, 300, 301 And 302 of the Revised Penal Code, as amended;
6. "Jueteng" and "Masiao" punished as illegal gambling under Presidential Decree No. 1602;
7. "Piracy on the High Seas" under the Revised Penal Code, as amended, and Presidential Decree No. 532:
8. "Qualified Theff" under Article 310 of the Revised Penal Code, as amended;
9. "Swindling" under Article 315 and "Other Forms of Swindling" under Article 316 of the Revised Penal Code, as amended:
10. "Smuggling" under Republic Act No. 455, and Republic Act No. 1937, As amended, otherwise known as the "Tariff and Customs Code of the Philippines";
11. Violations under Republic Act No. 8792, otherwise known as the "Electronic Commerce Act of 2000";
12. "Hijacking" and other violations under Republic Act No. 6235, Otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the Revised Penal Code, as amended;
13. "Terrorism" and "Conspiracy to Commit Terrorism" as defined and penalized under Sections 3 and 4 of Republic Act No 9372;
14. "Financing of Terrorism" under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of Republic Act No. 10168, otherwise known as the "Terrorism Financing Prevention and Suppression Act of 2012";
15. "Bribery" under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, and "Corruption of Public Officers" under Article 212 ofthe Revised Penal Code, as amended;
16. "Frauds and Illegal Exactions and Transactions" under Articles 213, 214, 215 and 216 of the Revised Penal Code, as amended;
17. "Malversation of Public Funds and Property" under Articles 217 and 222 of the Revised Penal Code, as amended;
18. "Forgeries" and "Counterfeiting" under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code, as amended;
19. Violations of Sections 4 to 6 of Republic Act No. 9208, otherwise known as the "Anti-Trafficking in Persons Act of 2003, as amended";
20. Violations of Sections 78 to 79 of Chapter IV of Presidential Decree No. 705, otherwise known as the "Revised Forestry Code of the Philippines, as amended",
21. Violations of Sections 86 to 106 of Chapter VI of Republic Act No. 8550, otherwise known as the "Philippine Fisheries Code of 1998";

22. Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the "Philippine Mining Act of 1995.;
23. Violations of Section 27(c), (e), (f), (g) and (i) of Republic Act No. 9147, otherwise known as the "Wildlife Resources Conservation and Protection Act";
24. Violations of Section 7(b) of Republic Act No. 9072, otherwise known as the "National Caves and Cave Resources Management Protection Act";
25. Violation of Republic Act No. 6539, otherwise known as the "Anti-Carnapping Act of 1972, as amended";
26. Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree "Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives";
27. Violation of Presidential Decree No. 1612, otherwise known as the "Anti- Fencing Law" ;
28. Violation of Section 6 of Republic Act No 8042, otherwise known as the "Migrant Workers and Overseas Filipinos Act of 7995, as amended;
29. Violation of Republic Act No. 8293, otherwise known as the "lntellectual Property Code of the Philippines, as amended';
30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the"Anti- Photo and Video Voyeurism Act of 2009";
31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the"Anti- Child Pornography Act of 2009";
32. Violations of Sections 5, 7, 8, 9, 10 (c), (d) and (e), 11, 12 and 14 of Republic Act No. 7610, otherwise known as the "Special Protection of Children Against Abuse, Exploitation and Discrimination",
33. Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the "Securities Regulation Code of 2000";
34. Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

In determining whether or not a felony or offense punishable under the penal laws of other countries is "of a similar nature"' as to constitute an unlawful activity under the AMLA, the nomenclature of said felony or offense need not be identical to any of the unlawful activities listed above.

III. DESCRIPTION of MONEY LAUNDERING and its STAGES

Money Laundering is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the Anti- Money Laundering Act, so that they appear to have originated from a legitimate source. Specifically, it covers all procedures to change, obscure or conceal the beneficial ownership or audit trail of illegally obtained money or valuables so that it appears to have originated from a legitimate source. It is also used to hide the link between those who finance terrorism and those who commit terrorist's acts.

Money Laundering covers all procedures to change, obscure or conceal the beneficial ownership or audit trail of illegally obtained money or valuables so that it appears to have originated from a legitimate source.

Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds shall be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts.

Terrorism can be funded from legitimate income.

3.1 STAGES OF MONEY LAUNDERING – the three (3) common stages of money laundering during which there may be numerous transactions made by launderers that could alert an insurance institution are:

1. Placement – This is the first and most vulnerable stage of money laundering. It is the physical disposal of cash proceeds derived from illegal activity. The aim is to remove cash from the location of acquisition to avoid detection. Owing to the nature of insurance contracts or policies, payment of premiums as well as settlement of insurance claims, and all other forms of insurance transactions, are presently no longer predominantly cash based, thus covered institutions are less likely to be used in the placement stage than other financial institution.

2. Layering – The second stage of the money laundering process. It involves moving funds around the financial system. It is the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. The business of insurance is most likely to be used at the second stage of money laundering, 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 cash in bank, from money in whatever form to an entirely different asset such as securities, investment contracts, pension, insurance policies, stock certificates, pre-need plans, bearer and other negotiable instruments.

Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or Reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions.

3. Integration – It is the final stage and the ultimate goal of money laundering. It is also the process at which the money is integrated into the legitimate economic and financial systems and is assimilated with all other assets in the system. Integration of laundered money into the economy is accomplished by making it appear to have been legally earned.

Thus, exceedingly difficult to distinguish between legal and illegal wealth. Insurance policies, particularly life insurance contracts, are treated not

only as protection and savings instruments, but also as investment contracts and as such, insurance transactions incorporate added attraction to the launderer in that the alternative asset is normally highly liquid.

The ability to liquidate investment portfolios containing both lawful and illicit proceeds, while concealing the criminal source of the latter, combined with the huge variety of investments and insurance products 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 insurance Institutions as instruments of money laundering.

IV. TERRORIST FINANCING

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering.Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations.

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking have played a role in moving terrorist funds. Transactions through informal banking are difficult to detect given the lack of documentation, their

size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex. (2014 FFIEC BSA/AML Examination Manual)

V. CUSTOMER/MEMBER -CLIENT IDENTIFICATION

As a regular part of the application process for insurance, Serviamus MBA, Inc. shall develop a systematic procedure for establishing the true and full identity of new individual customers/clients, and shall open and maintain the account/relationship only in the true and full name of the account/relationship owner/s. Unless otherwise stated, SMBA with average customer due diligence, shall gather from individual customers/clients, before or during the course of establishing the business relationship, the following minimum identification information and valid identification document.

5.1 INDIVIDUAL POLICYHOLDER

Must be an active member of Serviamus Foundation Inc., (SFI), staff and employee of the institution and other organized accredited groups. Only those applicant who can meet all of the requirements stated in the application form shall be eligible for membership.

1. Identification information:
   - ✓ Complete Name of customer/client/member
   - ✓ Date and Place of Birth
   - ✓ Sex
   - ✓ Address
   - ✓ Spouse Name
   - ✓ Nationality
   - ✓ Source of Income
   - ✓ Contact Number
   - ✓ Name, Address, Date & Place of Birth, Contact Number or Information, Sex, and Citizenship or Nationality of Beneficiary and/or Beneficial Owner, whenever applicable.
   - ✓ Specimen Signature

2. Identification Documents
   - ✓ Any ID with photo; or
   - ✓ Other identification document, as defined.

5.2 JURIDICAL PERSON

Serviamus MBA shall develop a systematic procedure for identifying customers/clients that are corporate, partnership and sole proprietorship entities, as well as their stockholders/ partners/ owners, directors, officers and authorized signatories. It shall open and maintain accounts only in the true and full name of the

entity. Unless otherwise stated, SMBA with average due diligence, shall obtain from their customers/clients that are juridical persons the following minimum identification information and documents before or during the course of establishing business relationships. Business or trade related transactions shall mean transactions of covered persons natural or juridical referred to below:

1. Banks, quasi-banks, trust entities, pawnshops, non-stock savings and loans associations, other non-bank financial institutions which under special laws are subject to BSP supervision and/or regulation, other persons and their subsidiaries and affiliates supervised or regulated by the Bangko Sentral ng Pilipinas (BSP);

2. Insurance companies, pre-need companies, insurance agents, insurance brokers, professional reinsurers, reinsurance brokers, holding companies, holding company systems, mutual benefits associations and all other persons and their subsidiaries and affiliates supervised or regulated by the Insurance Commission (IC);

3. Securities dealers, brokers, salesmen, investment houses and all other similar persons managing securities or rendering services as investment agent, advisor or consultant, mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities, and other entities administering or otherwise dealing in commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or properties supervised or regulated by the Securities and Exchange Commission (SEC);

4. Company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; and

5. Persons, including lawyers, accountants and other professionals, whoprovide any of the following services:

   a. Managing of client money, securities or other assets;
   b. Management of bank, savings or securities accounts;
   c. Organization of contributions for the creation, operation or management of companies; and

   d. Creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

Notwithstanding the foregoing, the term "covered persons" shall exclude lawyers and accountants acting as independent legal professionals in relation to information concerning their clients or where disclosure of information would compromise client confidences or the attorney-client relationship. Provided, that these lawyers and accountants are authorized to practice in the Philippines and shall continue to be subject to the provisions of their respective codes of conduct and/or professional responsibility or any of its amendments.

The following minimum information shall be required to be obtained from juridical person:

1. Customer Information
   - ✓ Complete Name of juridical person/s;
   - ✓ Name of Authorized Representative/Transactor/Signer
   - ✓ Name, Address, Date & Place of Birth, Contact Number or Information, Sex, and Citizenship or Nationality of Beneficiary and/or Beneficial Owner, whenever applicable.
   - ✓ Current Office address;
   - ✓ Contact numbers or information;
   - ✓ Source of Fund
   - ✓ Nature of business; and
   - ✓ Specimen signature of the Authorized Representative/Transactor/Signer

2. Identification Documents
   - ❖ Certificate of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, Certificate of Incorporation or Partnership issued by the Securities and Exchange Commission (SEC) for corporations and partnerships respectively, and by the BSP for money changers/foreign exchange dealers and remittance agents, and by the AMLC for covered persons;
   - ❖ Articles of Incorporation
   - ❖ Registration Data Sheet/Latest General Information Sheet
   - ❖ Secretary certificate citing the pertinent portion of the Board or Partners' resolution, authorizing the signatory to sign on behalf of the entity; and
   - ❖ For entities registered outside of the Philippines, similar documents and/or information shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

Approving Officers shall have the primary responsibility of requesting credit investigation on the business activity and validation of business registration documents to ensure that the entity has not been or in the process of being, dissolved, struck-off, wound up, terminated, or otherwise placed under receivership

or liquidation. In instances wherein, the bank officer is not comfortable and/or fully satisfied with the information provided, additional verification may be conducted by requesting credit investigation on business operations and authorized signatories of the company. Credit investigation is optional for companies listed in the Philippine Stock Exchange or in the Top 1000 Corporations in the Philippines.

If significant changes in the company structure or ownership occur subsequently or suspicions are aroused by change in the payment profile through a company account, further checks are to be made on the new owners.

Members shall be made aware of the Serviamus MBA, Inc.'s explicit policy that transactions will not be conducted with applicants in the event of failure to complete verification of any relevant subject or to obtain information on the purpose and intended nature of the business relationship, the Serviamus MBA, Inc. shall not conclude the insurance contract, perform the transaction, or shall terminate the business relationship. The Serviamus MBA, Inc. shall also consider making a suspicious transaction report to the Anti-Money Laundering Council.

5.3 Conducting the Interview and Establishing Identity

Usually done at the branch of Serviamus Foundation Incorporated (SFI), the Business Development Specialist (BDS) and/or MBA Staff: Orient/Briefs the prospective member client on the requirements and features of SFI loan product and services being applied and/or transaction being conducted.

1. Conducts an initial Interview and performs exploratory questioning to establish information pertaining to:
   - ✓ Personal circumstances
   - ✓ Purpose of micro-finance loan application or micro-insurance enrollment and/or transaction applied for
   - ✓ Nature of Business
   - ✓ Source of funds/source of wealth
   - ✓ Identification of Beneficiaries
   - ✓ Expected Transaction Amount
   - ✓ Expected Transaction Volume/Count
   - ✓ Reason for choosing SFI particularly when the residence of member client is outside the territorial jurisdiction of the concerned branch

2. Observes unusual behavior of member client during the conduct of interview and looks for the following warning signs:

- ❖ Member client has unusual or nervous demeanor
- ❖ Member client uses unusual or suspicious identification documents that cannot be readily verified.
- ❖ Member client is reluctant when establishing a new loan application, to provide complete information about the nature and purpose of its business, anticipated loan account activity, prior other MFI relationships, names of its officers and directors, or information on its business location.
- ❖ Member client home/business telephone is disconnected.
- ❖ Member client uses a temporary address.
- ❖ Customer's background differs from that which would be expected based on his or her business activities.
- ❖ A business or new member client asks to be exempted from reporting or record-keeping requirements.

3. Requests member client to produce the original documents of identity issued by an official authority bearing his photograph such as passport, driver's license, company identification cards, SSS card, GSIS card, Philhealth, DSWD, Voter's ID, and other valid IDs.
4. Examines carefully the documents of identity presented looking for any sign of erasures, alterations and tampering.
5. Interviews member client to validate information/data elicited during the initial interview and exploratory questioning against the presented identity documents.
6. Observes the following steps if the member client lacks the proper documents and/or results of the interview and exploratory questioning are poor.
7. Requests the member client to submit acceptable IDs before allowing the opening of the SFI loan product or micro-insurance enrollment or processing the transaction/service applied for if he lacks the proper documents.
8. Courteously decline the application for loan product application or micro-insurance enrollment and/or transaction –
   - ❖ if the member customer fails to satisfactorily explain discrepancies between the information elicited during the preliminary interview/questioning and documents presented
   - ❖ There are signs of erasures and tampering of documents presented.
   - ❖ Displayed suspicious and questionable behavior.
9. Requests member client to fill out microfinance loan application forms and micro-insurance enrollment form of SFI with photocopy of documents of identity presented if he/she satisfactorily meet the requirements and passed the initial interview and questions. Ensures that the forms are properly accomplished.
10. Determine the member client AML customer risk rating (i.e. Low Risk, Normal Risk, High Risk)
11. Forwards all documents to Business Development Officer/Branch Manager or Area Manager for review and approval.

5.4 Conducting Final Interview & Approval of Account

Done by the Business Development Officer (BDO) and or the Branch Manager. In the event there are doubts to the accuracy and completeness of member client information and document, conducts final interview of the member- client and validates information/data gathered against documents presented. Reviews the accuracy of data and completeness of opening documents.

1. Checks if the name of the customer, corporation including its incorporators and officers, and/or beneficial owners appears on the negative lists of known or suspected terrorists or terrorists' organizations available in AMLC and BSP website. In the event of "name match" print the result with date and time and refer to Area Head for guidance and subject to EDD. If upon further verification of the Area Head confirmed positive match, the transaction should not proceed. Responsible branch should submit STR within 48 hours to the designated AML and CTF Compliance Officer for endorsement to STR filing with the Executive Director of AMLC. The printed results shall be part of KYC and/or EDD documentation.

2. Courteously decline loan application and micro-insurance enrollment if the member client fails to satisfactorily meet requirements or pass the final interview and ensure if circumstances warrant, filing of a Suspicious transaction report.

3. For High Risk member client or customer secure approval from Senior Officer.

4. Branch Business Development Specialist or SMBA Staff approves processing of loan application and micro-insurance enrollment form if everything is in order. Then endorses the loan application and micro-insurance enrollment forms to appropriate authority.

5.5 Encoding AML/CIF Mandatory Information

The Accounting Staff Loan (ASL) and MBA Staff should ensure that all the mandatory information are encoded immediately upon micro-finance loan opening or micro-insurance enrollment.

5.6 Face-to-Face Contact

Prospective members of Serviamus Foundation Inc. (SFI) are interviewed personally. No micro-finance loan or micro-insurance account shall be opened and created without face-to-face contact and personal interview of SFI's duly authorized employee.

The use of Information and Communication Technology (ICT) in the conduct of face-to-face contact and interview may be allowed; provided, SFI is I possession of and has verified the identification documents submitted by the prospective member client prior to the interview and the entire procedure is documented.

SFI shall clearly define the instances when the conduct of face-to-face is reasonably practicable, depending on the product, type of business and risk involved, or when the use of ICT shall apply. Also, the covered person should adopt policies and procedures to address any specific risk associated with deferred or technology- aided face-to-face verification and personal interview.

5.7 Updating of Customer Identification Information and Documents based on Materiality and Risk

On-going Monitoring of Customers, Accounts and Transactions, branch and business units maintaining the accounts have to update the customer information and documents based on risk and materiality.

The updating of customer information and documents may be triggered by, but not limited to the following scenarios:

- ✓ Alerts from media and news
- ✓ An unusual activity was identified and EDD was conducted; and
- ✓ Upgrading and downgrading of member client AML Customer Risk Rating (CRR)

For customers with no updates, the branch shall certify in a call report to the effect that all information indicated in the CID file are current and updating is not needed.

However, where additional information cannot be obtained, or any information or document provided is false or falsified or result of the validation process is unsatisfactory, branch and business units shall deny business relationship with member client without prejudice to filing of STR with the AMLC, when circumstances warrant.

VI. Customer Acceptance Policy

It is the policy of SFI/SMBAI that no loan account or micro-insurance policy shall be opened or the transaction is cancelled if any of the following circumstances exists:

1. New member client account to be opened or transaction to be conducted is under anonymous or fictitious names.
2. Where the branch, unit or office is unable to verify the identity of the member client

3. Where the branch, unit or office is unable to obtain the required information and/or documents due to non-cooperation of the member client or non-reliability of the data or information furnished to TSPI or to the accredited Service Provider. In all cases, decision to close an account should be taken at the next higher level of authority.
4. Positive match vs. OFAC/SDN/Internal Negative File or with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available from BSP, AMLC Circulars, host country regulatory or enforcement agencies and other reputable/reliable sources.

6.1 Non-Discrimination Against Certain Types of Customer

SFI shall not decline any transaction from any customer/ member - client, such us PEPs, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny the person access to SFI products and services. However, all member client shall be subject to:

- ✓ Know Your Customer (KYC)
- ✓ Submission of valid IDs
- ✓ Customer Risk Rating
- ✓ OFAC and Other Watch list Validation
- ✓ Enhanced Due Diligence, if warranted.

And, the member client shall cooperate with TSPI in the submission of supporting document to determine the underlying trade or economic purpose of the transaction/s, if needed. And shall abide with the terms and conditions set by TSPI to its products and services.

6.2 Sharing of Customer/Member- client Information

SFI allows the sharing of information among its branches and offices when conducting Customer Due Diligence provided the needed information shall be requested by the designated Compliance AML and CTF Officer.

VII. RECORD KEEPING and RETENTION PERIOD

Serviamus MBA, Inc. shall prepare and maintain a record relative to its member relationships and transactions such that requirements of the Act are fully met. It shall retain all records as originals or in such forms as are admissible in court, pursuant to existing laws, such as the E-Commerce Act, and its implementing rules and regulations, and the applicable rules promulgated by the Supreme Court. SMBA

shall maintain transaction records sufficient to permit reconstruction of individual transactions so as to Provide, if necessary evidence for prosecution of money laundering, unlawful activity and terrorism financing. It shall ensure that all CDD

information and transaction records are available swiftly to the IC, AMLC and other competent authorities in the exercise of their official functions or upon appropriate authority.

Records/files maintained/stored in the work area or file room are orderly filed and arranged in filing cabinets or peerless boxes and under the custody of a duly designated custodian who is responsible for the safekeeping, control and accounting of all records and files of the division. Records/files are kept in storage areas which are fire resistant, well ventilated, well-lighted and free from dampness.

7.1 Period to Keep Records

Serviamus MBA shall maintain and safely store for five (5) years from the dates of transactions all customer records and transaction documents. lf a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5)-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality. Serviamus MBA shalt keep all records obtained through CDD, account files and business correspondence, and the results of any analysis undertaken, for at least five (5) years following the closure of account, termination of the business relationship or after the date of the occasional transaction. SMBA shall likewise keep the electronic copies of all covered and suspicious transaction reports for at least five (5) years from the dates of submission to the AMLC."

7.2 Accounts Reported as Suspicious and/or Subject to Court

Serviamus MBA ensures that suspicious accounts must be:

1. Safe keeps in a vault all records related to accounts reported as suspicious and/or subject of court action as follows:

   a. Duplicate copy of the Suspicious Transaction Report (STR)
   b. Original copy of all transaction records to support the STR
   c. Original copy of subject member account application forms,transaction forms including supporting documents
   d. All other communications related to subject transactions received from Management, AMLC and the courts.

2. Provides back-up copies of said files on electronic form, the custody of which shall be in accordance with the implementing guidelines under the Recovery Program.

3. Undertakes necessary measures to ensure the confidentiality of such files.

4. Ensures that said files are retained and safe kept beyond the period stipulated by the AMLA Implementing Rules and Regulations until it

5. is confirmed that the case has been finally resolved or terminated by the court.

6. Allows AMLC authorized officers and representatives full access to said
records.

7.3 Guidelines on Digitization of Member- Client Records

The organization shall develop and implement the Digitization of Member Client Record Program. All member client records and transaction documents shall be digitized in compliance with the AMLC issued AMLC Regulatory Issuance A, B and C No. 2 Series of 2018.

MIS Department must develop and install a program to auto-push the digitized customer records.

VIII. COVERED AND SUSPICIOUS TRANSACTIONS

Covered and Suspicious Reports shall be filed by Serviamus MBA in accordance with the registration and reporting guidelines of the AMLC.

Should a transaction be determined to be both a covered transaction and a suspicious transaction, it shall be reported by the SMBA as a suspicious transaction. In this regard, it shall be reported first as CTR, subject to updating if it is finally confirmed to be reportable as STR. CTRs shall be filed within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

Covered Transaction (CT) is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of FIVE HUNDRED THOUSAND PESOS (Php 500,000.00) within one (1) banking day. When the total amount of the premiums/fees for a policy, plan or agreement for the entire year, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), exceeds Five Hundred Thousand pesos (Php500,000.00), such amount shall be reported as a covered transaction, even if the amount of the amortizations are less than the threshold amount. The CTR shall be filed upon payment of the first premium/fee amount, regardless of the frequency of payment. Under this rule, CTR be file only once every year until the policy, plan or agreement matures or rescinded, whichever comes first. STRs shall be filed within the period prescribed under the registration and reporting guidelines of the AMLC. SMBA shall ensure the accuracy,

completeness and timeliness of covered and suspicious transaction reports, which shall be filed in such form as may be prescribed by the AMLC and shall be submitted in a secured manner to the AMLC in electronic form."

8.1 Certain Covered Transactions

The following are considered "non-cash, no/low risk covered transactions" the reporting of which to the AMLC are deferred per AMLC Resolution No. 10 dated Jan. 24, 2013.

1. For entities/units supervised by Securities and Exchange Commission (SEC)
   a. Transactions between banks and quasi-banks operating in the Philippines;
   b. Roll-over of client's investments or deposit substitutes;
   c. Transactions between parent bank and its subsidiary or associate financing company or affiliates;
   d. Payment of loan and/or its corresponding interest regardless of the manner of payment (cash/fund transfer, debit of account, check), provided that the grant of loan was previously reported as covered transaction;
   e. Loan repricing, loan renewal, loan restructuring, provided that there is no change in borrower's name, otherwise, the loan shall be considered as new loan, hence, reportable;
   f. Investment or Divestment of Mutual Funds;
   g. Internal operating expenses and capital expenditures of covered institutions (these are necessary expenses of covered institutions for the normal day-to-day running of a business. These are transactions of covered institutions and, therefore, not reportable. These may include payment of salaries, taxes, debt service, SSS premiums, Pag-IBIG contributions and employee's benefits).
   h. Adjusting entries or reclassification of accounts
   i. Service fees, proprietary revenue fees, arrangement fees, loan syndication fees and other form of fees incidental to loans granted or investments sold, provided that the loans granted or the sale of investment was reported at gross or at its principal amount.

2. For entities supervised by the Insurance Commission (IC)
   a. Transactions between domestic insurance companies/professional re-insurers/intermediaries licensed by the Insurance Commission;
   b. Renewal of non-life insurance policies under the same terms and conditions provided that a CTR has been previously filed;
   c. Automatic premium advance;
   d. Collection of premium payments from telemarketing, or direct marketing or through SMS and/or by way of salary deductions, where
   e. The bulk settlement exceeds P500,000.00 but the individual transactions are below the reporting threshold amount;
   f. Group life insurance and hospitalization insurance;
   g. Transaction of members of Mutual Benefit Associations pertaining to basic benefits;

h. Payment of loan and/or its corresponding interest regardless of the manner of payment, provided that the grant of loan was previously reported as covered all transaction;
i. Bulk settlement of claims on death and disability benefits of a policy where individual claim does not exceed P500,000.00;
j. Transactions coursed through brokers, agents and other intermediaries, in which case, however, the insurance company (principal) shall report the said transactions;
k. Internal operating and capital expenditures of covered institutions (these are necessary expenses of covered institutions for the normal day-to-day running of a business. These are transactions of covered institutions and, therefore, not reportable. These may include payment of salaries, taxes, debt service, SSS premiums, Pag-IBIG contributions and employee's benefits).
l. Adjusting entries or reclassification of accounts.

8.2 Suspicious Transaction Detection and Monitoring

Area Managers, Branch Managers, Business Development Officers, Business Development Specialist, Accounting Staff Bookkeepers and MBA staff:

1. Conducts due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the Branch knowledge of the member client's business and risk profile.

2. Upon receipt of information and confirmed knowledge, reviews, analyzes transactions processed based on the following sources of information/ data:

a. Transaction Report - Conducts due diligence on the business relationship and scrutiny of transactions. This is to ensure transactions conducted are consistent with the Branch knowledge of the member client's business and risk profile. Any unusual transaction observed must be immediately escalated to the Group Head and the designated AML and CTF Compliance Officer.
b. Source documents of transactions processed for the period.
c. Randomly checks if the name of member -client, corporation including its incorporators and officers, and/or beneficial owners appears of known or suspected terrorists or terrorist organizations made available by regulatory agencies or bodies such as the Anti-Money Laundering Council, Bangko Sentral Ng Pilipinas and Anti-
d. Money Laundering Council of any foreign government agency like the Office of Foreign Assets Control (OFAC).

The review process may be done by analyzing member-client's transactions within a specified rolling period of at least 90 days.

3. Notes down and examines the background and purpose of all complex, unusually large transactions and all unusual patterns of transaction. Validation with external parties may be conducted to determine source of funds, purpose and confirmation of client profile and relationship of the beneficiaries with the member- client.

4. Takes into account clues or early warnings signs or red flags to which member client and transactions warrant additional or extra attention.

5. If confirmed qualified for STR filing, prepares the Suspicious Transaction (STR) Report for submission to the Executive Director of the Anti-Money Laundering Council (AMLC).

8.3 Reporting Suspicious Transaction

Suspicious transactions (ST) are transactions with covered institutions, regardless of the amount involved, where any of the following circumstances exist:

1. There is no underlying legal or trade obligation, purpose or economic justification;
2. The member client is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the member client;
4. Taking into account all known circumstances, it may be perceived that the member client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA, as amended;
5. Any circumstance relating to the transaction which is observed to deviate from the profile of the member client and/or member client's past transactions with the covered institution;
6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense under the AMLA, as amended, 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.

Reporting of suspicious transactions to the Anti-Money Laundering Council (AMLC) shall be the responsibility of the designated AML and CTF Compliance Officer.

Transactions which, in the judgment of branches/offices other than the

maintaining branch, are deemed suspicious shall document and submit their findings to the branch maintaining the account for additional verification measures and/or reporting to the AMLC.

8.4 Process Flow in Filing Suspicious Transaction

Branch/ Support Unit

1. Investigate unusual transaction/s based on any of the trigger below or alerts/red flags
    a. Adverse News i.e. National, Local and Foreign
    b. Fraudulent Remittance
    c. AMLC Letter
    d. Court Orders (Freeze Order/Provisional Asset Preservation Order)
    e. Customer Complaint
    f. Presentation of fake KYC documents
    g. Attempt to defraud the organization

2. Gather sufficient information and perform the following:
    a. Know-Your-Client (KYC) Verification
        i. Verify if all mandatory information were obtained.
        ii. Validate the information provided in Member Client Loan Application Form or Micro-Insurance Enrollment Form if consistent with the submitted valid IDs.
        iii. Check if Customer Risk Rating (CRR) is appropriate. If CRR is High Risk, must be reviewed and approved by a Senior Officer

            "Senior Officer" shall refer to the next higher authority of the approving officer (Area Managers and the MFI Executive Director)

        iv. Assess deficiencies/lapses observed.
        v. Document observations and actions taken to address to issues.

3. Identification of Account with the organization
    a. Check the SFI Grameen System to identify the member- client Accounts with the organization.
    b. Get the following account details:
        i. Customer Identification number
        ii. Date opened
        iii. Total Debits with date range
        iv. Total Credits with date range
        v. Outstanding Balance and Status (as of date)
        vi. Maintaining Branch

c. Assess if total debits and credits indicated in the system are commensurate with the member client profile.
d. Document data/information gathered.

4. Analysis of Transactions

Assess total debits and credits if consistent with the profile of member- client.

a. Identify in the generated summary of transactions that warrants further review.
b. For closer scrutiny, do a year on year total debits/credits to determine the period that needs to be prioritized for review.

5. Other Documents and Other Non-Documentary Verification
   a. Verify name vs Internal Negative File and Google for any adverse findings.
   b. For Sole Proprietor and juridical persons, verify trade name with Department of Trade and Industry (DTI), Securities and Exchange Commission (SEC) and Bangko Sentral ng Pilipinas (BSP) list of Remittance Agents (RAs), if applicable.
   c. Request verification from Account Officer or Insurance Officer, Program Manager and Area Manager as necessary.
      i. Home and business address
      ii. Business activities
      iii. Business documents
      iv. IDs presented
   d. Conduct client visitation and document using the Call Report.

6. Other supporting documents, if any

7. Review completeness, accuracy of supporting documents and evaluate

8. Discuss, evaluate, deliberate and decide if "Filing or Not Filing of STR" for the reported transactions include the following details:
   a. Trigger of the review
   b. Account Name
   c. Reason for Filing/Not Filing based on AMLC Portal
   d. Case Description
   e. Amount of Debit/Credit with inclusive dates
   f. Branch/Unit
   g. Account Status
   h. Customer Information

1. Individual=Account name, place and date of birth, nationality, address, contact number, source of fund, nature of business, type of account, account number, date opened, outstanding balance, status and maintaining branch/unit

2. Juridical Persons=Account name, license, nature of business, address, contact number, source of fund/wealth, type of account, account number, date opened, outstanding balance, status and maintaining branch/unit, name of the authorized signatories, date and place of birth, address, source of fund, contact number, nationality, name of the beneficial owner, date and place of birth and address

8.5 Description of Transactions and STR Narrative

The reporting organization must strictly comply with the new reporting requirements as per new AMLC regulatory issuance (A) No. 1 Series of 2018 re: Amendments to the AMLC Registration and Reporting Guidelines (ARRG), Section 4 – Revision of Data Elements, which provides that time of transaction will be included in the CTR/STR format, effective October 30, 2018.

AML and CTF Compliance Officer Duties and Responsibilities

1. Evaluate and endorse filing a Suspicious Transaction Report/s (STR).
2. Provide a training program to branches on AML/CTF compliance awareness and give priority to high risk branches, if any to ensure effective implementation of the AML MTPP Program.
3. Coordinate with branches and provide necessary information pertaining to any AMLC queries and guide the branch on the necessary actions to take pursuant to the advisory from the Legal Group;
4. Coordinate with the branches to oversee its compliance with the AML law, rules and regulations, bank policies and procedures;

IX. TRAINING PROGRAMS for DIRECTORS, OFFICERS, and STAFF

It is mandated by Serviamus MBA that all its directors, officers and employees are informed and adequately trained in matters covered by the Money Laundering and Terrorist Financing Prevention Program to enable them to fully comply with their obligations and responsibilities under the AMLA as amended, its Revised Implementing Rules and Regulations, TF Suppression Act and its Implementing Rules and Regulations - AMLC, Bangko Sentral ng Pilipinas, Security and Exchange Commission and Insurance Commission Circulars, Letters, Memoranda.

Serviamus MBA shall develop, or create opportunities for, continuing education and training for its responsible directors, officers to promote AMLC/CTF awareness and strong compliance culture.

The education & training programs shall include relevant topics, such as:

a. Overview on MLTF, and the AMLA and TFPSA:
b. Roles of directors, officers and employees in ML/TF prevention;

c. Risk management:
d. Preventive measures:
e. Compliance with freeze, bank inquiry and asset preservation orders, and all Directives of the AMLC:
f. Cooperation with the AMLC and the lC: and
g. lnternational standards and best practices.

Attendance of SMBA directors, officers and employees in all education and training programs, whether internally or externally organized, shall be documented. Copies of AML/CTF continuing education and training programs, training certificates, attendance and materials shall be made available to the lC and the AMLC upon request. SMBA shall provide refresher programs, at least, every three (3) years. In cases where there are new developments brought about by new legislations, rules and regulations, and other lC and/or AMLC issuances, SMBA shall immediately cascade these information to its responsible directors, officers and employees; provided, that the cascading of the information is documented.

X. RECRUITMENT PROCEDURES OF EMPLOYEES

A. Recruitment and Selection

After determining the need for job position/s, this shall be made public through radio-television advertisements and posting of notices to schools or colleges within the city. Before one becomes an employee of SFI/SMBA, number of steps has to be taken. This is one way to help the management

decide whether to take the applicant in or not. It will also enable the applicant to weigh things out before making the final decision.

General Qualification Requirements for Applicants

The general qualification standards for applicants are as follows:

For Staff Position

Unless otherwise specified, an applicant must:

1. be of legal age, provided that he meets the requirements of the vacant position;

2. be a graduate/holder of a Bachelor's degree, preferably in Commerce, Business Administration, Economics, Accountancy, Computer Science, Social Work and other fields related to microfinance or micro-insurance, pass the Pre – Employment Examination. Likewise, he must take the Personality Test to determine suitability for the position;

3. not charged with and/or convicted of any criminal offense;

For Officer Position

As for officer position, depending on its organizational needs, may recruit highly qualified applicants for immediate appointment to officer position. To qualify for appointment to an officer position, an applicant must:

1. Be of legal age;

2. Be fit and proper for the position he is being appointed to. In determining whether a person is fit and proper for a particular position, integrity/probity, education/training and possession of competencies relevant to the function such as knowledge and experience, skills and diligence; and

3. Meet the other general qualification requirements mentioned above for staff position including the taking of exams for officer candidates.

General Steps to follow:

A.1 Submission of Documents

Upon application, the following documents should be submitted: Application Letter, Updated Resume, TOR and other credentials. Once hired, the following documents must be submitted: Authenticated Birth Certificate (photocopy), Baptismal Certificate (photocopy), Authenticated Marriage Certificate (photocopy) if applicable, Medical Certificate, Barangay and Police Clearance, NBI Clearance, Certificate of Employment (if any), 2x2 latest ID picture, TIN, Philhealth No., HDMF (Pag-ibig) and SSS Number.

A.2 Initial Interview

Upon submission of documents and filling up of SFI's official BIODATA Form, an applicant is initially interviewed by the person from HR Department. Result of this shall determine his/her going to the next level.

A.3 Pre-employment Examination

After evaluating the documents/data submitted and found to be favorable, applicant shall take the test which will be given by the HR supervisor or staff.

A.4 Psychological/Behavioral Tests

Passing the pre-employment examination means that applicant is qualified to take the psychological/behavioral test. This is battery of tests administered by a professional. SFI has made a tie-up with psychologists/guidance counselor who shall conduct and evaluate the result of the tests given. The main purpose of the activity is to help find the "FIT" between the applicant and the job applied for. Feed backing between the psychologist and the HR supervisor will follow.

A.5 Final Interview

Results of the two tests shall be evaluated and recommendations are made as to who shall qualify for this step. Successful applicants submit themselves to interview conducted by the panel composed of the HR supervisor, Branch Manager, Business Development Officer, and Business Development Staff or representative from a position which the institution needs to fill in. The panel shall then make recommendations to the Executive Director on who will be due for the next step.

A.6 Background Checking

This is required and will be done by the Audit section and/or HR staff to have a firsthand information regarding the character of the applicant from their neighborhood, previous employers and previous schools. This is part of a careful hiring and confirmation of what the applicant has written in their resume.

A.7 Orientation

Applicant/s who passed the final interview and background checking shall be given a three-day orientation. Vision, Mission, core Values of SFI; history and business of the organization will be discussed. Grameen banking methodology is introduced as well as the pertinent documents that are essential in conducting center meetings and processing of members 'loans. In addition, new products are also introduced like individual loan, micro-agri loan, business asset loan, Diocesan Employees Assistance Loan (DEAL) and its micro-insurance.

A.8 Exposure Period

After the orientation, prospective staff shall be assigned to a particular branch. For a period of two weeks, he/she will be allowed to go with a regular staff of SFI to the different areas or centers. This will enable him/her to observe and have a firsthand experience on what the job entails. It also aims to foster camaraderie between the new entrant and the rest of the employees as well as the members of the institution.

At the end of two weeks, feed backing session shall take place between the applicant/s and identified SFI officers. This is the time where prospective staff report experiences, expectations and learnings. It is also the time where commitment from the prospective staff is expressed.

B. Appointment

Before an official appointment shall be given to the prospective staff, he must comply all the required documents (as stated in A.1), the employment contract covers what is expected to do from the employee. Terms and conditions stipulated in the contract will be fully explained and discussed by the HR Supervisor to the employee. The employment paper states the nature of employment with the institution.

Internal Hiring

Whenever a job is declared vacant and open for manpower hiring, employees who maybe interest and who believe they possess the qualifications sought for that position, may express their intentions in writing to the HR officer. Nonetheless, it does not limit the authority of management to appoint whoever they see possesses the competencies and qualifications for the position.

Internal transfer may be affected as the organization's management may see fit.

XI. INTERNAL AUDIT SYSTEM

To test compliance with the Serviamus MBA's internal policies, procedures and controls, an audit function shall be in place. It is important that the audit function is independent and adequately resourced. Internal Audit unit of SMBA is through SFI.

11.1 Internal Audit Function

The internal audit function associated with money laundering and terrorist financing 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 direct reporting line to the Board or to a board level Audit Committee.

11.2 Risk Based Work Program

Internal Audit Unit shall develop an AML Risk-Based Work Program for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms and policies and procedures related to customer identification process, suspicious transaction reporting and record keeping and retention, the effectiveness of the employee's execution of the controls, the adequacy

and effectiveness of the compliance oversight and quality controls, and the effectiveness of the training as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing and management's ability to implement effective risk-based due diligence, monitoring, and reporting systems. Audits should be properly scoped to evaluate the effectiveness of the program and should proactively follow up on their findings and recommendations.

11.3 Compliance Testing and Review

The Compliance Office may be tasked to conduct periodic review and assessment of a unit's compliance on applicable rules and regulations including anti-money laundering and terrorist financing rules and regulations as well as to test the appropriateness/reliability of existing processes and adequacy of controls to mitigate the risks.

Annually, the Compliance Office shall conduct an overall compliance and control environment including AML-CFT area to identify high risk areas to which unit/branch are most likely be exposed to money laundering and terrorist financing risk. If there is identified high risk unit/branch, Compliance Officer may conduct compliance testing to determine additional AML/CTF mitigating controls required that must be implemented and submit compliance review results to the Board Audit and Compliance Committee.

Compliance Testing and Review Manual

Compliance Office shall develop a Compliance Testing & Review Manual which incorporates compliance review program for AML and CTF Framework and AML system.

The result of the overall assessment of the AML and CTF compliance review conducted by Compliance Office shall adopt a Certification Risk Rating.

5 components of AML Compliance Risk:

1. Board and Senior Management Oversight – reflects the efficiency and capability of the unit/entity to escalate to Board/Senior Management money laundering/terrorist financing issues and concerns as well as resolution of findings/exceptions noted by the internal/external auditors and regulators.

2. Policies and Procedures – reflects the unit's/entity's adequacy of AML/CFT policies and procedures vis-à-vis Philippine/host-country laws and regulations, adequacy of access to MTPP, AML and CTF Policy Guidelines.

3. Internal control and MIS – reflect adequacy and soundness of the monitoring and compliance testing conducted by the AML and CTF

4. Compliance Officer to identify, measure, monitor and control money laundering risks as well as compliance with the Philippine AML laws and regulations.

5. Implementation – reflects the level of effectiveness in the implementation of the MTPP which include customer acceptance and identification, covered and suspicious transaction reporting, transaction monitoring, record-keeping and retention.

6. Training – reflects the level of awareness and understanding of Branch /entity's personnel to AML laws, rules, regulations, policies and procedures.

Monitoring of all Deficiencies noted during the Audit and External Independent Reviews or Regulatory Body Examination

11.4 Internal Audit Examination Report

Internal Audit has the responsibility to follow-up and determine whether or not the auditee/s has taken steps to adequately, effectively and timely address the matters reported in the audit findings/recommendations. Internal Audit therefore monitors on a monthly basis the status of corrective actions implemented on outstanding/open issues/recommendations until fully resolved. However, the implementation of corrective actions in a timely manner is the shared and direct responsibility of line management including the Group Head.

11.5 Regulatory Body Regular and/or Special Examination

Compliance Monitoring of Report of Examination (ROE) Findings/Recommendations

Compliance Office shall monitor external audit findings and recommendations and the preventive corrective action plans taken by the business units to close all issues/comments. Results of which are reported to the President, Executive Director, Senior Management and to the Board Audit and Compliance Committee periodically.

All critical issues must be escalated to concerned Group Head of the business unit for immediate appropriate action. Initial findings and comments including resolutions, corrective actions and commitment dates are presented to Senior Management, President, Executive Director and Board Audit and Compliance Committee.

11.6 External Auditor and Examination Report Compliance Monitoring

It is important to monitor timely release of the external auditor reports related to independent assessment of the AML practices of the bank.

Compliance Monitoring Open Items Report shall be prepared by the Compliance Office and provided to the President, Executive Director and concerned Group Head/s on a monthly basis summarizing the closed issues/comments and highlighting the open items for appropriate action until all issues are closed. Recurring items and unresolved open items shall be reported to the Board Audit and Compliance Committee.

11.7 AML and CTF Compliance Review

AML Compliance Review of offices/units which were assessed at least "Needs Improvement" or "Less than Satisfactory" and below or "High Risk" by External Auditors and Internal Audit may be subjected to AML and CTF Compliance Review to support line management in addressing the risk and sustaining corrective actions.

The report of the review indicates the period when the review commenced and ended, period covered, objective, methodology, observations, recommendations, actions taken or to be taken and conclusion/overall assessment. A memo addressed to the Head of Office shall be prepared by the Compliance Office with copy to the President, Executive Director and Senior Management. Moreover, an Open Item Tracking Report is prepared shall be submitted to the Board Audit and Compliance Committee periodically to effectively manage the actions being required from business and operating units/branches on findings or observations.

11.8 AML Compliance Certification Process

The Compliance Office shall develop the AML Compliance Certification patterned after the BSP-AML Risk Rating System (ARRS) issued on April 4, 2012 under BSP Memorandum No. M-2012-017 and intended to maintain a thorough understanding of the organization's level of AML compliance thru self-assessment.

Under the AML Compliance Certification, the organization shall undergo an AML and CFT self-assessment on the 5 components of AML Compliance Risk. The component factors are as follows:

1. Board and Senior Management Oversight – the rating reflects the efficiency and capability of the unit to escalate to Senior Management money laundering/terrorist financing issues and concerns as well as resolution of findings/exceptions noted by the internal/external auditors and regulators.

2. Policies and Procedures – the rating reflects line management adequacy of access to AML and CTF policies and procedures, MTPP and interim AMLCFT Policy Guidelines.

3. Internal Control and MIS – the rating reflects the adequacy and soundness of the monitoring and compliance testing and reviews to identify, measure, monitor and control money laundering risks as well as compliance with the AMLA, its IRR and rules and regulations issued by BSP, SEC and IC;

4. Implementation – the rating reflects the level of effectiveness in the implementation of the MTPP which include customer acceptance and identification, covered and suspicious transaction reporting, record-keeping and retention and updating of customer records, among others;

5. Training – the rating reflects the level of awareness and understanding of employees' personnel to AML and CTF laws, rules, regulations, policies and procedures.

Composite rating is assigned based on a 1 to 4 numerical scale. The highest rating of 4 indicates the strongest risk management system and most effective operational practices that entail the least degree of supervision. The lowest rating of 1 on the other hand signifies the weakest risk management system and defective implementation which requires the highest degree of management concern.

The Composite Ratings are defined as follows:

RATING	DESCRIPTION
4	Sound. High level of effectiveness. All or mostly 4 with no sub-component rating less than 3
3	Adequately Sound. Acceptable level of effectiveness. All or mostly 3 but no sub-component rating of 2
2	Vulnerable. Implementation needs improvement. All 2 and no sub-component rating of 1
1	Grossly inadequate. Poor implementation. All or mostly 1

11.9 Cooperation with Regulatory Bodies and Examination Teams

All officers and employees shall provide full cooperation and support during examination conducted by regulatory bodies and government agencies' examination teams (i.e., AMLC, SEC, IC).

11.10 Cooperation with the AMLC

Anti-Money Laundering Council Documentary Requirements for Individuals & Entities subject of a CTR and/or STR

The covered transaction report (CTR) and the suspicious transaction report (STR) files, if any, submitted to the AMLC may trigger the council to require presentation of customer KYC documents and copies of customer IDs. Upon receipt of the AMLC letter, Compliance Office and Legal Counsel shall forward the same to maintaining business unit concerned for the requested customer documents. Once completed, Compliance Office shall obtain legal clearance prior to submission to AMLC. Compliance Office shall ensure delivery of the letter with the required documents within the deadline set by AMLC.

11.11 Penalties for Violation of the AMLA and TF Suppression Act

Failure to adhere to this Manual may subject SMBA employees to disciplinary action up to the extent of termination of employment. Penalties for money laundering and terrorist financing can be severe. Under the Philippine AML Law RA 9160 as amended, a person convicted of money laundering can face up to 14 years in prison and a fine of up to P3, 000,000 or twice the amount of the property involved. Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as client equity, member collateral, personal property, and, under certain conditions, entire member client accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. In addition, SFI risk losing their charters and/or licenses, and employees risk being subjected to AML criminal investigation.

11.12 Rules on the Imposition of Administrative Sanctions under republic Act No. 9160, as amended

The AMLC shall, at its discretion, impose administrative sanctions upon any covered person for the violation of the AMLA and its RIRR, or for failure or refusal to comply with the orders, resolutions and other issuances of the AMLC.

Fines shall be in amounts as may be determined by the AMLC to be appropriate, which shall not be more than Five Hundred Thousand Pesos (Php500,000) per violation. In no case shall the aggregate fine exceed five percent (5%) of the asset size of the respondent.

Fines – The following are the fines (in Philippine Peso) per violation based on the entity size and gravity of violations:

VIOLATIONS	MICRO	SMALL	MEDIUM	A (LARGE)	B (LARGE)
Grave	50,000	125,000	250,000	375,000	500,000
Major	30,000	75,000	150,000	225,000	300,000
Serious	20,000	50,000	100,000	150,000	200,000
Less Serous	10,000	25,000	50,000	75,000	100,000
Light	5,000	12,500	25,000	37,500	50,000

11.13 Your Protection under AMLA

When reporting covered or suspicious transactions to the Anti-Money Laundering Council (AMLC), the organization and its officers and employees shall not be deemed to have violated R.A. No. 1405, as amended, (Bank Secrecy Law) R.A. No. 6426, as amended, (FCDU Law), R.A. No. 8791 (General Banking Law), and other related laws (BSP 706 subsection X807.5 – Exemption from Bank Secrecy Laws).

No administrative, criminal or civil proceedings shall be imposed against any person for having made a covered or a suspicious transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in

any criminal prosecution under this Act or any other law (RIRR Rule 9c.3. – Safe Harbor Provisions).

11.14 Notice to Member -Clients for AMLA Requirements

In compliance with SEC Circular Memo No. 2 dated May 20, 2010, the following NOTICE TO CLIENTS FOR AMLA REQUIREMENT ON THE SUBMISSION OF SUPPORTING DOCUMENTS shall be posted in the conspicuous area of the branch.

The notice shall be as follows:

"To help the government fight money laundering activities, the Anti-Money Laundering Act, as amended, requires all covered institutions to obtain, verify and record information that identifies each person who opens an account.

In this regard, the organization shall obtain information such as name, address, date of birth, business, TIN, SSS or GSIS Nos. and presentation of acceptable valid IDs or other competent evidence of identity bearing your photograph and signature when you transact with us."

XII. RISK ASSESSMENT and MANAGEMENT POLICIES and PRACTICES OF THE ORGANIZATION

12.1 SFI Risk Assessment and Management

It is the responsibility of organizations registered with the Securities and Exchange Commission and the Insurance Commission to conduct AML risk assessment of customers, products, services, delivery channels and geographical locations to understand its risk exposure to money laundering and terrorism financing risks.

It is recommended that SFI take into consideration the results of the National Risk Assessment on the Money Laundering and Terrorist Financing in the risk assessment process and in implementing risk-based measures to manage and mitigate identified risks.

The ML-TF risk assessment methodology to be adapted must be appropriate to the nature of operations. Under Republic Act 10693, Micro-finance Act - MFI's are considered partners of the government in providing simple micro-finance credit, savings and micro-insurance products to the poor society. At the minimum, all member clients are enrolled with proper KYC documentation, customer verification and regular monitoring of the low ticket size transactions. On a regular basis, SFI shall monitor the various risks that could directly impact the quality of implementation of SFI Money Laundering and Terrorism Financing Prevention Program.

SFI Risk Assessment shall be conducted at least every two (2) years, or as often as the board or senior management, the AMLC or government bodies and government agencies may direct and aligned with new AML/CFT developments that may impact the operations.

12.2 SFI Risk Assessment Results

OVERALL ASSESSMENT: (RESIDUAL RISK –VERY LOW)

In 2018-2019, the Philippines faced major threats of money laundering (ML) and terrorism financing (TF) per the AMLC National Risk Assessment Report which identified predicate crimes with HIGH threat level such as drug trafficking, terrorism, graft and corruption, investment scams, smuggling and MEDIUM threat level web related crimes and illegal trafficking of persons.

SFI has no exposure to HIGH and MEDIUM risks crimes stated above. SFI shall continue to conduct effective member- client on-boarding and manual monitoring review of transactions to deter AML and CTF risks.

SFI shall adopt an AML and CTF risk and control framework suited to the pro-life of its target market, for its simple micro-finance and micro-insurance products and services and non-complex nature of the organization's activities. The

Board and Management Oversight are adequate. Internal control and internal audit shall be further enhanced to sustain satisfactory AML and CTF awareness and practices.

A. Threat Level of National Risk Assessment (NRA) identified Predicate Crimes

Below are the predicate crimes identified in the 2nd Philippine National Risk Assessment pose HIGH and MEDIUM threat levels of money laundering and terrorism financing for the Philippines.

NRA Predicate Crimes	Threat Level
1. Illegal drugs related crimes	High
2. Terrorism	High
3. Investment scams and estafa	High
4. Smuggling	High
5. Tax crimes	High
6. Illegal manufacture and possession of firearms, ammunitions and explosives	High
7. Violation of intellectual property rights	High
8. Violation of environmental laws	High

9. Web related cimes	Medium
10. Illegal trafficking of persons	Medium
11. Kidnapping for ransom	Medium

B. Products, Services and Delivery Channels Vulnerable to ML-TF

After considering the inherent risk and mitigating controls for the SFI products, services and delivery channels, below are the 5 products, services and delivery channels vulnerable to ML and TF risks:

1. MFI Loan Products- (Inherent risk-LOW). SFI Loan Products are designed as livelihood assistance program that provides group collateral-few loans as low as P2,000 up to a maximum of P300,000. SFI loan collections and payment of premium of the micro-insurance products provide payment terms of weekly contributions. Member clients are about 90% women micro-entrepreneurs engaged in vending essential food and consumer products, fruits, vegetable, fish and meat vendors and owner of small sari-sari stores or mini groceries. There is a small percentage of farmers, fisher folks and indigenous people among its member clients. Purpose and use of MFI loans are defined as financial assistance in the form of working capital for the livelihood programs of member -clients.

About 50% of the member client base are beneficiaries of the DSWD Pantawid Pamilyang Pilipino Program (4Ps). Given its well-defined target market to serve the less privileged sector of Philippine society in partnership with government, residual risk is VERY LOW.

2. Micro-insurance Products (Inherent Risk-LOW) – SMBA micro-insurance products premium range as low as P1,500 per annum for the Basic Life Insurance Policy (BLIP). Inherent risk is mitigated due to observance of KYC, customer acceptance and identification and on-going monitoring of transactions. Customers include SFI employees, member- clients and the immediate families. The micro-insurance products and services help cushion adverse effects of Hospitalization, disability or death members and members of the family. Hence, residual risk is VERY LOW.

12.3 SMBA Risk Assessment Methodology

SMBA shall conduct AML risk assessment at least every two years to assist in identifying the organization's AML risk profile. Understanding the risk profile enables the organization to apply appropriate risk management processes to the AML and CTF compliance program to mitigate risks. The risk assessment process enables the Board and Senior Management to have a clear understanding of identified gaps in the existing mitigating controls and the corrective actions implemented. The risk assessment provides a comprehensive analysis of the AML and CTF risks in a concise and organized manner.

The development of the AML risk assessment involves two steps. First is to identify the specific risk categories (i.e. product as to services, customers, entities, transactions, and geographic locations) unique to the organization; and second, is to conduct a more detailed analysis of the data gathered as basis for the risk assessment within certain categories.

The organization has adapted a methodology generally used by financial institutions towards a risk-based approach in AML risk assessment. The risk-based approach involved identifying and categorizing money laundering risks and establishing reasonable controls based on risk identified. Using the risk-based approach, the organization is able to determine potential money laundering and terrorist financing risk and to exercise reasonable business judgment in the formulation of policies and procedures that will effectively manage servicing of its member clients.

The AML risk-assessment process covers the following steps:

1. Identify specific risk categories. This includes the organization's services, customers/member clients, entities, channels, transactions and geographic locations.
2. Conduct a more detailed analysis of the data gathered for at least 12 months as basis for the assessment of risk within the categories and determines the residual risk, the related mitigating factors and management of such risks.
3. Use retrospective and quantitative techniques in risk assessment or combination. Historical data in risk assessment has the benefit of drawing on data from past events to help anticipate future problems. Although the past is not always a reliable indicator of the future, consistent patterns can be used to analyze data associated with AML and/or CTF suspicious transactions, if any. To enhance the review and analysis, the number and volume of transactions, the nature of the customer relationships are considered in the risk assessment.

12.4 AML Risk Rating Methodology

It is the policy of the organization to conduct risk assessment of its member-clients during micro-finance loan application and micro-insurance enrollment. This is to ensure the organization can properly identify, evaluate and estimate the levels of AML risk involved in the transaction and determine acceptable level of risk, appropriate monitoring controls to detect and report suspicious transaction in a timely manner.

When to conduct Customer Risk Rating

Customer Risk Rating is assigned to member clients at account application or account enrollment stage based on several components considered including the documentary and non-documentary evidence in knowing/identifying the customer and subject to periodic review pursuant to the provisions hereof.

I. Risk Rating Classification

After identifying, evaluating and estimating the levels of risk that a member client is likely to engage in money laundering or terrorist financing, customers are classified as follows:

Low Risk – member client or customer pose a minor risk compared to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities and is an ideal level of risk;

Normal Risk – member client or customer does not pose a significant risk compared to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities and is an acceptable level of risk;

High Risk – member client or customer pose a major risk comparable to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities although within tolerable level of risk, but subject to enhanced monitoring.

II. Periodic Risk Assessment

After the initial risk rating is assigned to each member client, customer risk rating shall be periodically undertaken by the branch as follows:

Low risk - At least every 36 months
Normal risk - At least every 24months
High risk - At least every 12 months

The designated AML and CTF Compliance Officer, whenever necessary, may trigger the periodic review.

Risk rating may be conducted as frequent as necessary when adverse information or knowledge relating to an account is acquired by the branch that, based on reasonable judgment, will warrant the accelerated re-assessment of the said member client.

The member client or customer's initial or current risk rating can be affected by a change in circumstances as well as the unusual transactions monitoring results. Therefore, customer risk rating may change over time.

III. Basic Risk Parameters

The risk parameters are generally classified into 3 categories, namely:

a. Account/Entity Risk - specific risk associated with the member client's type, nature of business, occupation or declared/anticipated transaction activity.
b. Geographic Risk - specific risk associated with doing business in, granting microfinance loans or micro-insurance enrollment for member clients from a certain province or region, or facilitating transactions involving certain geographic locations.
c. Products, Services, Transactions and Delivery Channel Risk - risk associated with the nature of specific microfinance and micro-insurance products or services offered that can facilitate a higher degree of anonymity or involve the handling of high volume of currency or currency equivalent or instantaneous transfer of funds from one account to another account for deposit or withdrawals.

1. Account/Entity Risk

Existing and potential member clients and entities are categorized and described as follows:

a. Individual. Natural person who is a Filipino citizen who is granted SFI microfinance loan products (RL. MPL, HSL, AGRI Loan, BAL, Education Loan) and provided with social development services.
b. Individual Natural person who is a Filipino citizen enrolled in micro-insurance products (BLIP) and avails of the social services provided by the organization.
c. Juridical. Corporation, partnership, association that may infuse funds in the form of donations or grants to the organization.
d. Philippine Government Agency or Instrumentality. A government owned or controlled corporation (GOCC), local government unit, agency, police, military, judiciary or legislative.
e. Non-Governmental Organization/Non-Profit Organization/Foundation or religious
f. Organization shall refer to a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".
g. Remittance Agent. A natural person or entity that offers to remit, transfer or transmit money on behalf of any person and/or entity. These include money or cash couriers, money transmission agents, remittance companies and the like.

h. Designated Non-Financial Business and Profession (DNFBP)
   i. Company service providers.
   ii. Persons, including lawyers and accountant, who provide any of the following services:
      1. Managing client money, securities and other assets;
      2. Management of bank, savings, securities or accounts
      3. Organization of contributions for the creation, operation, or management of companies; and
      4. Creation, operation or management of juridical persons or arrangement, and buying and selling business entities.

i. Politically Exposed Person (PEP). An individual who is or has been entrusted with prominent public positions in the Philippines or in a foreign state including heads of state or of government, senior politicians, senior national or local government, judicial or military officials, senior executives of government or state owned or controlled corporations, important political party officials, their immediate family and close associates.

2. Geography Risk

Geography includes the geographic location of the branch, the geographic regions of the member clients' customer base.

High Risk Philippine areas due to reported cases of kidnapping and concerns related to peace and order situation with a perception of terrorist financing, cybercrime activities, New People's Army (NPA) rebel areas,Islamic extremists' activities, and presence of alleged narco-politicians based on the intelligence information from law enforcement agencies.

3. Products, Services and Delivery Channel Risk

IV. Default Risk Classification of Select Member Client Accounts

Regardless of the result of the Customer Risk Rating, the following are considered HIGH RISK and shall be subject to Enhanced Due Diligence and require appropriate Senior Officer, Management Committee or Board Committee approval:

Enhanced Due Diligence Review must be performed by designated AML and CTF Compliance Officer to ensure transactions have legal purpose or economic reasons and loan proceeds is consistent with its intended purpose of individuals classified as

Politically Exposed Persons, Close Relationships and Associates such as the following local government officials which are known to have close relationships with prominent PEPs.

- ✓ Barangay Chairman
- ✓ Kagawads
- ✓ LGU staff

"Senior Officer" shall refer to the next higher authority of the approving officer (i.e., Area Heads, and the Executive Director).

Risk Factor Numeric Weight

RATING	Weight
Low Risk	1
Normal Risk	2
High Risk	3

Individual:

RISK FACTOR	REMARKS
Classification of Person >If risk rating is 3 (High Risk), CRR shall be authomatically tagged as High	Classified as follows: 1. Individual is Filipino 2. Individual person acting as collecting agent 3. Has relationship with prominent PEPs, its immediate family members, close relationships and close associates
Citizenship > If risk rating is 3 (High Risk), CRR shall authomatically tagged as High	Classified as follows: 1. Resident Filipino Citizen 2. Non-resident Filipino Citizen 3. Filipino Citizen with affiliation with entities operating with no legitimate business or economic reason
Geographical Address > If permanent or present address is included in the FATF Identified Jurisdiction with AML/CFT Deficiencies risk	Classified as follows: 1. Permanent or present address is within the vicinity of branch area and known to branch personnel and properly identified thru KYC documents.

rating is 3 (High Risk), CRR shall authomatically tagged as High	2. Permanent or present address is not falling under any of the High Risk Philippine Areas or outside the branch vicinity 3. Is within the High Risk Philippine Areas and outside the branch or outside Philippines address
Individual Identification	Classified as follows: 1. Use of primary and secondary photo-bearing Philippine Government issued IDs 2. Use of primary or secondary photo-bearing Philippine Government issued IDs 3. Use of Foreign government photo-bearing issued ID
Occupation/Nature of work or self-employment	Classified as follows: 1. Employed locally; retired employee;pensioner, OFW; beneficiary of an OFW 2. Student; self-employed or unemployed with spouse income 3. Unemployed but income is not derived from spouse or immediate family member
Source of funds	Classified as follows: 1. Salary-income from employment/professional fees; Property-rent, sale of property, inheritance; Pension-retirement fund; Financial products-Insurance proceeds, investment 2. Allotment-medical,remittances; business-income from legal business; commission-agent or sales percentage 3. Donations-contribution,aids, tithes church collection, stipend; gamings-winnings
Account opening method: SFI Loan Application and SMBA Application Form	Classified as follows: 1. Face-to-face with client member borrowers and SMBA applicants 2. Face-to-face with some member client member borrowers and SMBA applicants but authenticated by maintaining account at branch level
Length of being a member	Classified as follows: 1. Less than a year of being a member 2. 1 year a member 3. New member and no prior records

Product & Services Transactions	Classified as follows: 1. SFI Loan Products - 1 2. SMBA Insurance- 1 3. Interbranch Cash payment - 3

Non-Individual

RISK FACTOR	REMARKS
A. Designated Authorized signatories	Classified as follows: A. Citizenship B. Resident Filipino Citizen C. Non-Resident Filipino Citizen D. Resident and Non-resident E. Filipino affiliated with prominent PEP F. Individual Identification: G. Use of primary and secondary H. photo-bearing Philippine Gov't. issued IDs I. Use of primary or secondary J. photo-bearing Philippine K. Government issued IDs L. Use of Foreign government M. photo-bearing issued ID N. Risk classification of person O. Individuals other than those listed as designated professionals P. Designated professionals Q. PEP and its immediate family members and close associates
Nature of Business > If risk rating is 3 (High Risk), CRR shall authomatically tagged as High	Classified as follows: 1. Simple micro business 2. With exposure to complex business 3. Linked to high risk business
Place Incorporation and Registration > If risk rating is 3 (High Risk), CRR shall authomatically tagged as High	Classified as follows: 1. Incorporated and registered in the Phils. 2. Incorporated and Registered outside the Phils. but country is not listed in FATF list 3. Incorporated and Registered outside the Phils. and country is not listed in FATF listwith highest impact of terrorism
Corporate Address > If permanent or present address is included in the FATF Identified Jurisdiction with	Classified as follows: 1. Permanent or present address is within the vicinity of branch area and known to branch personnel and properly identified thru KYC

AML/CFT Deficiencies risk rating is 3 (High Risk), CRR shall authomatically tagged as High	documents. 2. Permanent or present address is not falling under any of the High Risk Philippine Areas or outside the branch vicinity 3. Is within the High Risk Philippine Areas and outside the branch or outside Philippines address
Organization Documets	Classified as follows: 1. Use of Phil. issued registration/incorporation documents 2. Use of non-Philippine incorporation registration documents duly authenticated by the Office of the Phil. Consulate 3. Use of registration documents as a remittance agent

Customer Risk Rating Range

Customer Risk Rating Total (CRRT) refers to the overall result when all the Risk Factors are summed up according to each of their relative numeric weights. The risk rating range is as follows:

RATING	Range
Low Risk	25 or less
Normal Risk	226-35
High Risk	336 or higher

SMBA member clients are classified "LOW RISK" unless there is confirmed information that will require higher numeric range to classify as "NORMAL RISK" or will automatically qualify tagging the member client as "HIGH RISK."

a. Individual - this CRR tool is used for individuals when opening and during periodic risk assessment of Microfinance Loans and Micro-insurance applications

b. Non-Individual – this CRR tool is used to non-individuals entering into third party service provider business relationships with TSPI.

Customer Risk Rating Tagging of Member Client

Tagging shall be performed by the designated branch personnel and approved by the authorized bank officer/s only. Random Day 2 validation of customer information encoded in the system vis-a-vis properly accomplished

forms and identification documents is necessary to ensure customer data integrity in the system.

The customer risk ratings are subject to periodic reviews based on defined "cycles" for high risk, normal risk and low risk customers.

A. SMBA Employees - All new and existing employees of SMBA are classified "LOW RISK". However, if SMBA employee has been a subject of investigation related to internal fraud or AML related financial crimes, account should be classified "HIGH RISK."

B. Remittance Agent - shall refer to persons or entities that offer to remit, transfer or transmit money on behalf of any person to another person and/or entity. These include money or cash couriers, money transmission agents, remittance companies and the like (Subsection 4511N.1 of MORNBFI). Remittance Agents are generally HIGH RISK.

C. Pawnshop Business shall refer to the business of lending money on personal property that is physically delivered to the control and possession of the pawnshop operator as loan collateral. (BSP Circular No. 938). Pawnshop Business are generally "HIGH RISK."

D. Pawnshop with MSB License shall refer to the business of lending money on personal property that is physically delivered to the control and possession of the pawnshop operator as loan collateral with BSP registered corollary business activities including remittance operations. (Circular No. 938) Pawnshop with MSB License are generally "HIGH RISK".

<u>Persons Ultimately Responsible for High Risk Member Client Accounts and Transactions</u>

In all instances of acceptance of a HIGH RISK member client or customer requires senior officer approval.

Senior Officer shall mean:

1. Sector Head, Region Head, MFI Strategic Head (for Branches)
2. Group Head for Head Office Units

The above mentioned Senior Officers shall be ultimately responsible in the effective implementation of the following policies/procedures when dealing with HIGH RISK customers:

A. Gathering of the minimum information and documents required from individual member clients and corporate or juridical persons.
B. Perform Negative List verification.
C. Conduct face-to-face interview and review of Customer Risk Rating
D. Approval of Senior Officer for HIGH Risk member client.
E. Conduct second level transaction annually to validate and support the reviews conducted at branch/business unit level.
F. Issue AML Compliance Quarterly Certification to the effect that HIGH RISK KYC records and transactions were reviewed, unusual transactions were escalated to designated AML and CTF Compliance Officer and STRs were filed for transactions found to be indeed suspicious, if there is any.

National Risk Assessment and Management

National Risk Assessment (NRA) is a comprehensive exercise to identify, assess and understand a country's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions. The Anti-Money Laundering Council, together with relevant government, public and private offices and sectors, shall conduct a National Risk Assessment (2018 IRR Chapter IV Rule 13 Section 1) in compliance with the Financial Action Task Force (FATF) Recommendation 1. It should apply a risk-based approach to ensure the mechanisms and measures to prevent ML/TF risks are commensurate to the risks and context identified.

The NRA shall be updated once every three years or as often as the AMLC may deem necessary.