



**SOUTH ASIALINK**  
**FINANCE CORPORATION**

**REVISED**  
**ANTI-MONEY LAUNDERING**  
**TERRORIST FINANCING**  
**PREVENTION PROGRAM**  
**(MTPP)**

DECEMBER 2022





Republic of the Philippines  
**ANTI-MONEY LAUNDERING COUNCIL**

## **CERTIFICATE OF REGISTRATION**

This is to certify that SOUTH ASIALINK FINANCE CORPORATION has duly complied with the registration process of the Anti-Money Laundering Council (AMLC) for the purpose of submitting Covered and Suspicious Transaction Reports pursuant to the Anti-Money Laundering Act (Republic Act 9160), as amended, and its Revised Implementing Rules and Regulations.

This certification is issued this 12<sup>th</sup> day of November 2021 in the City of Manila.

A handwritten signature in black ink, appearing to read 'Matthew M. David', written over a light gray rectangular background.

**MATTHEW M. DAVID**  
Officer-in-Charge

Control No. : SEC-20191119600788-3



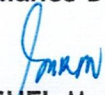
**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

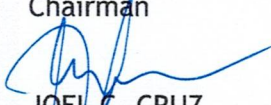
Policy applies to:  Company-wide  Specific group or employees only

Documented type:  New  
 Revision of existing documented information

Policy document status:  Initial Draft  Initial Review  
 Final Review  Approved

Policy/Process Control Review: **Compliance Department**

Compliance governance review officer:   
**ROSEHEL M. BARRUN**  
Chief Compliance Officer

Board Approval Authority: **SG**  
**RUBEN Y. LUGTU II**  
Chairman  
  
**JOEL C. CRUZ**  
President and COO

Implementation effectivity date: **December 02, 2022**

Approval Date of last revision: **September 2021**

Effectivity Date of last revision: **September 30, 2021**

Date of governing policy review\* **November 2022**

*\*unless otherwise indicated, this policy will still apply beyond the review date.*

Related legislation, standards, policies, procedures, guidelines, and local protocols **MTPP**



## TABLE OF CONTENTS

### **PART 1 - OVERVIEW**

- I. INTRODUCTION
- II. COMPANY PROFILE AND ORGANIZATIONAL STRUCTURE
- III. LEGAL FRAMEWORK
- IV. POLICY STATEMENT
- V. POLICY OBJECTIVES
- VI. POLICY SCOPE
- VII. DEFINITION OF TERMS
  - TERRORIST FINANCING
  - MONEY LAUNDERING AND ITS STAGES
  - PROLIFERATION FINANCING

### **PART 2 - GOVERNANCE & OVERSIGHT**

- I. INSTITUTIONAL RISK ASSESSMENT & MANAGEMENT
- II. CORPORATE GOVERNANCE
  - CHARTER OF THE ANTI-MONEY LAUNDERING (AML) COMMITTEE
    - A. COMPOSITION
    - B. MEETINGS
    - C. OVERSIGHT AUTHORITY AND RESPONSIBILITIES
  - III. COMPLIANCE MANAGEMENT
    - ROLE AND RESPONSIBILITIES OF THE CHIEF COMPLIANCE OFFICER OF SOUTH ASIALINK FINANCE CORPORATION
  - IV. INTERNAL CONTROLS AND AUDIT
    - BOARD AND MANAGEMENT OVERSIGHT
    - INTERNAL AUDIT SYSTEM
    - MONITORING OF ALL DEFICIENCIES NOTED AND/OR SEC & AMLC REGULAR OR SPECIAL EXAMINATION
  - V. HIRING POLICIES AND PROCEDURES

### **PART 3 - POLICY AND PROCEDURES**

- I. CUSTOMER ACCEPTANCE AND DUE DILIGENCE
  - CUSTOMER IDENTIFICATION / KNOW YOUR CUSTOMER (KYC)
    - CUSTOMER RISK PROFILING AND ASSESSMENT
    - CUSTOMER VERIFICATION
    - IDENTIFICATION AND VERIFICATION OF AGENTS
    - ULTIMATE BENEFICIAL OWNERSHIP
    - DETERMINATION OF THE PURPOSE OF RELATIONSHIP
    - ONGOING MONITORING PROCESS (OMP) OF CUSTOMER'S INFORMATION AND ACCOUNTS/TRANSACTIONS
  - II. PREVENTIVE MEASURES FOR SPECIFIC TRANSACTION AND ACTIVITIES
  - III. POLITICALLY EXPOSED PERSON



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

1. REQUIREMENTS ON POLITICALLY EXPOSED PERSON
2. POLICIES / REQUIREMENTS ON POLITICALLY EXPOSED PERSONS (PEP)
3. CROSS-CHECKING OF CLIENT'S NAME AGAINST WATCHLIST DATABASE

**IV. REPORTING OF COVERED TRANSACTION AND SUSPICIOUS TRANSACTIONS**

1. MONITORING AND REPORTING / RED FLAGGING OF TRANSACTIONS
2. REPORTING OF SUSPICIOUS TRANSACTIONS

**V. CONFIDENTIALITY AND TIPPING-OFF**

**VI. TRAINING AND CONTINUING EDUCATION PROGRAM**

**VII. RECORD KEEPING AND RETENTION ON DIGITIZATION OF CUSTOMERS RECORD**

**VIII. RELIANCE ON THIRD PARTIES AND SERVICE PROVIDERS**

**IX. OUTSOURCING OF CONDUCT OF CUSTOMER IDENTIFICATION AND DUE PROCESS**

**X. CUSTOMER REFUSAL**

**XI. PROHIBITED ACCOUNT**

**XII. TARGETED FINANCIAL SANCTIONS (TFS) AND TFS PROLIFERATION FINANCING (PF)**

**XIII. COOPERATION WITH THE ANTI-MONEY LAUNDERING COUNCIL**

1. AMLC DOCUMENTARY REQUIREMENTS FOR COVERED TRANSACTION (CT) AND SUSPICIOUS TRANSACTIONS (ST)
2. HANDLING OF FREEZE ORDER FROM AMLC
3. FREEZING MECHANISM
4. PROHIBITION AGAINST DISCRIMINATION
5. FORFEITURE OF EQUAL VALUE
6. SHARING OF CUSTOMER INFORMATION AMONG EMPLOYEES
7. PENALTIES FOR VIOLATION OF THE AML/PF/TF SUPPRESSION ACT (RPAC)
8. RULES OF PROCEDURES IN ADMINISTRATIVE CASES
9. SAFE HARBOR PROVISIONS

**PART 4 - FORMS AND TEMPLATES**

South Asialink Finance Corporation LOAN APPLICATION FORM FRONT PAGE

South Asialink Finance Corporation LOAN APPLICATION FORM BACK PAGE

South Asialink Finance Corporation CUSTOMER RISK ASSESSMENT FORM FRONT PAGE



*Revised Money Laundering Terrorist Financing Prevention Program (MTPP)*

South Asialink Finance Corporation CUSTOMER RISK ASSESSMENT  
FORM BACK PAGE

Compliance Testing Template  
REPORT ON AML COMPLIANCE TESTING TEMPLATE

REPORT ON AML COMPLIANCE TESTING PAGE 2

REPORT ON AML COMPLIANCE TESTING PAGE 3

**PART 5 – APPROVING AUTHORITY**

**PART 6 – UPDATING OF MONEY LAUNDERING TERRORIST FINANCING  
PREVENTION PROGRAM**

**PART 7 – ANNEXES**

ANNEX A – ANTI MONEY LAUNDERING (AML) PROCEDURES AND  
GUIDELINES ON COMPLIANCE TESTING

I. CUSTOMER DUE DILIGENCE

- A. REVIEW ON DOCUMENTATIONS
- B. REVIEW ON PROHIBITED ACCOUNTS
- C. REVIEW ON RENEWAL OF IDENTIFICATION
- D. REVIEW ON AVERAGE CDD
- E. REVIEW ON CORPORATE ACCOUNTS
- F. REVIEW ON TRUST, NOMINEES AND FIDUCIARY
- G. REVIEW ON HIGH RISK CUSTOMERS
- H. AREA OF RISKS
- I. AUDIT PROCEDURES

II. MONITORING, RECORDING AND REPORTING

- A. REVIEW ON MONITORING PROCESSES
- B. REVIEW ON RECORD KEEPING
- C. REVIEW ON REPORTING TO THE AMLC

III. INTERNAL CONTROL AND PROCEDURES, COMPLIANCE  
AND TRAINING

IV. VALIDATION/MONITORING OF AML CUSTOMER SELF-  
ASSESSMENT FORM QUESTIONNAIRES, HIGH RISK CUSTOMER, AML  
RELATED SYSTEMS AND DATABASES

ANNEX B – AML COMPLIANCE TESTING SCORING MATRIX

ANNEX C – CUSTOMER RISK RATING METHODOLOGY

ANNEX D - LIST OF POLITICALLY EXPOSED PERSON

ANNEX D - CTR LOAN TRANSACTION CODES

ANNEX F –SOUTH ASIALINK FINANCE CORPORATION ANTI-MONEY  
LAUNDERING COMMITTEE



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### PART 1 OVERVIEW

#### I. INTRODUCTION

This Anti-Money Laundering and Terrorism Financing Prevention Program (MTPP) of **South Asialink Finance Corporation**, herein referred to as “**The Company**”, aims to assess whether the elements, processes and controls of the compliance program are designed appropriately; to ensure compliance with the existing Anti-money laundering laws, rules and regulations; and to ensure that the Companies reputation is not compromised.

As a Securities and Exchange Commission (SEC)-supervised covered institutions, they are covered by the money laundering, terrorist financing and proliferation financing (ML/TF/PF) regulations.

This Manual was developed to help the employees and all concerned units to understand the importance of knowing the Company’s customers, recognize and report suspicious or “red flag” activities in the conduct of day-to-day business responsibilities, understand how to detect and respond to “red flag” situations according to Company’s internal policies and procedures consistent with the guidelines established by governing agencies, understand and avoid the penalties for non-compliance, satisfy legal and ethical responsibilities to prevent any adverse impact on the Company’s Organization and overall accountabilities as covered person relative to corporate objective and goals.

#### II. COMPANY PROFILE AND ORGANIZATIONAL STRUCTURE

##### A. COMPANY BACKGROUND

**South Asialink Finance Corporation**, defined as “**The Company**”, is a financial services company that provides loan products in the Philippines focusing on individuals and small business entities (SMEs) located in 6/F & 7/F THE CURRENCY TOWER, J. VARGAS AVE. cor F. ORTIGAS JR RD., ORTIGAS CENTER PASIG CITY. It is one of the leading and fastest-growing finance companies in the Philippines. The Company was established in June 2007 when a group of enterprising executives ventured into the consumer financing business with only three million pesos in capitalization. With good demand and sound credit, the Company was off to a good start.

Today, it employs more than three hundred fifty personnel, thousands of independent Loan Consultants, and with over eighty branches nationwide serving the financial needs of businesses and individuals alike.

The Company offers financial loan services such as sangla, pre-owned/brand new financing, real estate mortgage and personal loan for doctors.

- Sangla OR/CR - Secured loan for individuals who owns cars, trucks, multicabs, or taxis/PUVs.
- Secondhand & brand new financing- Secured loan for individuals who want to purchase car, truck, and multicab.
- Real-estate mortgage- Secured loan for property owners (residential, condominium, and commercial units) within key cities in the Philippines.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- Personal loan for doctors - Applicable for general practitioners, ophthalmologists and dentists.

“OUR PURPOSE IS: TO SPEARHEAD THE REVOLUTION TOWARDS A POSITIVE AND SUSTAINABLE CHANGE IN THE FINANCIAL SERVICES INDUSTRY IN THE PHILIPPINES.”

“OUR MISSION IS: TO SPEARHEAD THE REVOLUTION TOWARDS A POSITIVE AND SUSTAINABLE CHANGE IN THE FINANCIAL SERVICES INDUSTRY IN THE PHILIPPINES.”

“OUR VISSION”

FOR THE CUSTOMERS: To provide the best financial solutions that will make peoples’ lives better.”

FOR THE COMPANY: To be the fastest-growing financing company in the Philippines with annual revenue growth of 50%.

“OUR VALUES”

INTEGRITY - We commit to honesty and integrity. We will be honest in all our dealings, true to ourselves, to our company and to the people we serve.

ACCOUNTABILITY - We take responsibility in everything we do.

PASSION - We strongly believe that our actions will help us achieve our goal.

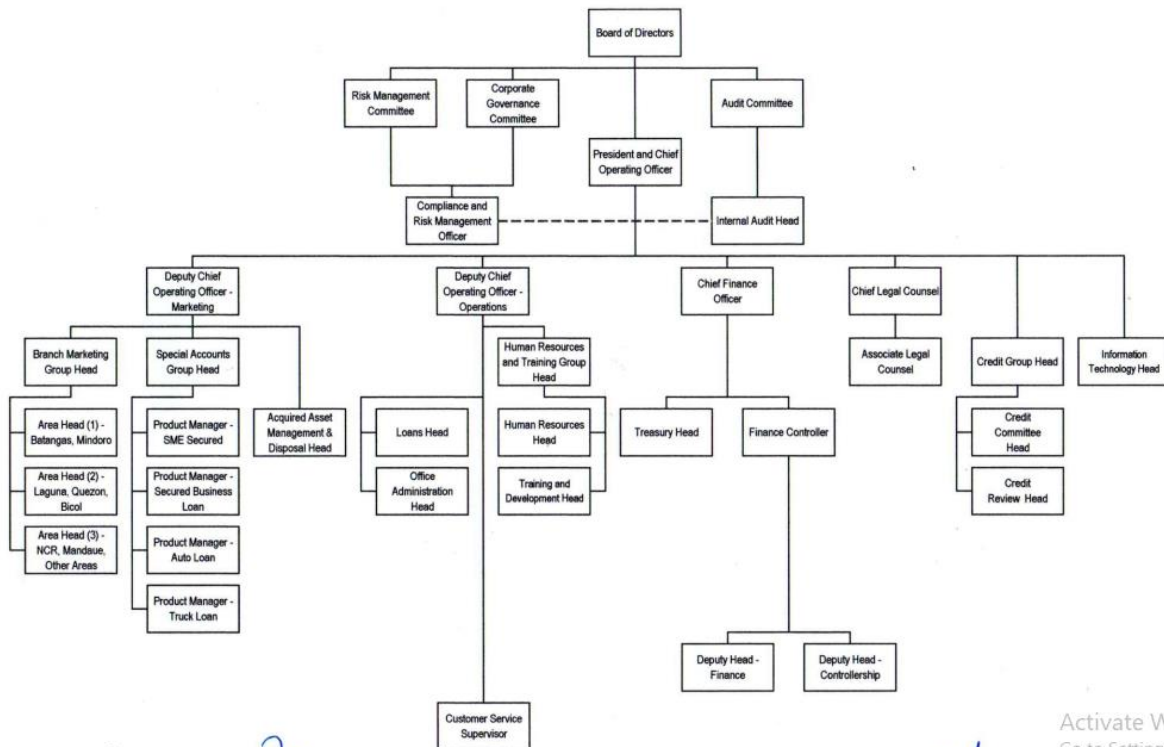
TEAMWORK - We are united in the pursuit of achieving company’s goal.

COMMITMENT - We value YOU more than us.

EXCELLENCE - We do ordinary things extraordinarily well.

**B. ORGANIZATIONAL STRUCTURE**

**SOUTH ASIALINK FINANCE CORPORATION**  
ORGANIZATIONAL CHART 2022





## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### III. LEGAL FRAMEWORK

Covered and suspicious transaction reporting framework is one of the cornerstones of the Philippines' MT/TF/PF regime. Covered Persons, as the first line of defense against MT/TF/PF, are mandated to report all covered and suspicious transactions to the Anti-Money Laundering Council (AMLC). The reports should be complete, accurate, and timely as they provide vital information for the effective identification and detection of financial crime patterns and trends through financial analysis. The results of analysis on these reports are essential in the investigation and prosecution of civil forfeiture, ML/TF/PF and other related cases, as well as in assessing institutional, sectoral, and national ML/TF/PF risks. Thus, the importance of complete, accurate, and timely reports cannot be overemphasized.

RA No. 9160	An Act Defining The Crime Of Money Laundering, Providing Penalties Therefore and for Other Purposes IRR Effectivity: 2 April 2002	17 October 2001 (Effectivity)
RA No. 9194	An Act Amending Republic Act No. 9160, Otherwise Known as the "Anti-money Laundering Act of 2001" RIRR Effectivity: 7 Sept. 2003	23 March 2003
RA No. 10167	An Act to Further Strengthen The Anti-money Laundering Law, Amending for the Purpose Sections 10 And 11 Of Republic Act No. 9160, Otherwise Known as the "Anti-money Laundering Act of 2001", as amended, and for other Purposes RIRR Effectivity: 7 Sept. 2003	6 July 2012
RA No. 10365	An Act Further Strengthening the Anti-Money Laundering Law, Amending for the Purpose Republic Act No. 9160 , Otherwise Known as the "Anti-money Laundering Act of 2001", as Amended	7 March 2013
RA No. 10927	An Act Designating Casinos as Covered Persons Under Republic Act No. 9060, Otherwise Known as the "Anti-money Laundering Act of 2001", as Amended	7 July 2017 (Approved)
RA No. 10168	An Act Defining the Crime of Financing Terrorism, Providing Penalties Therefore and for Other Purposes (The Terrorism Financing Prevention and Suppression Act of 2012)	05 July 2012 (Effectivity)
RA No. 10697	An Act Preventing the Proliferation of Weapons of Mass Destruction by Managing the Trade in Strategic Goods, the Provision of Related Services, and For Other Purposes	13 November 2015
RA No. 11521	An Act Further Strengthening the Anti-Money Laundering Law, Amending for the Purpose Republic Act No. 9160, Otherwise Known as the "Anti-money Laundering Act of 2001", as Amended	10 February 2021
AMLC Issuances	2018 Implementing Rules and Regulations (IRR) of Republic Act (R.A.) No. 9160	



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

2021 AMLC Registration and Reporting Guidelines (ARRG)
Rules of Procedure on Administrative Cases
Guidelines on Digitization of Customer Records and its amendments
AMLC Sanctions Guidelines (2021)

**A. Anti-Money Laundering Act Republic Act No. 9160**, also known as the Anti-Money Laundering Act of 2001, as amended (AMLA), provides the primary legal framework for reporting covered and suspicious transactions:

- **Section 7(1) of the AMLA** authorizes the AMLC to require, receive and analyze covered and suspicious transaction reports from covered persons. To be able to file the reports, Rule 22, Section 4, of the 2018 IRR requires covered persons to register with the AMLC's electronic reporting system.

- **Section 9(c) of the AMLA** requires covered persons to file covered and suspicious transaction reports in accordance with the standards set therein. Under Section 3(h) of the AMLA, in relation to Rule 2, Sections 1 (a) and (z), of the 2018 IRR, a transaction refers not only to individual transactions, but also to any act establishing any right Page 3 of 270 or obligation or giving rise to any contractual or legal relationship between the parties thereto (i.e., an activity or account of a customer). Any covered person who, knowing that a covered or suspicious transaction is required to be reported to the AMLC, fails to do so shall be guilty of ML under the last paragraph of Section 4 of the AMLA.

- **Rule 22, Section 6, of the 2018 IRR, in relation to Section 9(c), paragraph 4, of the AMLA**, refers to the "Safe Harbor Provision". This provision encourages covered persons to vigorously report covered and suspicious transactions as there is a legal assurance that they shall not be held administratively, criminally, or civilly liable for filing covered and suspicious transaction reports in the regular performance of his duties and in good faith. Notwithstanding the foregoing, Rule 22, Section 3, of the 2018 Implementing Rules and Regulations (IRR) of the AMLA emphasizes the importance of complete, accurate and timely reporting of covered and suspicious transactions. Malicious reporting is a criminal offense under Section 14(c) of the AMLA.

- **Rule 22, Section 7, of the 2018 IRR, in relation to Section 9(c), paragraph 5, of the AMLA**, refers to the "Confidentiality Provision". This provision prohibits the covered persons, and their officers and employees from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction has been or is about to be reported, the contents of the report, or any other information in relation thereto. Breach of confidentiality is a criminal offense under Section 14(d) of the AMLA. Section 4 of the AMLA provides that money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required to be reported fails to do so.

**B. Terrorism Financing and Suppression Act Republic Act No.10168**, also known as the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA), provides the legal framework for reporting suspicious transactions related to TF:

- **Section 17 of TFPSA** requires that TF be subject to the suspicious transaction reporting requirements under the AMLA.

- **Rule 3.a.15 of the IRR of the TFPSA** provides additional circumstances that would make transactions suspicious in the context of terrorism financing.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### IV. POLICY STATEMENT

The Anti-Money Laundering Council (AMLC) comprised of the Bangko Sentral ng Pilipinas (BSP), Security and Exchange Commission (SEC) and Insurance Commission (IC) provide rules and regulations to covered institutions relative to the implementation of R.A. 9160 also known as The Anti-Money Laundering Act (AMLA) of 2001, as amended by R.A. 9194, R.A. 10167, R.A. 10365 and RA 10927, and R.A 10168 also known as The Terrorism Financing Prevention and Suppression Act (TFPSA) of 2012 and R.A. 11521 as An Act Further Strengthening the Anti-Money Laundering Law, Amending for the Purpose Republic Act No. 9160, Otherwise Known as the “Anti-money Laundering Act of 2001”, as Amended.

This manual, however, is designed to ensure that all operating units and branches of the Company and its service providers shall comply with the ML/TF/PF requirements, their respective Implementing Rules and Regulations (IRR) and other AML issuances. This manual also includes obligations set out in Philippine legislation, rules, regulations, government regulatory bodies and agencies’ guidance, global best practices; and that adequate systems and controls are in place to mitigate the ML/TF/PF risks and that the organization is not used to facilitate financial crime.

### V. POLICY OBJECTIVES

This manual serves as comprehensive operating guidelines for use of Company’s officers and employees in implementing the Anti-Money Laundering Law and other rules and regulations issued by the Anti-Money Laundering Council and the Securities and Exchange Commission. This manual aims to achieve the following:

1. To promote adequate awareness regarding the rationale of the enactment of the anti-money laundering law and its importance to the general economy. It is also important that employees understand the concept of money laundering as a crime and the various activities and stages by which it is perpetrated in the economic system and through the different financial institutions;
2. To establish detailed policies and procedures on the Company’s compliance and implementation of the major requirements of the AMLA, as amended, its RIRR, and these rules such as customer identification process including acceptance policies and on-going monitoring processes, record keeping retention and covered and suspicious transaction reporting;
3. To ensure that officers and staff of the Company clearly understand the responsibilities of the institution and each individual employee in carrying out the requirements of the anti-money laundering law and the accountabilities and penalties involved for non-compliance with the requirements; and
4. To ensure that the provisions of Securities and Exchange Commission and any succeeding AMLC issuances and amendments as contained in this manual shall serve as a guide for the Company in maintaining its safety and soundness through proper implementation and adoption of these rules and regulations and to further protect the integrity and confidentiality of bank accounts.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### VI. POLICY SCOPE

This policy manual serves as a guide of the Company's employees which includes comprehensive, risk-based, and written internal policies, controls and procedures to implement the relevant laws, rules and regulations, and best practices to prevent and combat ML/TF/PF and associated unlawful activities.

In adhering to this Policy Manual, as with every aspect of its business vehicles, the Company expects that its employees nationwide and the employees of its accredited service providers will conduct themselves in accordance with the highest ethical and professional standards. The Company also expects its employees including its third party service providers to conduct business in accordance with applicable AML laws. The employees shall not knowingly provide advice or other assistance to individuals who attempt to violate or avoid anti-money laundering laws.

Anti-money laundering laws apply not only to criminals who try to launder their ill-gotten gains but also to the Company's employees who participate in those transactions, if the employees know that the property is criminally derived. "Knowledge" includes the concept of "willful blindness" and "conscious avoidance of knowledge." Thus, employees of the Company whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, maybe considered under the law to have the requisite "knowledge". The employees who suspect money laundering activities should refer the matter to appropriate personnel, such as, their immediate supervisor, the designated Chief Compliance Officer, the Group Head and Senior Management and Board of Directors.

### COVERED INSTITUTION

The Company is a covered institution of the Anti-Money Laundering Council (AMLC) because it is an entity being supervised or regulated by the Securities and Exchange Commission.

Its Institution Code is **600187**. It is also registered in AMLC portal thru its Chief Compliance Officer to send reportorial requirements which includes Covered Transaction Reports (CTRs), Suspicious Transactions Reports (STRs), AMLC requested documents, digitization status reports, etc.

### VII. DEFINITION OF TERMS

Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the AMLA, as amended, and its RIRR.

**Average Due Diligence (EDD)** refers to the due diligence procedures performed on low/normal risk customers to investigate them less meticulously requiring less significant evidence and detailed information and to establish the sources of fund of the customer or potential customer.

**Beneficial Owner** refers to any natural person (s) who ultimately owns or controls the customers and/or whose behalf a transaction or activity is being conducted; or those who has ultimate effective control over a legal person or arrangement.

**Ultimate effective control** refers to situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

Beneficial owner shall be:

- The natural persons, if any, who ultimately have controlling ownership interest in a juridical person.
- A shareholding or ownership interest of at least twenty percent (20%) in the customer held by a natural person shall be an indication of direct ownership. A shareholding or ownership interest of at least twenty percent (20%) in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership.
- The natural persons, if any, exercising control over the juridical person through other means, to the extent that there is a doubt under item '1' above, as to whether the persons with the controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests. Control through other means, includes control exerted by means of trusts, agreements, arrangements, understandings, or practices, or when an individual can exercise control through making decisions about financial and operating policies. In addition, control also includes:
  - power to govern the financial and operating policies of the enterprise under statute or an agreement;
  - power to appoint or remove the majority of the members of the board of directors or equivalent governing body;
  - power to cast the majority votes at a meeting of the board of directors or equivalent governing body; or
  - any other arrangement similar to any of the above.

**Client/Customer** refers to any person or entity that keeps an account, or otherwise transacts business with a covered person. It includes the following: (1) any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions; (2) beneficiary of a trust, an investment fund or a pension fund; (3) a company or person whose assets are managed by an asset manager; (4) a grantor of trust and (5) any insurance policy holder, whether actual or prospective.

**Covered transactions (CT)** is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of five hundred thousand pesos (P500,000.00) within one business day.

**Customer Due Diligence (CDD)** refers to the process used by the Company's personnel to collect and evaluate relevant information about a customer or potential customer.

**Customer Identification** involves verifying information provided by a customer before establishing business relationship.

**Customer Verification** refers to the process of authenticating a customer's identity including email verification, address verification, confirmation, checking, etc.

**Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computer for communication and document or data storage. Criminals who



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyber-terrorism are also of significant concern.

The cybercrime law of the Philippines (Cybercrime Prevention Act of 2012- RA 10175) defines and punishes certain acts, generally classified as:

- Offenses against confidentiality, integrity and availability of computer data and systems
- Computer-related offenses
- Content-related offenses



**Enhanced Due Diligence (EDD)** refers to the due diligence procedures performed on high risk customers to investigate them more thoroughly requiring significantly more evidence and detailed information about reputation and history to be collected.

**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:

- to carry out or facilitate the commission of any terrorist act;
- by a terrorist organization, association or group; or
- by an individual terrorist

### TERRORIST FINANCING (Republic Act R.A. 10168)

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.

<b>Objectives</b>	:	Launder Clean and Dirty Money
<b>Motive</b>	:	Ideological
<b>Source of Funds</b>	:	Donations
<b>Use of Funds</b>	:	Intimidation of Population
<b>Transaction Volume</b>	:	Smaller Transfer
<b>Business Involved</b>	:	Charities and Front Operations



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

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.

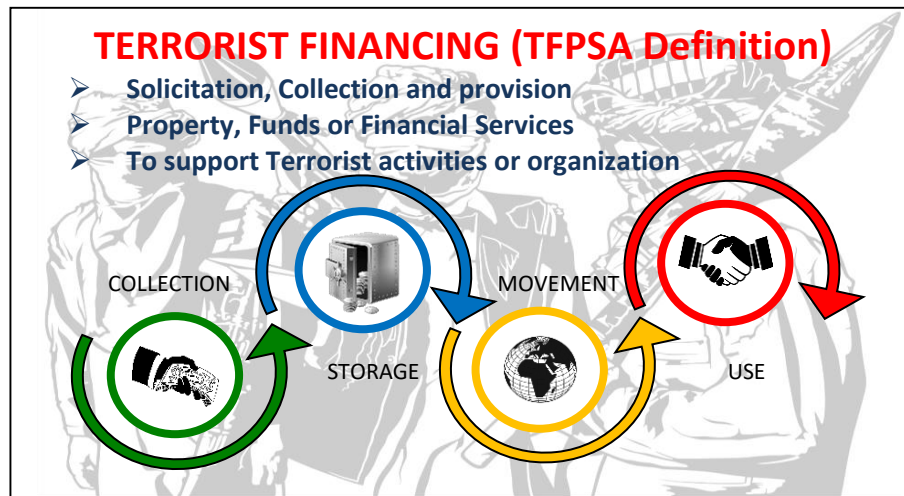


Figure 2.  
Terrorist Financing

**Juridical person** refers to an entity other than a natural person as defined under Chapter 3 of the Civil Code of the Philippines, which can establish a permanent customer relationship with any financial institution or otherwise own property.

**Money laundering** is a crime whereby the proceeds of an unlawful activity as herein defined are transacted; thereby making them appear to have originated from legitimate sources. It is committed by the following:



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- Any person knowing that any monetary instrument or property represents, involves, or relates to, the proceeds of any unlawful activity, transacts or attempts to transact said monetary instrument or property.
- Any person knowing that any monetary instrument or property involves the proceeds of any unlawful activity performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraph (1) above.
- Any person knowing that any monetary instrument or property is required under the act to be disclosed and filed with the Anti-Money Laundering Council, fails to do so.

### Money Laundering and Its Stages

Money laundering is the criminal practice of processing ill-gotten gains, or “dirty” money, through a series of transactions; in this way the funds are “cleaned” so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process.

<b>Objectives</b>	:	Launder Dirty Money
<b>Motive</b>	:	Profit and Greed
<b>Source of Funds</b>	:	Crimes
<b>Use of Funds</b>	:	Personal Luxury
<b>Transaction Volume</b>	:	Large and Repetitive
<b>Business Involved</b>	:	Shell Companies and Offshore Centers

Although money laundering is a diverse and often complex process, it basically involves three independent stages, namely: placement, layering and integration that can occur simultaneously:

- 1. Placement.** The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier’s checks or money orders) that are then collected and deposited into accounts at another location or financial institution.
- 2. Layering.** The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in on or more financial institutions.
- 3. Integration.** The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a believable explanation for the source of the funds.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

4. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

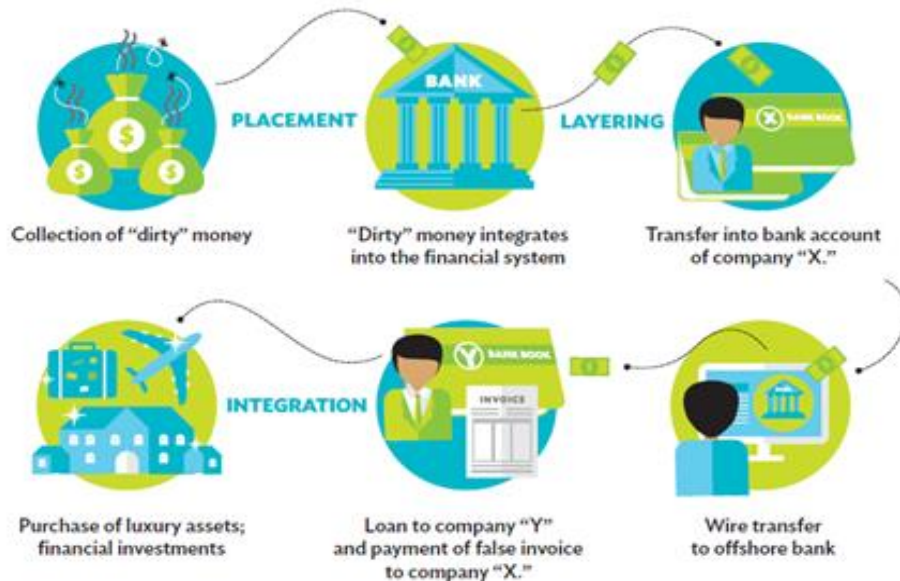


Figure 1. The Money Laundering Stages

**Monetary instrument** shall include, but is not limited to the following:

- Coins or currency of legal tender of the Philippines, or of any other country;
- Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property;
- Drafts, checks, and notes;
- 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;
- A participation or interest in any non-stock, non-profit corporation;
- 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;
- Contracts or policies of insurance, life or non-life, contracts of suretyship, 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.

**Monetary instrument or property related to an unlawful activity** refers to:

- All proceeds of an unlawful activity;
- All monetary, financial or economic means, devices, accounts, documents, papers, items or things used in or having any relation to any unlawful activity;



#### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- 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.
- "Related accounts" refer 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.
- 'Materially-linked accounts" shall include the following:
  - 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;
  - 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;
  - All "In Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
  - 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; and
  - All other accounts, shares, units, or monetary instruments those are similar, analogous, or identical to any of the foregoing.

**Politically exposed person** or *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.

The term PEP shall include immediate family members, and close relationships and associates that are reputedly known to have:

- Joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP; or
- Sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP.

*Immediate family members of PEP* refers to individuals who are related to a PEP within the second degree of affinity or consanguinity;

*Close associates of PEPs* refer to persons who are widely and publicly known 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.

**Official document** refers to any of the following identification documents:

- For Filipino citizens: Those issued by any of the following official authorities:
  - Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
  - Government-Owned or -Controlled Corporations (GOCCs); or
  - Covered persons registered with and supervised or regulated by the BSP, SEC or IC;
  - Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys)



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- For foreign nationals: Passport or Alien Certificate of Registration;
- For Filipino students: School ID signed by the school principal or head of the educational institution; and
- For normal risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the client's identity.
- Other identification document that can be verified using reliable, independent source documents, data or information.

**Philippine Identification Card (PhilID)** refers to the non-transferrable identification card Issued by the PSA to all citizens and resident aliens registered under the PhilSys, which serves as the official government issued identification document of cardholders in dealing with all government agencies, local government units, government and controlled corporations, government financial institutions, and all private sector entities.

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

**Processing** refers to payment transactions that are conducted electronically without the need for manual intervention.

**Proliferation Financing.** Amendments to the 2018 IRR of the AMLA, as amended, which include the following, among others:

- The expansion of the list of covered persons to include real estate developers and brokers as well as the offshore gaming operators and their service providers;
- Inclusion in the list of unlawful activities the violations of Section 19 (A)(3) of Republic Act No. 10697, otherwise known as the “Strategic Trade Management Act”, in relation to the proliferation of weapons of mass destruction (WMD) and its financing and Section 254 of Chapter II, Title X of the National Internal Revenue Code of 1997, as amended); and
- The additional authority of the AMLC to apply for the issuance of a search and seizure order or a subpoena ad testificandum and/or subpoena duces tecum with any competent court, in the conduct of its investigation; and to implement TFS in relation to the proliferation of WMD and its financing, including ex parte freeze.

<b>Objective</b>	:	Laundry Clean and Dirty Money
<b>Motive</b>	:	National
<b>Source of Funds</b>	:	Government
<b>Use of Funds</b>	:	Weaponry
<b>Transaction Volume</b>	:	Complex/Inconsistent Patterns
<b>Business Involved</b>	:	Shell Companies/ Offshore Center



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)



Figure 3.  
Proliferation Financing

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

**Shell Company** - Legal entities which have no business substance in their own right but through which financial transactions may be conducted.

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

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

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

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



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**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 institution.

**Unlawful activity** refers to any act or omission or series or combination thereof involving or having direct relation to the following:

- Kidnapping for ransom
- Drug trafficking and other violations of the Comprehensive Dangerous Drugs Act of 2002;
- Crimes covered by Anti-Graft and Corrupt Practices Act
- Plunder under R.A. 7080
- Robbery and extortion
- *Jueteng* and *Masiao*
- Piracy and hijacking on the high seas
- Qualified theft
- Swindling
- Smuggling
- Violations of Electronic Commerce Act of 2000;
- Hijacking, destructive arson and murder, including those perpetrated by terrorists against non-combatant persons (terrorist acts)
- Fraudulent practices and other violations under the Securities Regulation Code of 2000;
- Felonies or offenses of a similar nature punishable under penal laws of other countries.
- Terrorism and conspiracy to commit terrorism;
- Financing of terrorism, attempt or conspiracy to commit terrorism financing, accomplice to terrorism financing offense, accessory to terrorism financing offense;
- Bribery and corruption of public officers;
- Frauds and illegal exactions and transactions;
- Malversation of Public Funds and Property;
- Forgeries and counterfeiting;
- Violations of the Anti-Trafficking in Persons Act of 2003;
- Violations of the Revised Forestry Code;
- Violations of the Philippine Fisheries Code of 1998;
- Violations of the Philippine Mining Act of 1995;
- Violations of the Wildlife Resources Conservation and Protection Act;
- Violations of the National Caves and Cave Resources Management Protection Act;
- Violation of the Anti-Carnapping Act;
- Violations of the Decree Codifying the laws on illegal/unlawful possession, manufacture, dealing in, acquisition or disposition of firearms, ammunition or explosives;
- Violation of the Anti-Fencing Law;
- Violation of the Migrant Workers and Overseas Filipinos Act of 1995, as amended;
- Violation of the Intellectual Property Code of the Philippines;
- Violation of the anti-Photo and Video Voyeurism Act of 2009;
- Violation of the Anti-Child Pornography Act of 2009; and
- Violations of the Special Protection of Children against abuse, Exploitation and Discrimination Act.
- Violation of Section 19 (A) (3) of RA 10697, otherwise known as the Strategic Trade Management Act
- Violation of Section 254 of Chapter II, Title X of the National Internal Revenue Code of 1997, as amended



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### PART 2 GOVERNANCE & OVERSIGHT

#### I. INSTITUTIONAL RISK ASSESSMENT & MANAGEMENT

In pursuant with Memorandum Circular No.26 series of 2020 entitled “Guidelines in the Implementation of a Risk-Based Approach to Anti-Money Laundering Combating the Financing of Terrorism and Adoption and Development of a Risk Rating System for SEC”, South Asialink Finance Corporation is conducting Institutional Risk Assessment (IRA) to identify, understand and assess its ML/TF/PF risks, arising from **customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels**. IRA considers all relevant risk factors, including the results of national and sectoral risk assessments; (b) adequately document results and findings; and (c) be updated periodically or as necessary.

Based on the results of the IRA, The Company coordinates with the concerned person and departments/units and take appropriate measures to manage and mitigate ML/TF/PF risks and take enhanced measures on identified high risks areas, and is incorporated in its Money Laundering Terrorist Financing Prevention Program (MTPP).

The Company also identifies and assesses the ML/TF/PF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Such risk assessment should be an integral part of product or service development process and should take place prior to the launch of the new products, business practices or the use of new or developing technologies. The financing company takes appropriate measures to manage and mitigate the identified risks.

**Frequency of IRA:** The institutional risk assessment of the Company is conducted, every year, or as often as the Board or senior management may direct, depending on the level or risks identified in the previous risk assessment or other relevant AML/CFT developments that may have an impact on the company’s operations.

The Company has conducted institutional risk assessment (IRA) for the cutoff period covering January 1, 2021 to December 31, 2021 last May 13, 2022 to July 1, 2022. The final IRA report was submitted for approval to the Board of Directors of the Company on July 1, 2022. Overall, the residual Institutional AML/CT/PF Risk Assessment threat level of the Company was assessed as **MID-HIGH**. Final IRA report forms part of this manual

**Methodology:** The Company established an IRA methodology that considers both quantitative and qualitative data and information. The IRA methodology considers the inherent risk factors described and the preventive measures required in the relevant AML/CTPF regulations and standards. The Company created questionnaires to facilitate gathering the information and computing for the risk scores for the IRA.

The BOD, senior management and relevant officers and employees of the Company are duly involved in the IRA exercise. The Company follows an integrated approach in the IRA, which means that the Compliance Department works with the relevant business units and departments in conducting the IRA. In conducting the IRA, the Company performed the following:

- Completion of the questionnaires
- Analysis of results and other qualitative factors
- Discussion of control enhancement and risk mitigation opportunities



## **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

Moreover, they also exercise active control and supervision in the formulation and implementation of institutional risk management. They shall be ultimately responsible for the Company's compliance with the AMLA and TFPSA, their respective IRR, and other AMLC issuances.

### **II. CORPORATE GOVERNANCE**

South Asialink Finance Corporation has AML Committee (Management-level), Corporate Governance Committee (Board-level Committee) and Board of Directors (BOD) to oversee the AML Compliance of the company. They ensure that oversight on the Financing Company's compliance management is adequate (a) approve and oversee policies; (b) have clear understanding of ML/TF/PF risks; (c) Establish reporting structure; and (d) allocate responsibility to ensure effective implementation to ensure effective implementation of AML policies.

The Compliance Department and Company Management oversees the day-to-day management and ensure effective implementation of AML policies approved by the BOD. They establish a management structure that promotes accountability and transparency and upholds checks and balances. Made an alignment of activities with the strategic objectives, risk profile and corporate values set by the BOD.

It is the ultimate responsibility of the Board of Directors and Senior Management to fully comply with the provisions of these rules, the AMLA, as amended, and its RIRR. For this reason, it ensures that oversight on the Company's compliance management is adequate.

The AML Committee, which is composed of senior management, reviews and recommends internal policies and guidelines pertaining to reporting of Suspicious Transaction Reports, including criteria or basis on what comprise a suspicious transaction. It evaluates and deliberates on the evidence or findings gathered on account suspected of money laundering as referred by branch or department. Based on the findings/reports of the branch/business unit, the Committee decides whether there is reasonable basis for considering a covered transaction or suspicious transaction or any other illegal or unlawful activity and whether a report will be made to the Anti-Money Laundering Council or evaluates the report and determines if the suspicion is based on reasonable grounds. Where a report will be filed with the AMLC, the official STR is being prepared by the Branch/Department Head and approved by the Group/Area Head and the Compliance Officer.

The Committee reviews and approves system requirements, policies and procedures to ensure company's compliance. Review and define scenarios that may result to a suspicious transaction trigger or alerts. It also coordinates with AMLC regarding updates and other Anti-Money Laundering issues that need to be communicated within South Asialink Finance Corporation.

It also recommends revisions of the Money Laundering and Terrorist Financing Prevention Program (MTPP) for submission to the Board of Directors to ensure full compliance to the Anti-Money Laundering Revised Implementing Rules and Regulations.

All of the issues/concerns regarding the AML compliance of the company are being discussed and elevated to the Corporate Governance Committee and Board of Directors. They oversee the compliance and address the significant issues being raised.

### **CHARTER OF THE ANTI-MONEY LAUNDERING (AML) COMMITTEE**

The AML Committee is a Management-level Committee is tasked to assist the Corporate Governance Committee (CGC) and Board of Directors (BOD) in fulfilling its oversight responsibility for the implementation of the



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

Company's Money Laundering and Terrorist Financing Prevention Program (MTPP). The Committee aims to implement the risk-based approach to prevent the company from being used to facilitate illegal activity, and ensure compliance with the provisions of the Anti-Money Laundering Act, as amended, its Revised Implementing Rules and Regulations (RIRR), rules and regulations of Securities and Exchange Commission (SEC) and other relevant laws related to AML.

#### **A. COMPOSITION (Effective 16 June 2022)**

Chairman: President/Chief Operating Officer  
Members: Deputy Chief Operating Officer (COO), Operations  
Deputy Chief Operating Officer (COO), Sales and Marketing  
Credit and Collection Head  
Information Technology Group Head  
Legal Department Head  
Compliance Department Head  
Chief Finance Officer  
Auto and Truck Loans Department Head

Resource Persons:

Internal Audit Department Head  
Risk Management Department Head  
Any personnel involved on the issue for discussion, as determined  
needed by the AML Committee

#### **B. MEETINGS**

- a. The AML Committee meet on a monthly basis or frequently as considered necessary. Meetings of the AML Committee are being convened by the Chairman as deemed appropriate, or upon request of the majority of the members.
- b. A quorum will comprise of majority of the members of the AML Committee. Attendance of at least five (5) of the nine (9) members constitutes a quorum. Further, unanimous or majority votes of the members are considered official and binding.
- c. Voting on Committee matters shall be on one member – one vote basis. Majority vote of all members present shall constitute an official action of the AML Committee.
- d. The members of the AML Committee attend its meetings in person or through teleconferencing and videoconferencing conducted in such a manner that will allow the member who is taking part in said meetings to actively take part in the deliberations on matters taken up therein, except when justifiable causes prevent his attendance to ensure that the quorum requirement will be met. Justifiable causes include, but are not limited to, grave illness or death of an immediate family or serious accidents.
- e. The notice and agenda of the meeting be furnished to the members prior to each meeting and will include relevant supporting papers as appropriate.
- f. Issues raised during the meeting will be elevated to the Corporate Governance Committee.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### C. OVERSIGHT AUTHORITY AND RESPONSIBILITIES

This Charter of the AML Committee sets out the roles, responsibilities, and authority of the AML Committee as delegated by the Corporate Governance Committee and Board of Directors, and the rules of procedure that will guide the Committee in the performance of its functions including:

- a) The AML Committee oversees the implementation of the Company's Money Laundering and Terrorist Financing Prevention Program (MTPP) and to recommend to the Corporate Governance Committee and Board the adoption of a comprehensive and risk-based MTPP geared toward the promotion of high ethical and professional standards and the prevention of the company being used, intentionally or unintentionally, for money laundering and terrorism and proliferation financing and recommend revision of the manual based on the new rules and regulations of the AML.
- b) The AML Committee reviews and recommends internal policies and guidelines pertaining to reporting of Suspicious Transaction Reports, including criteria or basis on what comprise a suspicious transaction. It shall evaluate and deliberate on the evidence or findings gathered on account suspected of money laundering as referred by branch or department.
- c) Review and approve the AML client risk profiling model and changes thereto and review and note changes in the risk profiles of clients, i.e., downgrading from high risk to normal or low risk, and upgrading from low risk to normal or high risk.
- d) Based on the findings/reports of the branch/department, the Committee decides whether there is reasonable basis for considering a covered transaction or suspicious transaction or any other illegal or unlawful activity and whether a report will be made to the Anti-Money Laundering Council (AMLC) or evaluates the report and determines if the suspicion is based on reasonable grounds.
- e) The Committee should ensure that all accounts subject to suspicious transactions review and evaluation should be treated with utmost confidentiality.
- f) Review and approve system enhancements and requirements, policies and procedures to ensure company's AMLA compliance. Review and define scenarios that may result to a suspicious transaction trigger or alerts.
- g) Coordinate with AMLC regarding updates and other Anti-Money Laundering issues that need to be communicated within South Asialink Finance Corporation.
- h) Ensure that infractions discovered either by internally initiated audits or by special or regular examination conducted by the AMLC or SEC, are immediately corrected.
- i) Note and confirm the Covered Transactions Reports and decline accounts.
- j) Review and approve AML compliance risk assessments, annual testing plan and changes thereto, review the findings of Compliance Testing for AML and approve sanctions to be



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

imposed as a result of such findings, monitor and oversee timely compliance and responses to BSP/AMLC findings on regular or special examination in relation to AML.

- k) Recommend or approve database and system enhancements and initiatives in compliance with AML rules and regulations.
- l) Organize the timing and content of AML training of officers and employees including regular refresher trainings.

### **III. COMPLIANCE MANAGEMENT**

The Compliance Department implements the Company's MTPP. The Compliance Department manages the implementation of the MTPP of the Company on a company-wide basis up to branches. To ensure the independence of the department, it has a direct reporting line to the Corporate Governance Committee and Board of Directors on all matters related to ML/TF/PF and their risk management. The department is responsible for the following functions among other functions that may be delegated by senior management and the board to wit:

- ✓ Ensure compliance by all responsible officers and employees with this Anti-Money Laundering Laws and Regulations and the Financing Company's MTPP. It conducts periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML/TF/PF prevention reporting channels, effectiveness of the transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It also reports compliance findings to the AML Committee, Corporate Governance Committee and to the Board;
- ✓ Ensure that infractions, discovered either by internally initiated audits, or by special or regular examination conducted by the Security and Exchange Commission, or other applicable regulators, are immediately corrected;
- ✓ Inform all responsible officers and employees of all resolutions, circulars and other issuances by the Security and Exchange Commission and the Anti-Money Laundering Council in relation to matters aimed at preventing ML/TF/PF; and
- ✓ In coordination with Human Resources Department, Compliance Department formulates AML Training and periodic refresher program aimed at providing responsible officers and personnel with efficient, adequate and continuous education program to enable them to fully and consistently comply with all their obligations under these Rules, the AMLA, as amended, and its RIRR.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**  
**ROLE AND RESPONSIBILITIES OF THE CHIEF COMPLIANCE OFFICER OF SOUTH ASIALINK FINANCE CORPORATION**

The role of the Chief Compliance Officer is a critical factor in enabling an organization to achieve compliance with its statutory and regulatory obligations. The Chief Compliance Officer acts as the focal point for oversight of the Company's anti-money laundering activities with an adequate level of authority, access and resources.

- ✓ Be a member of senior management;
- ✓ Be independent and autonomous;
- ✓ Be informed of any relevant knowledge or suspicion of money laundering within the firm;
- ✓ Possesses the trust and confidence of management, staff and the Anti- Money Laundering Council (AMLC);
- ✓ Have sufficient knowledge of the organization, its products, services and systems;
- ✓ Have access to all relevant information throughout the organization and, of course, have knowledge as to the existence of such information; and
- ✓ Warrant the trust and confidence of the enforcement agencies.

**The Responsibilities of the Chief Compliance Officer are as follows:**

- Responsible for establishing and maintaining a manual of compliance procedures, in relation to the business of the Company. He is the lead implementer of the Money Laundering and Terrorist Financing Prevention Program (MTPP) of the Company.
- Responsible for ensuring compliance by the staff of the Company with the provisions of the Anti-Money Laundering Act (AMLA), as amended, it's implementing Rules and Regulations, and the Company's manual of compliance procedures.
- Responsible for disseminating to its board, officers and all employees memorandum circulars, resolutions, instructions and policies issued by the AMLC and by the Securities and Exchange Commission in all matters relating to the prevention of money laundering.
- The liaison between the Company and the AMLC in matters relating to the Company's compliance with the provisions of the AMLA and its implementing Rules and Regulations.
- Receives internal reports (covered and suspicious transactions).
- Takes reasonable steps to access any relevant "Know-Your-Client" (KYC) information.
- Provides periodic compliance testing on branches and other Bank's units regarding the relevant rules and regulations on Anti-Money Laundering particularly customer identification requirements, record keeping requirements and reporting of covered and suspicious transactions.
- Responsible for the preparation and submission to the AMLC written reports on the Bank's compliance with the provisions of the AMLA and its implementing Rules and Regulations, in such form as the AMLC may determine.



#### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- Likewise, responsible for the submission/sending of covered and suspicious transaction reports electronically to the Anti-Money Laundering Council (AMLC) and make other external reports to the AMLC whenever necessary.
- Takes reasonable steps to establish and maintain adequate arrangements for awareness and training.
- Monitors day-to-day operation of Company's AML policies.
- Responds promptly to any reasonable request for information made.
- Makes compliance reports to be submitted on a monthly/quarterly basis to the Senior Management and Board Level Committees at least annually.
- Participates in the development of the products and services of the Company to ensure AML-compliant.
- Obtain and use national and international findings concerning countries with inadequacies in their approach to ML prevention

#### **IV. INTERNAL CONTROLS AND AUDIT**

The Internal Audit is responsible for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, covered transaction and suspicious transaction reporting and record keeping and retention, as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

#### **BOARD AND MANAGEMENT OVERSIGHT**

The Internal Audit shall directly report to the Audit Committee and Board of Directors. The directors and committee members shall oversee the AML Compliance of the company to ensure that the Company's compliance management is adequate and the AML policies and procedures are properly implemented. The internal audit department shall apprise the Audit Committee and Board of Directors for any exceptions/findings noted in the audit including the updates on the unresolved/recurring/outstanding issues on a regular basis.

#### **INTERNAL AUDIT SYSTEM**

The Internal Audit Department of the company has developed the risk-based audit procedures on the implementation of the Anti-Money Laundering Act and SEC Memorandum Circular No. 26 series of 2020 with the following objective and scope:



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 1. AUDIT OBJECTIVE

To ensure company's compliance with the requirements of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001" dated 29 September 2001, as amended by Republic Act No. 9194 (AMLA, as amended) dated 07 March 2003 and SEC Memorandum Circular no. 16 series of 2018, an adoption of the Updated Anti-Money Laundering Rules and Regulations.

### 2. AUDIT SCOPE

- 1) Assess the adequacy and effectiveness of policies and procedures in implementing the requirements of the Anti-Money Laundering Council (AMLC);
- 2) Review of the application and effectiveness of risk management procedures and risk assessment methodologies related to customer identification processes.
- 3) Transaction testing, documentation and assessment of existing internal control procedures related to KYC, money laundering and terrorist financing.
- 4) Assess monitoring of reports required from branches / departments / sections in compliance with the regulations of AMLC and the SEC
- 5) Risk management framework;
- 6) Compliance with the AMLA and TFPSA, their respective IRR, and other issuances by the AMLC and other SAs
- 7) Adequacy and effectiveness of the MTPP

### 3. ASSESSMENT OF RISK EXPOSURE

The non-compliance with the guidelines and procedures aimed to control and prevent money laundering and terrorist financing could expose the Financing Company to sanctions that may be imposed by AMLC and SEC and other regulatory bodies (regulatory risk) and may put the Bank in an unfavorable situation in case of legal disputes (legal and reputational risks).

## MONITORING OF ALL DEFICIENCIES NOTED DURING THE AUDIT AND/OR SEC & AMLC REGULAR OR SPECIAL EXAMINATION

### 1. INTERNAL AUDIT EXAMINATION

The Internal Audit Department implemented a system of risk-based audit reporting, monitoring and tracking of outstanding issues. The Compliance Department was informed of the results of audit of branches / H.O. Units and monitors compliance of all uncorrected exceptions/findings.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 2. COMPLIANCE MONITORING

The Compliance Department monitors external audit findings and recommendations and the preventive corrective action plans taken by the branches/departments/ to close issues/comments. Results of which are reviewed by the Chief Compliance Officer and reported to the AML Committee, Corporate Governance Committee and to the Board of Directors.

One of the roles of the Compliance Department is the management of the SEC on-site examination and communication of all the issues/comments and recommendations of the SEC to all the branches / departments / section head concerned. All critical issues are discussed with the concerned branch / department / section for appropriate action.

Initial SEC findings and comments including resolutions, corrective actions and commitment dates are presented to the members of the AML Committee, Corporate Governance Committee and to the Board of Directors.

As the company is committed to comply with all the AMLC and SEC rules and regulations, the Compliance Department monitors continued compliance to the corrective actions already implemented by the Financing Company and eliminate potential repeat findings in the previous SEC Report of Examination (ROE).

Initially, the company submits a report containing actions that have been taken on each directive including documentary evidence to support management's representation noted in the report as "required actions" or highest priority supervisory matters requiring immediate action from management; and the plan of actions on directives that have not been fully complied with and the corresponding committed timelines. Internally, status and actions taken are requested from concerned units and the results of which are forwarded to the President.

The results are summarized and reviewed by the Chief Compliance Officer and the AML Committee, Corporate Governance Committee and to the Board of Directors for concurrence, notation and approval.

### 3. AML RISK-BASED COMPLIANCE TESTING PROCEDURE

Compliance Testing is performed to enhance the understanding of all personnel of the compliance function and how they affect the operation of banks and to enhance the understanding of the regulatory environment and the specific laws and regulations on ML/TF/PF. This includes effective monitoring of compliance risks by the personnel of the three (3) groups / units to enable the company to manage its compliance risks particularly on those areas of potential compliance failure, so as to prevent or minimize compliance breaches; and identify compliance breaches quickly and manage them appropriately.

#### Persons to conduct Compliance Testing:

- AML Compliance Officer
- Designated Compliance Coordinators in the branches and business units
- Internal Auditors

#### Frequency of conducting the Compliance Testing

- Frequency of conducting the Compliance Testing on branches / Head Office Units is determined based on its Risk Rating, as follows:



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

RISK RATING	FREQUENCY
UNACCEPTABLE	As needed based on the monitoring
BELOW ACCEPTABLE	Annually
ACCEPTABLE	Every two (2) years
ABOVE ACCEPTABLE	After the Two (2) year Testing Cycle

**Risk Rating** – This is the impact arising from non-compliance after taking into account the mitigating actions.

Prioritization of Compliance Testing is based on the Annual Compliance Testing Program approved by the AML Committee, Corporate Governance Committee and to the Board of Directors.

Please refer to the attached **AML Compliance Testing Procedures and Guidelines** for the comprehensive details on the processes of Compliance Testing.

On the other hand, please refer to the **Anti-Money Laundering (AML) Risk Scoring Matrix** for the detailed risk level definition is used by the Anti-Money Laundering (AML) Unit in evaluating the individual risk issues noted during AML Compliance Testing.

**Testing Frequency**

Frequency of compliance testing in the branch/unit/department is based on the results of the previous compliance testing and/or AML Risk Assessment. Annual compliance testing will be conducted on branches and units which will help the branch/unit with the highest compliance risk rating and/or highest consequence ratings.

Coordination of AML Compliance Testing with Internal Audit. Conduct of AML compliance tests will be closely coordinated with internal Audit to maximize coverage and have a broader scope of the assessment of the state of compliance of the company. Monitoring of the unresolved AML issues noted in the branch/unit coming from the AML Compliance testing conducted will depends on the stated frequency below:

Monitoring Frequency	Description
Biennial (In two year cycle period)	<ul style="list-style-type: none"> <li>• If the branch/unit have low risk unresolved AML issues noted in the testing.</li> <li>• If routing actions are taken to improve the AML process</li> </ul>
Annual (within the cycle period)	<ul style="list-style-type: none"> <li>• If the branch/unit have moderate risk unresolved AML issues noted in the testing</li> <li>• If necessary corrective actions are taken to resolve the AML issues noted.</li> </ul>
As Needed	<ul style="list-style-type: none"> <li>• If the branch/unit have high risk unresolved AML issues noted in the testing.</li> <li>• If urgent compliance has already taken to resolve the AML issues noted.</li> </ul>

**Resolution / Escalation of Compliance Issues**

1. The results of the internal audit examination shall be timely and directly reported to Company’s Audit Committee and Board of Directors; copy furnished the Chief Compliance Officer. The branch/department shall promptly address the audit findings noted in the report. The audit department shall monitor updates on the compliance of the branch/department on a regular basis until all



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**  
outstanding issues are being resolved. Copy of internal audit report shall always be readily available upon the request of the AMLC and other Supervising Agencies.

2. Full compliance is expected from all branches and/or units of the bank at all times. As such, the resolution of all Compliance issues is given priority.
3. Any compliance issue that cannot be immediately resolved being escalated directly to the Chief Compliance Officer (CCO).
4. Any compliance issue which is still unresolved/recurring issue to the branches and/or units constitute a possible serious offence with reference to the HRD Policy under Code of Conduct and Discipline. Hence, this will be dealt accordingly if resulted evaluation will prove non-compliance to the company's policy and procedures.
5. The respective branch/unit personnel concerned are required to provide AML Office a regular update on the status of resolution on outstanding issues.

## **V. HIRING POLICIES AND PROCEDURES**

The Human Resource Department, in coordination with concerned business units/group, implements an adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed in South Asialink Finance Corporation. This function is performed in accordance with the Background Investigation Policy and Recruitment and Hiring Policies and Procedures. Continuous evaluation of employees' performance, conduct and training needs be in placed to ensure that all officers and employees of the company are equipped to comply with AML laws.

### **Know Your Employee (KYE)**

Based on submitted documents and information, credit and court checking conducted by the company, conduct due diligence to ascertain if an employee-applicant qualifies based not only on his/her professional and career background but also has on passing the requirements under AMLA.

- **Family/ Personal Background.** Determine based on the Background Investigation report, if employee-applicant has family members / associates who are engaged in activities prone to ML/TF/PF or other criminal acts. Check if candidate falls under the high-risk category as defined for customers, such as PEP or closely related to one.
- **Credit Background.** Determine if employee-applicant has outstanding overdue loans with any bank or financial institution or past records show default in credit obligations.
- **Criminal Background.** If with same name in NBI or court checking, require the candidate to secure court clearances.
- **Watchlist.** Determine if employee-applicant is not in the watchlist of the AMLC for ML/TF/PF offenses, the OFAC, UNSL, other regulator and similar reliable sources.

### **AML Orientation**

Once hired, the employee shall need to undergo Ant-Money Laundering (AML) Orientation to be given by the Chief Compliance Officer or AML Officer so that he/she will be familiarized with the governing laws and regulation on AML as well as the internal policies and procedures of the company in AML compliance.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### PART 3 POLICY AND PROCEDURES

#### I. CUSTOMER ACCEPTANCE AND DUE DILIGENCE

The customer identification process is being performed by the Sales and Marketing personnel of the Company before establishing business relations or engaging in transactions with customers, pursuant to applicable laws and regulations.

This is being observed for all types of financial transactions by a customer and the authorized signatories of a corporate or juridical entity.

##### 1. CUSTOMER IDENTIFICATION / KNOW YOUR CUSTOMER (KYC)

###### FACE-TO-FACE CONTACT

Face-to-face contact is being conducted at the commencement of the relationship, or as reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business and the risks involved; provided that money laundering risks are effectively managed.

To verify the true identity of the customer, aside from online submission of the documentary requirements and phone calls, the customer need to be present in the interview of the credit investigators.

The face-to-face contact through the use of Communication Technology is subject of the following:

- It shall be subject to minimum mandatory information/document for individual client
- Branch/unit is in possession of and has verified the identification documents submitted by the prospective client prior to the interview
- The entire procedure is documented.
- The proof of Face-to-face contract through the use of technology such as the screen shot during shall form part of the KYC documents on file.
- The conduct of face-to-face contact through the use of Communication Technology shall be in accordance with the approved manual and procedure of concerned unit and shall form part of the MTPP.

###### INDIVIDUAL CUSTOMER

The Sales and Marketing personnel obtains from individual customers, at the time of loan application/establishing the relationship, the following minimum information and confirming this information with the official or valid identification documents:



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

Minimum Information	
1.	Name;
2.	Present address;
3.	Permanent address;
4.	Date and place of birth;
5.	<b>Gender</b>
6.	Nature of work, name of employer or nature of self-employment/ business;
7.	Contact details;
8.	Specimen signatures;
9.	Source of funds;
10.	Citizenship or Nationality;
11.	Tax or Social Security Information, if any;
12.	Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, whenever applicable

**Valid Identification Documents:**

**Per Policy No/Memo:** 2022-LoansDoc-008 issued on May 30, 2022, the following guidelines on acceptable identification cards. Client to present original ID upon releasing of loan proceeds.

**Primary ID – Valid digitized government issued IDs:**

- Philippine Passport
- Driver’s License
- PRC
- UMID/SSS/GSIS E-card
- SRC Seafarer’s Record Book
- PHILIPPINE IDENTIFICATION (Philsys ID)\***

**Secondary IDs – Non-digitized government recognized IDs**

- Senior Citizen
- PWD
- Solo Parent
- Voter’s ID
- TIN ID
- Barangay ID

**For Foreign Co-borrowers**

- Passport
- Alien Certificate of Registration (ACR)

**For Students and Employees**

- School ID
- Company ID

**Supporting Valid ID/Document**

- Marriage Certificate
- Barangay/Police/NBI Clearance**
- Philhealth Card**

Required to submit by the Customer/Borrower:

- Any ONE (1) PRIMARY plus ONE (1) Secondary
- Any TWO (2) SECONDARY plus ONE (1) Supporting Document

Required to submit by the Co-borrower: Any ONE (1) PRIMARY plus ONE (1) Secondary plus Supporting Valid ID

Note that:

- One Valid Identification card must be photo-bearing and with clear signature
- NO signature ID like Philippine National ID must be accompanied by any ID with signature



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- The Philippine National ID is official and sufficient proof of Identity – subject to the authentication requirements under the PhilSys Act and its IRR. Other Government issued ID are acceptable as Competent Proof of Identity required in legal documents.

**CORPORATE AND JURIDICAL ENTITIES**

The branch/unit opens and maintains accounts only in the true and full name of the entity and have primary responsibility to ensure that the entity has not been, or is not in the process of being dissolved, struck-off, wound-up, terminated or otherwise placed under receivership or liquidation. The following minimum information and/or documents before establishing business relationships:

Minimum Mandatory Requirements (Juridical Entities)	
Information	Documents
Name; Present address; Permanent address; Date and place of Incorporation/Establishment Nature of Business Contact details; Specimen signatures; Source of funds; <b>Signatories</b> ; Citizenship or Nationality; Tax or Social Security Information, if any; Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, whenever applicable	<ul style="list-style-type: none"> <li>✓ Identification Cards of the Signatories</li> <li>✓ Identification Card/s Ultimate Beneficial Owner</li> </ul>
1. Business Name / Registration	<ul style="list-style-type: none"> <li>✓ SEC Certificate of Incorporation or Partnership (Corporation or Partnership);</li> <li>✓ DTI Registration Certificate (Single Proprietorship);</li> <li>✓ BIR Registration Certificate;</li> <li>✓ Business Permit or Mayor’s Permit or Barangay Permit, whichever is applicable; and</li> <li>✓ Social security enrolment documents.</li> </ul>
2. Corporate Structure	<ul style="list-style-type: none"> <li>✓ Ownership composition;</li> <li>✓ List of Directors and Officers; and</li> <li>✓ Subsidiaries or affiliates, if any.</li> </ul>
3. Financial Documents	<ul style="list-style-type: none"> <li>✓ Audited Financial Statement (AFS);</li> <li>✓ Balance Sheet or Cash Flow; and</li> <li>✓ List of depository banks.</li> </ul>

- The Company enters into credit or financing transaction only in the true and full name of the borrower, account owner/entity.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- The mandatory information under AMLA as provided herein is obtained from the client. The **Loan Application Form (LAF)** is accomplished completely by the individual and corporate customers.
- The **Loan Application Form (LAF)** is accomplished completely by authorized signatories of corporate/juridical entities.
- The Customer Identification is updated every semester or during the lifetime of the account or as often as possible as warranted by policies and circumstances.

**2. CUSTOMER RISK PROFILING AND ASSESSMENT**

The Sales Personnel shall accomplish AML Customer Risk Assessment Form (CRAF) to assess the risk profile of the applicant or customer and to determine what due diligence procedures shall be performed. *(Please see Annex C – Risk Rating Methodology FAQs)*

**1) Risk Classification of Customers**

- Criteria for classifying Customers as to risk shall be as follows:

Risk Classification	Criteria
<b>Low/ Normal Risk</b>	<ul style="list-style-type: none"> <li>a. Residence / place of work which is within the Company’s service area;</li> <li>b. Retirement pays, pensions or allotments;</li> <li>c. Corporations or juridical entities with established business;</li> <li>d. Banks, quasi-banks and trust entities authorized by respective state regulators;</li> <li>e. Publicly listed companies subject to regulatory disclosure requirements;</li> <li>f. Government agencies, including government-owned and controlled corporations (GOCCs);</li> <li>g. Accounts with slow moving transactions;</li> <li>h. E-Money or Cash Cards; or</li> <li>i. Long-time (more than 5 years) client of the Company with no change in transaction nature, type, volume, movement and business activity</li> </ul>
<b>High Risk</b>	<ul style="list-style-type: none"> <li>a. Politically Exposed Persons(PEPs):               <ul style="list-style-type: none"> <li>✓ Elected/Appointed Government Officials; or</li> <li>✓ Head of Government Departments and Offices.</li> </ul> </li> <li>b. Customers who have unnecessarily complex or opaque beneficial ownership structure;</li> <li>c. Unexpected high volume of cash transactions of a borrower;</li> <li>d. Online gaming and gambling entities;</li> <li>e. Transactions continuously exceeding threshold; or</li> <li>f. Client from a country that is recognized as:               <ul style="list-style-type: none"> <li>- Having inadequate internationally accepted AML/CFT standards;</li> </ul> </li> </ul>



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

	<ul style="list-style-type: none"> <li>- Does not sufficiently apply regulatory supervision or the Financial Action Task Force (FATF) recommendations; or</li> <li>- Presents greater risk for crime, corruption or terrorist financing</li> </ul> <p>g. Customers from High Risk Business sectors (i.e. Pawnshops, Money Changers, Foreign Exchange Dealers and Remittance Agents, Non-Bank Financial Institutions (NBFIs), Professional Service Providers, Non-Governmental Agencies (non-profits) and cash intensive businesses).</p> <p>h. <b>High-Risk Jurisdiction or Geographical Location.</b>          The personnel shall apply EDD, proportionate to the risks, to accounts, transactions, and business and professional relationships with customers who are nationals or citizens from foreign jurisdiction or geographical location that presents greater risk for ML/TF/PF or its associated unlawful activities, or is recognized as having inadequate internationally accepted ML/TF/PF standards, as determined by the relevant domestic or international bodies. Since the company is only offering products to Filipino citizen, this is not applicable to the extent of foreign jurisdictions. As to national level, the company identified negative areas wherein it did not put branches due to history of collection concerns and other AML and credit risk factors.</p>
--	--

- Clients shall be treated as low/normal risk, unless, classified/ proven to be high risk.
- Sales/Marketing Associates (SA/MA) shall at all times document how a client was profiled for purposes of financing, credit and business relationship.
- Periodic updating of Client information and/or documents specified under **Customer Identification** and **other related Manuals** shall be observed.

Below are the lists the Low/Normal Risk and High Risk clients of the Company:

RISK ASSESSMENT PROFILE (RAF)					
<input type="checkbox"/> <b>NORMAL RISK</b> *Indicate some details/specifications of the chosen item in the space provided.					
INDIVIDUAL EARNINGS	SELF-EMPLOYED	PRIVATE PRACTITIONER	AGRICULTURAL INDUSTRY	BUSINESS	OTHER SERVICES
<input type="radio"/> Salaried Employee	<input type="radio"/> Store	<input type="radio"/> Doctor	<input type="radio"/> Farmer/Fisher	<input type="radio"/> Wholesaler	<input type="radio"/> Construction
<input type="radio"/> Pensioner/Retiree	<input type="radio"/> Leasing Space	<input type="radio"/> Lawyer	<input type="radio"/> Rice Dealer	<input type="radio"/> Distributor	<input type="radio"/> Food/Hospitality
<input type="radio"/> OFW/Allottee	<input type="radio"/> Trucking Business	<input type="radio"/> Accountant	<input type="radio"/> LiveStock Dealer	<input type="radio"/> Manufacturing	<input type="radio"/> Healthcare
<input type="radio"/> Foreign Individual	<input type="radio"/> PUV Operator	<input type="radio"/> Others _____	<input type="radio"/> Others _____	<input type="radio"/> Others _____	<input type="radio"/> Others _____
Please specify: _____					
<input type="checkbox"/> <b>HIGH RISK</b> *Indicate some details/specifications of the chosen item in the space provided.					
HIGH VALUE GOODS	MONEY TRADINGS	NON-PROFIT ORGANIZATION	GAMBLING BUSINESS	SERVICE PROVIDERS	
<input type="radio"/> Pawnshops	<input type="radio"/> Foreign Exchange	<input type="radio"/> Charities	<input type="radio"/> Casino Agent	<input type="radio"/> Business trading via Internet	
<input type="radio"/> Jewelry Shop	<input type="radio"/> Money Changers	<input type="radio"/> Foundations	<input type="radio"/> Lotto Outlet	<input type="radio"/> Virtual/Electronic Currencies	
<input type="radio"/> Car Dealer	<input type="radio"/> Remittance Agent/Center	<input type="radio"/> Religious Sect	<input type="radio"/> Online Gambling Franchise	<input type="radio"/> Private Armed Service Providers	
<input type="radio"/> High Value Items	<input type="radio"/> Lending Business	<input type="radio"/> Civic Organization	<input type="radio"/> Cock Fighting & Horse Race	<input type="radio"/> Arms and Ammunition Dealers	
<input type="radio"/> Vehicle Buy & Sell	<input type="radio"/> Money Transfers/Service	<input type="radio"/> Cultural Associations	<input type="radio"/> Off-Shore Gaming	<input type="radio"/> Networking/Commission Based	
	<input type="radio"/> Private Banking	<input type="radio"/> Cooperatives	<input type="radio"/> Other Gaming Services	<input type="radio"/> Other Cash Incentive Activities	
Please specify: _____					
<input type="radio"/> OTHERS					



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**2) Due Diligence**

- Sales/Marketing Associates shall conduct **due diligence** based on how Clients were profiled. The required due diligence shall be as follows:

Due Diligence	Type of Customers
Average Due Diligence (ADD)*	Low/Normal Risk
Enhance Due Diligence (EDD)	High Risk

\*Average Due Diligence is the standard due diligence to be performed by the personnel for low risk and normal risk applicants and customers of the Company.

- Steps in performing due diligence

Due Diligence	Actions				
Average Due Diligence*	<ul style="list-style-type: none"> <li>➤ Obtain <b>minimum information and acceptable identification documents</b> specified in <b>Customer Identification</b> provisions.</li> <li>➤ Conduct <b>validation procedures</b> on any or all of the information provided such as, but not limited to, the following:               <table border="1" data-bbox="570 1010 1370 1606"> <thead> <tr> <th>Individual</th> <th>Corporate/Juridical Entities</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> <li>• Confirm the date of birth from a duly authenticated official document (e.g. Compare the date of birth from the valid ID submitted by the client)</li> <li>• Verify the permanent address through evaluation of utility bills, bank or credit card statement or through on-site visitation;</li> <li>• Determine the authenticity of identification documents through validation of issuance by requesting a certification from the issuing authority or by any other means; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul> </td> <td> <ul style="list-style-type: none"> <li>• Require the submission of audited financial statement (AFS) conducted by a reputable accounting/ auditing firm;</li> <li>• Inquire from the supervising authority the status of the entity;</li> <li>• Obtain bank references;</li> <li>• Conduct on-site visit to the company; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul> </td> </tr> </tbody> </table> </li> </ul>	Individual	Corporate/Juridical Entities	<ul style="list-style-type: none"> <li>• Confirm the date of birth from a duly authenticated official document (e.g. Compare the date of birth from the valid ID submitted by the client)</li> <li>• Verify the permanent address through evaluation of utility bills, bank or credit card statement or through on-site visitation;</li> <li>• Determine the authenticity of identification documents through validation of issuance by requesting a certification from the issuing authority or by any other means; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul>	<ul style="list-style-type: none"> <li>• Require the submission of audited financial statement (AFS) conducted by a reputable accounting/ auditing firm;</li> <li>• Inquire from the supervising authority the status of the entity;</li> <li>• Obtain bank references;</li> <li>• Conduct on-site visit to the company; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul>
Individual	Corporate/Juridical Entities				
<ul style="list-style-type: none"> <li>• Confirm the date of birth from a duly authenticated official document (e.g. Compare the date of birth from the valid ID submitted by the client)</li> <li>• Verify the permanent address through evaluation of utility bills, bank or credit card statement or through on-site visitation;</li> <li>• Determine the authenticity of identification documents through validation of issuance by requesting a certification from the issuing authority or by any other means; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul>	<ul style="list-style-type: none"> <li>• Require the submission of audited financial statement (AFS) conducted by a reputable accounting/ auditing firm;</li> <li>• Inquire from the supervising authority the status of the entity;</li> <li>• Obtain bank references;</li> <li>• Conduct on-site visit to the company; and</li> <li>• Contact the Client by phone</li> <li>• Send "Thank You letter" via registered mail</li> </ul>				

In strictly limited circumstances and where there is proven low risk of ML/TF/PF, the SAs may issue guidelines allowing certain exemptions on CDD measures, taking into account the nature of the product, type of business and the risks involved; Provided, that ML/TF/PF risks are effectively managed.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- In the conduct of Enhanced Due Diligence (EDD), a copy of the **Client Risk Assessment Form (CRAF)** is made integral.

Due Diligence	Actions			
Enhanced Due Diligence	Observe actions a and b under Average Due Diligence			
	<p>When conducting EDD, covered persons shall perform the following:</p> <p>(a) Gather documents to support the:</p> <ol style="list-style-type: none"> <li>(1) Sources of wealth and fund;</li> <li>(2) Nature of occupation and/or business;</li> <li>(3) Reason for intended or performed transaction; and</li> <li>(4) Other identification information, which the covered person deems necessary to verify the identity of the customer, and their agents and beneficial owners.</li> </ol> <p>(b) Conduct additional validation procedures, such as:</p> <ol style="list-style-type: none"> <li>(1) verifying volume of assets, information available through public databases, internet and other records;</li> <li>(2) verifying the declared residence address and conducting face-to-face contact with the customers, and their agents and beneficial owners; and</li> <li>(3) other modes of validation, which the covered person deems reliable and practical.</li> </ol> <p>(d) Conduct enhanced ongoing monitoring, including more frequent or regular updating of identification information and identification documents;</p> <p>(c) Secure the approval of senior management to commence or continue transacting with the customer;</p> <p>(e) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and</p> <p>(f) Such other measures as the covered persons may deem reasonable or necessary.</p> <p>Obtain <b>additional information</b> other than the minimum information and/or documents such as but not limited to the following:</p> <table border="1" data-bbox="574 1381 1354 1877"> <thead> <tr> <th data-bbox="574 1381 956 1413">Individual</th> <th data-bbox="956 1381 1354 1413">Corporate/ Juridical Entities</th> </tr> </thead> <tbody> <tr> <td data-bbox="574 1413 956 1877"> <ul style="list-style-type: none"> <li>• List of banks where the Client has maintained or is maintaining an account;</li> <li>• List of companies or businesses where the Client is a director, officer or stockholder or authorized signatory; and</li> <li>• <b>If non-resident of the Company's service area</b>– reason for opening an account with the Company despite residence is outside of the service area</li> <li>• <b>If Non-Resident Alien/ Citizen and Client from a country recognized as having inadequate</b></li> </ul> </td> <td data-bbox="956 1413 1354 1877"> <ul style="list-style-type: none"> <li>• Prior or existing corporate references</li> <li>• Name, present address, date and place of birth, nature of work, nationality and source of funds of each of the primary officers (i.e., President, Treasurer and authorized signatories), stockholders owning at least two percent (2%) of the voting stock and directors/ trustees/ partners as well as their respective identification documents</li> <li>• <b>For pawnshops, money changers, foreign exchange dealers and</b></li> </ul> </td> </tr> </tbody> </table>	Individual	Corporate/ Juridical Entities	<ul style="list-style-type: none"> <li>• List of banks where the Client has maintained or is maintaining an account;</li> <li>• List of companies or businesses where the Client is a director, officer or stockholder or authorized signatory; and</li> <li>• <b>If non-resident of the Company's service area</b>– reason for opening an account with the Company despite residence is outside of the service area</li> <li>• <b>If Non-Resident Alien/ Citizen and Client from a country recognized as having inadequate</b></li> </ul>
Individual	Corporate/ Juridical Entities			
<ul style="list-style-type: none"> <li>• List of banks where the Client has maintained or is maintaining an account;</li> <li>• List of companies or businesses where the Client is a director, officer or stockholder or authorized signatory; and</li> <li>• <b>If non-resident of the Company's service area</b>– reason for opening an account with the Company despite residence is outside of the service area</li> <li>• <b>If Non-Resident Alien/ Citizen and Client from a country recognized as having inadequate</b></li> </ul>	<ul style="list-style-type: none"> <li>• Prior or existing corporate references</li> <li>• Name, present address, date and place of birth, nature of work, nationality and source of funds of each of the primary officers (i.e., President, Treasurer and authorized signatories), stockholders owning at least two percent (2%) of the voting stock and directors/ trustees/ partners as well as their respective identification documents</li> <li>• <b>For pawnshops, money changers, foreign exchange dealers and</b></li> </ul>			



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

	<p><b>AML standards</b> – legitimate purpose of the account</p>	<p><b>Remittance Agents</b>– AML Training Certificate of the authorized signatories</p> <ul style="list-style-type: none"> <li>• <b>For Cooperatives, except, cooperative Banks</b> – main purpose of the Cooperative</li> </ul>	
<p align="center"><b>For both individual and corporate/ juridical entities accounts with unexpected high volume of cash transactions</b> – determine the source of large volume of cash.</p>			
<p>Obtain approval from <b>Senior Management</b> for establishing business relationship.</p>			

- Senior Management shall refer to any of the following officers:
  - Executive Officer; and
  - Senior Sales Associate
  
- Sales Associates shall conduct EDD if the concerned unit of the Company acquires information in the course of account and transaction monitoring that:
  
- Raises doubt as to the accuracy of any information or document provided or the ownership of the entity;
  
- Justifies re-classification of the customer from low/normal risk to high risk such as but not limited to the following:
  - Deviation from the known threshold/capacity of the client as documented on the initial risk assessment (CRAF).
  - Change in the client profile (e.g. regular account to FX trading, remittance agents or money changers)
  - Any of the circumstances for the filing of a suspicious transaction exists.
  - The type of due diligence applied shall be documented **at all times** using the prescribed forms

Further, the Company shall apply **enhanced due diligence** on its customers if it acquires information in the course of its customer account or transaction monitoring that:

- Raises doubt as to the accuracy of any information or document provided or the ownership of the entity
- Justifies re-classification of the customer from normal risk to high-risk pursuant to these rules or by its own criteria;
- Any of the circumstance for the filing of a suspicious transaction exists such as but not limited to the following:
  - Transacting without any underlying legal or trade obligation, purpose or economic justification;
  - Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profiles



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- Structuring of transactions in order to avoid being the subject of covered transaction reporting; or
  - Knowing that a customer was engaged or is engaged or engaging in any unlawful activity.
- **Timing of CDD Measures. The personnel shall conduct appropriate customer due diligence measures before opening, renewal and updating of an account including the following procedures:**
    - (a) Customer Identification Process;
    - (b) Customer Verification Process;
    - (c) Identification and Verification of Agents;
    - (d) Beneficial Ownership Verification;
    - (e) Determination of the Purpose of Relationship; and
    - (f) Ongoing Monitoring Process;
  - **When CDD is required. The personnel shall undertake CDD measures when:**
    - (a) Establishing business or professional relationship;
    - (b) Carrying out occasional transactions above (Php 100,000.00) or any other threshold as may be determined by the relevant SAs, with notice to the Council, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked;
    - (c) Carrying out occasional wire transfers in the circumstances under Rule 19, Section 6 hereof;
    - (d) There is a suspicion of ML/TF/PF, regardless of any exemptions or thresholds that are referred to elsewhere under this IRR; or
    - (e) The covered person has doubts about the veracity or adequacy of previously obtained identification information and/or data.
  - **Existing Customers. Customer Due Diligence is also apply to existing customers on the basis of materiality and risk, the CDD is conducted on existing relationships at the time of update of profile, account renewal or performing a credit review since CDD have previously been undertaken and the adequacy of information and document obtained from the client.**

## 2. CUSTOMER VERIFICATION

Customers and/ or authorized signatories of a corporate or juridical entity who engage in a financial transaction with the Company for the first time presents the original and submit a clear copy of **at least one (1) valid photo-bearing ID issued by an official authority**. Official authority shall refer to any of the following:

- Government of foreign jurisdiction or of the Philippines, if applicable;
- Its political subdivisions and instrumentalities;
- Government Owned and/ or Controlled Corporations (GOCCs); or
- Private entities or institutions registered with or supervised or regulated by the government or state of foreign jurisdiction, or by the Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI), Bangko Sentral ng Pilipinas (BSP), if applicable.



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- Photocopies shall be signed and stamped with “**Original Seen and Verified**” by the Sales Associate who is responsible for authentication;
- Submission of a valid ID shall be on a **one-time basis only** at the commencement of business relationship;
- The Company shall require customers to submit an updated photo and other relevant information on the basis of risk and materiality;
- The Company may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer.
- Whenever it deems necessary, the Company may accept other IDs not enumerated above (e.g., birth certificate, marriage contract); provided, that, it shall not be the sole means of identification.
- The Company may utilize its own technology to take the photo of the customer or authorized signatory, in cases when:
  - the acceptable identification documents do not bear any photo; or
  - the photo-bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory.

Notwithstanding the reliability and authenticity of identification and documentary requirements, a separate background checking is indispensable in reinforcing the conduct of KYC. The said background checking shall be reduced in a written report. Positive and negative items about the borrower shall be included and be clearly indicated for appreciation of the approving authority.

### WATCHLIST VALIDATION

Before establishing business relationship, the Sales and Marketing personnel of the Company shall check if the customers if they are engaged in illegal activities or terrorist related activities as circularized by the BSP, AMLC, and other international entities or organizations, such as the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List.

Sales and Marketing personnel shall use the KaiserCheck database in watchlist validation. This is provided by 64ai Inc., a platform provider that focuses on Regulatory Technology (RegTech). The database includes (a) Domestic Politically Exposed Persons (PEPs), (b) Most wanted individuals listing from FBI, PNP, PDEA, NBI and Interpol, (c) Watch-listed names of individuals based on negative media reports (publiclyavailable sources) and AMLC Resolutions, (d) SEC Advisories on Investment Scams, (e) Philippine Ambassadors and Consul Generals, (f) AMLC Freeze Orders and ATC Watchlist Designations (g) International Sanction Listings such as Office of Foreign Assets Control (OFAC) list, United Nations Security Council (UNSC) consolidated list, European Union Financial Sanction (EUFS) list, Consolidated Canadian Autonomous Sanctions (CCAS) List, Office of Financial Sanctions Implementation (OFSI) list or HMT list.

The Sales and Marketing personnel shall upload the result of the screening in the CRM system of the Company. They also need to use Google Search for enhance due diligence to check if the customer has derogatory records



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

and adverse information in 34 predicate crimes. Result in Google search shall also be uploaded to the CRM system.

**1.) Positive Match.** In case confirmed positive match, the branch/unit should politely decline the loan application. The Sales and Marketing Personnel shall immediately report to the Compliance Department copy furnishes the Area Head and Group Head. The Compliance Department shall report it to the AMLC within 24 hours.

**2.) Negative Match.** In case of negative match, the Sales and Marketing personnel shall proceed to next step of loan transactions. It is subject for further evaluation of the Credit Review personnel.

### **MINIMUM VALIDATION PROCEDURES**

Validation procedures for individual customers to be conducted by the Branch or Business Unit personnel shall include but is not limited to the following:

- Confirming the date of birth from a duly authenticated official document;
- Verifying the permanent address through evaluation of utility bills, bank or credit card statement or other documents showing permanent address or through on-site visitation;
- Contacting the customer by phone, email or letter (such as sending of “thank you letters”); and
- Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other means.
- Customer under fictitious name shall be absolutely prohibited.
- Where a customer is not clearly acting on his own behalf, reasonable measure should be taken to obtain information about the true identity of the principal.

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

- Requiring the submission of audited financial statements conducted by a reputable accounting/auditing firm;
- Inquiring from the supervising authority the status of the entity;
- Obtaining bank references;
- On-site visitation of the Financing Company; and
- Contracting the entity by phone, email or letter (such as “thank you letters”).

When in doubt whether such person is being used as dummies in circumvention of existing laws, make necessary inquiries to verify the status of the business relationship between the parties.

### **3. IDENTIFICATION AND VERIFICATION OF AGENTS**

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

Where an account is opened or an occasional transaction in excess of the threshold is conducted by any person in behalf of another, covered persons shall establish and record the true and full identity and existence of both



#### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

the account holder or person purporting to act on behalf of the customer, and the beneficial owner or the principal on whose behalf the transaction is being conducted.

The Company shall verify the validity of the authority of the agent. In case it entertains doubts as to whether the account holder or person purporting to act on behalf of the customer is being used as a dummy in circumvention of existing laws, it shall apply EDD and file an STR, if warranted

#### **4. ULTIMATE BENEFICIAL OWNERSHIP (UBO)**

The Sales and Marketing personnel shall also identify the beneficial owner of the customer, if it is a juridical entity/ corporation. The said personnel shall check this to the updated General Information Sheet (GIS) being submitted. If it is not indicated in the GIS, the said personnel shall use any of the three approaches including Ownership Prong (at least 25% direct/indirect ownership), Control Prong (exercising control over the corporation) and Senior Management Officials. This is to determine who ultimately owns or controls the customers and/or whose behalf a transaction or activity is being conducted; or those who has ultimate effective control over a legal person or arrangement. If the company is publicly-listed, the said personnel can check the GIS in the website of the company.

The Sales and Marketing personnel shall verify the identity of the beneficial owner same with the process of individual customer, before establishing business relationship. These include UBO acceptance, UBO verification, due diligence procedures, watch list validation, risk profiling and assessment, etc.

#### **1. DETERMINATION OF THE PURPOSE OF RELATIONSHIP**

The Company shall understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or the business or professional relationship with their customers.

#### **2. ONGOING MONITORING PROCESS (OMP) OF CUSTOMER'S INFORMATION AND ACCOUNTS/TRANSACTIONS**

**General Requirement for OMP.** The Company, on the basis of materiality and risk, conduct ongoing monitoring by establishing a system that will enable them to understand the normal and reasonable account or business activity of customers, and scrutinize transactions undertaken throughout the course of the business or professional relationship to ensure that the customers' accounts, including transactions being conducted, are consistent with the covered person's knowledge of its customer, their business and risk profile, including where necessary, the source of funds.

**EDD After Conduct of OMP .** The Company shall apply EDD on the customer if it acquires information in the course of its customer account or transaction monitoring that:

- (a) Raises doubt as to the accuracy of any information or document provided or the ownership of the juridical person or legal arrangement;
- (b) Justifies reclassification of the customer from low or normal risk to high risk, pursuant to this IRR;
- (c) Indicates that any of the suspicious circumstances, as herein defined, exists.

**Review and Updating of Records.** Covered persons shall, based on materiality and risk, ensure that information and documents collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers. Updating of records shall be mandatory when enhanced OMP is warranted.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

Type of Customers	Frequency
Low/Normal Risk Customers	Every three (3) years
High Risk Customers	Every year

### SHELL BANK, SHELL COMPANY AND BEARER SHARE ENTITY

- The Company shall always apply EDD on both the entity and its beneficial owners when dealing with a shell company.
- The Company shall refuse to deal, enter into, or continue, correspondent banking relationship with shell banks. They shall likewise guard against establishing relations with foreign financial institutions that permit their accounts to be used by shell banks.
- When the company is dealing with bearer share entities shall be required to conduct EDD diligence on said entities and their existing stockholders and/or beneficial owners at the time of opening of the account, it shall be subject to ongoing monitoring procedure at all times and the list of stockholders and/or beneficial owners shall be updated within thirty (30) days after every transfer of ownership and the appropriate enhanced due diligence shall be applied to the new stockholders and/or beneficial owners.

## II. PREVENTIVE MEASURES FOR SPECIFIC TRANSACTION AND ACTIVITIES

The Company implemented preventive measures required in the relevant AML/CTPF regulations and standards which is already incorporated in the IRA report, which is also attached on this MTPP.

## III. 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, judiciary or military officials, senior executives of government or state owned or controlled corporations and important party officials.

### 1. REQUIREMENTS ON POLITICALLY EXPOSED PERSONS (PEP)

Endeavor to establish and record the true and full identity of PEPs as well as their immediate family members and the entities related to them and apply enhanced due diligence. Refer to **Annex D** for list of PEPs. The due diligence to be applied for customers that are assessed by the Company as high-risk for money laundering and terrorist financing is **enhanced due diligence**.

Upon the establishment of the business relationship, identify if the customer is a PEP by asking the necessary questions, performing database check, referring to publicly available information, and so forth. Prior approval by senior management is needed before establishing a business relationship with a PEP. For some existing customers who become PEPs after they enter a business relationship with the Company, the Sales and Marketing personnel shall use the KaiserCheck or publicly available information to identify such individuals. Once identified, this should be reviewed and included among the PEP list and enhanced due diligence requirements must be applied.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 2. POLICIES / REQUIREMENTS ON POLITICALLY EXPOSED PERSONS (PEP)

Apply Enhance Due Diligence to All PEPs, Foreign and Domestic Laws and regulations should make no distinction between domestic and foreign PEPs. Enhanced due diligence for both foreign and domestic PEPs must be adopted.

- **Require a Declaration of Beneficial Ownership**  
At the establishment of business relationship and as needed thereafter, the Company shall require customers to complete a written declaration of the identity and details of natural person (s) who are the ultimate beneficial owner (s) of the business relationship or transaction as a first step in meeting their beneficial ownership customer due diligence requirements.
- **Request Asset and Income Disclosure Forms**  
A public official should be asked to provide a copy of any asset and any income declaration form filed with their authorities, as well as subsequent updates. If a customer refuses, the bank should assess the reasons and determine, using a risk-based approach, whether to proceed with the business relationship.
- **Periodic Review of PEP Customers**  
Senior management or a committee including at least one Senior Manager using a risk-based approach, at least yearly should review PEP customers and the results of the review should be documented.
- **Frequency of monitoring PEP's, high risk client/s**  
The unit compliance designate shall be responsible for the periodic evaluation of high risk client/s such as existence of customers and completeness of the minimum information and or documents establishing the true and full identity of, and the extent of enhance due diligence.
- **Updating of PEPs. Once a PEP, always a PEP.**
- **Frequency of updating KYC Documents**  
Client Risk Rating Form shall be updated by the SCO-compliance designate every one (1) year from the date it was prepared.
- **Avoid Setting Limits on the Time a PEP remains a PEP.**  
When a person has ceased to be entrusted with a prominent public function, the Bank should not introduce time limits on the length of time the person, family member, or close associate needs to be treated as a PEP.

### 3. CROSS-CHECKING OF CLIENT'S NAME AGAINST WATCHLIST DATABASE

The branch or responsible unit shall cross-check client's name as well as the beneficial owners, beneficiaries and authorized signatories (individual and corporate) against the negative watchlist (OFAC, UN Sanctions List, Al Qaeda, AMLC, BSP, negative news and advisories, Targeted Financial Sanctions) before establishing business relationship.

The screenshot of the cross-checking should be included in the KYC documents of the specific account.



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

Politically Exposed Person or PEP refers to an individual who is or has been entrusted with prominent public position in

- the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources;
- a foreign state, or
- an international organization. Loan Application of PEP shall be subject to Senior Management Approval.

## **IV. REPORTING OF COVERED TRANSACTIONS AND SUSPICIOUS TRANSACTIONS**

### **1. MONITORING AND REPORTING / RED FLAGGING OF TRANSACTIONS:**

**Covered Transaction** is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (P500,000.00), Philippine Currency, or its equivalent in any foreign currency on a day's prevailing foreign exchange rate, within one (1) business day.

**Suspicious Transaction** is a transaction, regardless of amount, where any of the circumstances exists as defined in the Definition of Terms.

**Unlawful Activity** (also termed as “**Predicate Crimes**”) enumerated in the Definition of Terms.

#### **Recognition of Suspicious Transactions:**

Suspicious transactions shall refer to transactions as defined in this Policies and Guidelines.

Since the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction.

Any and all executive officer or sales associate, upon receipt of information related to any unlawful activities under AML/CFT, shall immediately disseminate to appropriate and concerned units for verification on the existence of clients/accounts. An Officer of the Company shall require complete report from the concerned units and shall immediately report the information to the Compliance Officer or any Executive Officer in charge of the Company.

#### **Flagging /Monitoring of Transactions**

The Company through its Compliance Department has a mechanism of flagging and monitoring transactions to ensure compliance with functionalities as those required herein until an automatic system of flagging will put in place.

In coordination with Treasury Department, the Compliance Department is assessing/evaluating the list of pre-terminated accounts for the month. These include pre-payment of loan amortization exceeding 50K within the month and full payment/termination of accounts. Upon identification and assessment, this will be reported to the AML Committee for final approval.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### Suspicious Transactions (ST) During Loan / Credit Application

**Pre-Credit Evaluation and Assessment** is the preliminary analysis of a potential borrower by the Company to determine whether they can be eligible for funding, or to pay for products within a specified period or to undertake credit accommodation pending examination of worthiness and risk involved.

At this stage, indicators of suspicion shall be recognized whether or not to grant a borrower's request for credit or financial accommodation.

For purposes of ST reporting in case suspicion or doubtful conjecture at this stage, Sales/Marketing personnel shall observe the following protocols:

- 1<sup>st</sup> : Identify suspicious criteria or indicator during loan documentation and review;
- 2<sup>nd</sup> : Reduce in written report the basis for the suspicion by stating the justifiable grounds or reasons for such determination and upload said findings and documentation in the loan system;
- 3<sup>rd</sup> : If suspicious circumstances were established, to tick the criteria or indicator as provided in the loan system;
- 4<sup>th</sup> : Advise the Credit Committee of such suspicious transaction for appropriate disposition; and
- 5<sup>th</sup> : Notify the Compliance Officer for regulatory reporting, without prejudice and in support of the data extraction from the loan system.

In case of doubt whether the circumstances surrounding the loan application is suspicious within the ambit of the law, legal definition or requirement, it shall be resolved as suspicious transaction and the Compliance Officer shall finally dispose of the issue for reporting or non-reporting purposes.

It is the responsibility of the Compliance Officer to check on a daily basis and extract systematically suspicious loan applications as indicated and documented through the loan system of the Company.

The Compliance Officer shall periodically (i.e. Board of Directors' Meeting), or whenever necessary, advise and present to the Board of Directors suspicious transactions reported or uploaded in the AMLC portal.

### Suspicious Transactions During Loan / Credit Term

**Post-Credit Evaluation and Assessment** refers to the process of ascertaining the continuous eligibility of the borrower after a loan or credit accommodation is granted by the Company. It simply refers to the continuity of qualification and none of the disqualification of the borrower's acceptability in reference to financial, reputation or business activity which served as basis of loan granting and should be possessed all throughout the term of the loan.

Considering that suspicious circumstances may arise during the term of the loan, all existing loan accounts shall be subjected to bi-annual post-credit checking by Sales/Marketing personnel who owns the account, which, update (positive or negative scenarios) shall be contained in a Call Report, without prejudice to verification or validation of its veracity by the Company's Quality Assurance Department. The Quality



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

Assurance Department shall not be precluded to conduct its post-credit checking periodically and as warranted.

**Suspicious Transaction Committed by Stakeholders**

Suspicious transactions are not confined to external clients’ commission of any unlawful activity. The Company’s stakeholders (shareholders, directors, officers and employees) can be held accountable for AML/CFT violations, which can be committed individually or collectively, for financial gain or relational consideration.

In any case or manner of commission violative of AML/CFT regulatory provisions, the Compliance Officer shall be immediately notified of such suspicious occurrences for purposes of disposition and propriety of ST reporting. The Compliance Officer shall be provided with copies of relevant documents for evaluation and assessment as to propriety of ST reporting.

**Indicators / Criteria of Suspicious Transactions (ST):**

Whether during loan application, during its term or those AML/CFT violations committed by stakeholders, the following are some examples of the most basic ways in which money may be laundered, be sourced for terrorist financing and for other unlawful activity, thereby, creating an impression of suspicion or doubt on the probity of a transaction or business activity. Identification of any of the examples should prompt initial inquiries and, if necessary, further investigation as to the details of the transaction:

Type	Examples
1. There is no underlying legal or trade obligation, purpose or economic justification	a. Loan purpose is disparate or inconsistent with the business activity of the borrower; b. A customer who is reluctant to state a purpose or source, or provides a questionable purpose and/ or source; or c. Fraud, misrepresentation or submission of forged documents, inclusive of security or collateral papers.
2. The Client is not properly or particularly identified	a. Any major discrepancy or mismatch in the personal identifiable information of the borrower upon examination of minimum documentary requirements; b. Pertinent or apposite inconsistencies in the borrower’s information provided vis-à-vis result of personal / background checking; or c. Background checking does not contain material detail for profiling purposes.
3. The amount involved is not commensurate with the business or financial capacity of the Client	a. Amount being borrowed or granted is far higher than aggregated source of income or cash flow for repayment purposes; b. Amount being borrowed or granted is far lower than aggregated source of income or cash flow for repayment purposes; or c. Amount being borrowed or granted relative to financial position does not match the business or income generating activity of the borrower.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

<p>4. Taking into account all known circumstances, it may be perceived that the Client's transaction is structured in order to avoid being the subject of reporting requirements under the Anti-Money Laundering Act (AMLA), as amended</p>	<p>a. Customer has applied for or maintaining multiple loan accounts in amounts not exceeding ₱500,000.00 for the same loan purpose or of different purposes absent of proof of such utilization for the purpose indicated</p>
<p>5. Any circumstance relating to the transaction which is observed to deviate from the profile of the Client and/or Client's past transactions with the covered institution</p>	<p>a. Major deviation from the Company's business process and protocols on loan approvals; or b. Loan proceeds was used for a different purposes other than what it was intended during application.</p>
<p>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</p>	<p>a. Any act that can be related to predicate crimes aforementioned whether be directly or indirectly related or committed and whether the customer acted as principal, accomplice or accessory to the unlawful activity.</p>
<p>7. Any transaction that is similar, analogous or identical to any of the foregoing or may be not suspicious under Section 3 (B-1) of the AMLA, as amended.</p>	<p>a. Customer who repays problem loans unexpectedly; or b. Request to borrow against assets held by the Company or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing; or c. Request by a customer for the Company to provide or arrange financing where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.</p>

**Covered Transaction also a Suspicious Transaction.**

Should a transaction be determined to be both a covered and a suspicious transaction, the same shall be reported as a suspicious transaction. In this regard, it shall be reported first as a CTR, subject to updating if it is finally confirmed to be reportable as STR.

**Submission of CTR and STR:**

Submission of Covered/ Suspicious Transaction Reports (CTR/ STR)

Particulars	Covered Transaction	Suspicious Transaction
<b>Prescribed Format</b>	Electronic File – CSV Format (encrypted)	Electronic File – CSV Format (encrypted) <b>and</b> STR Documents
<b>Frequency</b>	Daily	As necessary
<b>Responsible for Submission</b>	AML Compliance Officer or Specialist	AML Compliance Officer or Asset-Backing Auditor



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

<b>Deadline of Submission to AMLC, SEC or other regulatory agencies</b>	<b>Within five (5) working days</b> from date of transaction or as prescribed by the supervising authority	<b>Next working day</b> from date of discovery or date of approval by the Board of Directors, whichever is earlier.
---	--	---

The Board of Directors designated the Chief Compliance Officer and AML Compliance Officer as the reporting users (primary and alternate) and has been registered with the AMLC as authorized by the Company to transmit electronically the CTR and STR.

Submission of CTRs beyond 12:01 am of the day following the 5th working day from occurrence of the transaction shall be considered as non-compliance with the requirement to file CTRs in accordance with the standard set by the AMLA, and may be subject to appropriate administrative sanctions, if circumstances so warrant.

The Compliance Department shall report to the AMLC all covered transactions, regardless of the mode of payment used in the settlement thereof, including transactions in checks, fund transfers, and/or debiting or crediting of accounts, except those transactions that are deferred for reporting to the AMLC and covered under the low risk transactions.

**Processing and Generation and Submission of CTR**

Covered Transaction Reports (CTRs) shall be generated by the AML Compliance Officer every after two (2) working days thru ‘Data Extractor’, an internally made database. The AML Compliance Officer shall check the completeness and accuracy of the report being extracted. He shall coordinate with the specific department (i.e. Loans and IT) if there are issues/concerns noted.

The said CTR report shall be forwarded to the Chief Compliance Officer (CCO) to verify the veracity of the report. Once it is already reviewed and approved, the AML Compliance Officer shall sign and encrypt the report using Kleopatra. Afterwards, the encrypted report shall be submitted by the AML Compliance Officer to the AMLC portal on the third day thru the registered/official access provided and its institution code.

The AML Compliance Officer shall document all the submitted CTRs by uploading to the One Drive. This can be accessed by all personnel of the Compliance Department.

All CTRs submitted within the month shall be reported to the AML Committee, Corporate Governance Committee and Board of Directors in their meetings of the following month for confirmation and notation.

Retention and custody of records / files:

Record / File	Retention Period	Designated Custodian
CTR Electronic File	<b>Five (5) years</b> from transaction date	AML Compliance Officer

**Processing and Generation and Submission of STR**

Suspicious transaction shall be reported to the AML Committee and Corporate Governance Committee via meetings. The Chief Compliance Officer shall present to the committees all the pertinent facts, information and



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

documents for the grounds of suspicion. This may also contain suspicious events, news or publication on alleged involvement of the Client.

These shall be properly documented by the AML Compliance Officer and should be readily available upon request.

STR covers all transaction, whether attempted or completed. List of STRs and unlawful activities and grounds for suspicions are listed/enumerated in the Definition of Terms.

Once the transaction was approved to be suspicious, a report shall be processed by AML Compliance Officer for electronic submission of report to AMLC portal. Same process in submission of CTR shall be followed.

Compliance Officer shall provide list of STRs submitted for a period to the Board of Directors during the regular meeting for their reference, notation and confirmation.

The Sales and Marketing Personnel and Credit Reviewer shall establish or determine the existence of any of the suspicious circumstances enumerated thereto in any transaction or activity, including any attempt thereof, within ten (10) calendar days from the date of the transaction or from the date the covered person knew of or should have known the suspicion or suspicious nature of the transaction regardless whether such suspicious circumstances are embedded or conclusively incorporated in the transaction monitoring system (TMS); provided, however, that for transactions that are related to an unlawful activity, the provisions in the next paragraph shall apply.

For transactions or persons related to an unlawful activity and Marketing Personnel and Credit Reviewer shall establish or determine that the transaction is in any way related to an unlawful activity, or the person transacting is involved in or connected to an unlawful activity or money laundering offense, including any attempt thereof, within a reasonable period of time, which in no case shall exceed sixty (60) calendar days from the date of the transaction or from the date the covered person knew of or should have known such suspicion or suspicious nature of the transaction regardless whether such suspicious circumstances are embedded or conclusively incorporated in the transaction monitoring system (TMS).

Such determination period shall allow covered persons to gather facts in order to enable the submission of a meaningful STR.

## **2. REPORTING OF SUSPICIOUS TRANSACTIONS**

Suspicious transaction (ST) refers to a transaction with a covered person, regardless the amount involved. Refer to the Definition of Terms for the list of STRs, predicate crimes and unlawful activities.

To ensure that the Suspicious Transactions Reports (STR) being submitted to the Anti-Money Laundering Council (AMLC) are complete and accurate, the following minimum procedure shall be carried out:

- Where any employee or personnel, director or officer knows that a client has engaged in any of the unlawful activities under the AMLA, the matter must be promptly reported to the AML Compliance Officer or Chief Compliance Officer.
- Suspicious transactions, as defined under AMLA and this Manual, shall be reported by the Branch Manager/Head of the branch/unit to the AML Compliance Officer or Chief Compliance Officer



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

using the Incident Reporting the next working day after occurrence of the incident/s rendering such transaction as suspicious.

- After review, the AML Compliance Officer shall inform the reporting branch/unit of any information that needs to be corrected – the next working day.
- The AML Compliance Officer or Chief Compliance Officer shall then correct the STR based on the review made. If everything is in order, a soft copy of the report will be sent through e-mail. A hard copy of the STR shall be printed and signed by the Branch Manager/Head.
- AML Compliance Officer or Chief Compliance Officer shall generate a CSV file of the Suspicious Transaction Report (STR) and send the same to AMLC using the system.
- The signed hard copy of the STR shall be transmitted to AML Compliance Officer or Chief Compliance Officer for final review where the Compliance Officer signs the recommending approval and the same is forwarded for final approval to the General Manager or in her absence, the Assistant General Manager.
- The approved copy of the STR shall then be transmitted by Compliance Office to AMLC on the next working day from date of the occurrence of the suspicious transaction. Likewise, the CSV file shall be generated by AML Compliance Officer or Chief Compliance Officer and transmitted to AMLC via FTP.
- When reporting suspicious transactions to the AMLC, the Company and its officers and employees, are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person, entity, the media, the fact that a suspicious transaction report was made, the contents thereof, or any other information in relation thereto. Neither may such reporting be published or aired in any manner or form by the mass media, electronic mail, or other similar devices. In case of violation thereof, the concerned officer and employee of the Company or the media shall be held criminally liable.

## **V. CONFIDENTIALITY AND TIPPING-OFF**

### **Failure to Satisfactorily Complete CDD.**

When the applicant/customer is unable to comply with the relevant CDD measures, the personnel shall:

- (a) refuse to open an account, commence business relations or perform the transaction; or shall terminate the business relationship; and
- (b) File an STR in relation to the customer, if circumstances warrant.

### **CDD and Tipping-off.**

In cases where the personnel form a suspicion of ML/TF/PF and associated unlawful activities, and they reasonably believe that performing the CDD process will tip-off the customer, they need not pursue the CDD process, but should file an STR, closely monitor the account, and review the business relationship.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### VI. TRAINING AND CONTINUING EDUCATION PROGRAM

#### 1. SUBJECT CONTENT

The training module covers the salient provisions of the Anti-Money Laundering Law as amended and the guidelines contained in the MTPP. Additionally, new rules and regulations including Implementing Rules and Regulations, such as RA No. 9160 and RA No. 10168 shall be covered in the training. It should be updated at least every after (2) years for refresher trainings and immediately for new hires and for specific needs.

#### 2. EMPLOYEE COVERAGE

- Key Personnel and Front-liners
- Senior Officers
- Non-Key Personnel / Back-office Personnel
- New hires

#### 3. ATTENDANCE AND FREQUENCY OF TRAINING

- All employees not categorized as key personnel shall receive AML training every after two (2) years
- For Key Personnel, refresher training shall be given every after two (2) years
- For Senior Officers, frequency of training will depend on the function of the unit or group and need to attend refresher course every after two (2) years
- For new hires, need to attend AML Orientation at least one (1) month after onboarding

#### 4. ASSESSMENT

- Assessment/examination shall be after the end of the training/seminar to test the knowledge of the attendees.
- The attendee shall meet the passing score given by the resource speaker
- The Compliance Department shall document the assessment/examination

#### 5. DOCUMENTATION

- Human Resource Department shall document the attendance of the trainings conducted
- Certificate of Attendance shall be given to those who attended and passed the assessment
- Materials being used in the training shall be kept by the Compliance Department

#### 6. OTHER TRAININGS

- The Compliance Department shall give other trainings and seminar when there are new rules and regulations specific for AML compliance
- The Compliance Department shall give training if there are new policies to be implemented



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 7. SANCTIONS AND PENALTIES

- Employees who did not attend the AML training and seminar shall be given corresponding sanctions including those who failed to pass the assessment.

#### Non-attendance

1. Written explanation
2. Reprimand/warning
3. Suspension

#### Failed in the assessment/examination

1. Retake the examination
2. Re-attend the training/seminar
3. Suspension

## VII. RECORD KEEPING AND RETENTION ON DIGITIZATION OF CUSTOMERS RECORD

### 1. CENTRALIZED DATABASE

The Company developed Customer Relationship Management (CRM), an internal centralized database of customer records to be maintained by the Information Technology (IT) Group. This is also in compliance with AMLC Regulatory Issuance (ARI) A, B, and C No. 2, Series of 2018, otherwise known as the Guidelines on Digitization of Customer Records (DIGICUR).

The Sales and Marketing personnel uploaded the KYC documents and other related requirements in the database. The personnel in Loan Documentations Department and Credit Reviewer shall check the completeness of the documents being uploaded which include:

1. Signed Loan Application Form
2. Copy of valid IDs
3. Proof of Tax Identification
4. Proof of Billing
5. Promissory Note and Disclosure Agreement
6. Chattel Mortgage
7. Data Privacy Consent Form
8. Security Agreement and Collaterals
9. Any documents supporting source of funds (GIS, SEC Registration, Business Permits, etc.)
10. AML Customer Risk Assessment Form
11. Name Screening Documentation (KaiserCheck and Google Search)
12. Credit Approval Memorandum

The AML Compliance Officer and Chief Compliance Officer have direct access on the CRM and can easily retrieved files herewith. They shall submit the customer records extracted from the CRM to the AMLC's File Transfer and Reporting Facility (FTRF), using their respective log-on credentials, or in such other mode as the AMLC may prescribe.

The Company has also set a policy for Security and Integrity of the Database also. Digital copies are uploaded in the CRM and jointly safe kept by the Loans Department.



## **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

### **2. HARD COPIES OF KYC DOCUMENTS**

The Company duly complies with the AMLA's requirement on records retention. All customer identification records shall be maintained and safely stored as long as the account exists. All transaction records shall be maintained and safely stored for five (5) years from the date of transaction. With respect to closed accounts, the records on customer identification, account files and business correspondences shall be preserved and safely stored for at least five (5) years from the date of closure.

Customer records are being maintained by the Sales and Marketing Department. These are being scanned and uploaded to the Customer Relationship Management (CRM) system. Collateral documents are being safekept in the vault by responsible officers. On the other hand, customer records of closed/terminated accounts are being archived in the warehouses in Burgundy and Pasig. In terms of Covered Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs), these are being maintained in One Drive and local disk of the Compliance Department.

The Loans Documentation Manager is the record-keeping officer of the Company.

### **3. CLOSED ACCOUNTS**

With respect to closed accounts, the records on customer identification, account files and business correspondences shall be preserved and safely stored for at least five (5) years from the date of closure.

### **4. RETENTION OF RECORDS**

Digitize all customer records in accordance with the timelines set in Section of DIGICUR guidelines, including those pertaining to accounts existing prior to implementation period thereof, but excluding customer records of closed accounts beyond the five (5)-years retention period and until it is confirmed that the case has been finally resolved or terminated by the court.

#### **2. DIGITIZATION AND CENTRALIZATION OF CUSTOMER RECORDS (DIGICUR):**

These guidelines cover safekeeping and retention by the Company of customer identification requirements and transaction records in accordance with the AML/CFT Digitization of Customer Records (DIGICUR) and establishment of a central database located in HO.

The aim is to strengthen the public policy on the confidentiality of financial investigations and prohibition of communications thereon wherein revelation is inimical to public interest. It is the objective of the Company to provide process on swift retrieval of customer records submitted in a manner, quality and period relevant to AMLC investigations and institution of legal action.

To achieve this end, the Company shall maintain a central database of its customers' records in the quality and standard required by regulations (i.e. ARI A, B and C, No. 2 Series of 2018, among others).



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 5. INCLUSION IN DIGICUR AND MANNER OF STORAGE IN CENTRAL DATABASE

The central database shall be the repository of customer records. It shall be maintained by the Information Technology Unit of the Company and the Compliance Officer shall be given access thereto to retrieve documents, papers and effects whenever directed or required to submit by AMLC.

Customer records (collectively referred to as “CDD records” or “CDD documents”) refer to:

- Those obtained by the Company at the onset of a transaction to establish the true and full identity of customers in accordance with the Know-Your-Customer (KYC) / Customer Due Diligence (CDD) policies and procedures, which, includes:
  - Customer information file;
  - Official identification documents;
  - Account files and business correspondence, including the results of any analysis undertaken, to establish the background and purpose of complex, unusually large transactions; and
  - Account transaction histories or statements of accounts, whether in Philippine pesos or other currency;
- Credit investigation reports during pre-credit assessment and evaluation;
- Credit approval memorandum or document of imprimatur in the grant of loan or other credit accommodation; and
- Call report or post-credit expositions;

Customer records shall be scanned and stored in the data server of the Company.

Every document scanned and stored shall be labeled with particularity as to the type or kind of document in relation to the transaction in such forms as may be admissible in court or as may prescribed by the AMLC.

All documents of each customer, whether approved or denied, shall be stored in the central database within a period of five (5) years, unless, a longer period is required by circumstances (i.e. when an account is subject of investigation or litigation, retention period shall remain until such investigation or litigation has been finally resolved or adjudicated).

#### Physical Safekeeping of Records (Hard Copies)

- All customer identification records of the Company shall be maintained and safely stored as long as the account exists and in accordance with the Company’s record retention policies.
- Pursuant to AMLA, records/ documents shall be maintained and safely stored as follows:



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

<b>Records/ Documents</b>	<b>Retention Period</b>
<b>All transaction records</b> - including unusual or suspicious patterns of account activity, whether or not a Suspicious Transaction Report (STR) was filed with AMLC – BSP, SEC and other regulatory agencies	Within 5 years from date of transaction
All <b>customer identification documents</b> specified in this Policies and Guidelines	Within 5 years from date of closing of account
All customer and transactional records subject of <b>litigation (judicial or administrative proceeding)</b>	Within the litigation period until the case is finally resolved or adjudicated

**Maintenance and Custodianship**

**Custodianship.** The Sales / Marketing Unit shall be jointly responsible on the safekeeping of records pertaining to transactions and identity documents of the clients.

The Compliance Officer or authorized alternate shall be responsible on the safekeeping of records of accounts/clients subject of the money laundering investigation and reports.

Records and files shall contain the full and true identity of the borrowers or holders of the accounts involved in the transactions such as:

- identification card;
- photo of individual customer;
- required documents for entities mentioned in this P and G;
- customer information file;
- specimen signature of authorized signatories, and
- all other pertinent identification documents and all factual circumstances and records involved in the transaction

The Company shall undertake necessary adequate security measures to ensure confidentiality of such files.

The Company shall prepare and maintain documentation in accordance with the customer identification requirements on customer accounts, relationships and transactions such that these can be reconstructed to enable AMLC – BSP, SEC and other regulatory agencies and/ or the courts to establish an audit trail for money laundering.

In case a Money Laundering Case has been filed in Court

- The Case File must be retained **beyond the 5-year** retention period and until it is confirmed that the case has been finally resolved or terminated by the court.
- The Compliance Officer or authorized alternate shall advise concerned Sales Unit of the account subject of AMLC investigation.

For monitoring purposes, Sales Unit shall maintain a **confidential listing** of the following:



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- Accounts with Suspicious Transaction Report
- Accounts with money laundering case or under investigation

The list must be kept by the designated Records Custodian in accordance with existing guidelines and shall form part of the documents to be turned over in case of resignation or transfer.

#### **Penalties**

All personnel identified in the implementation of this policy who fails to observe and comply shall be subject to investigation and be meted with an appropriate penalty, the degree of which is relative to the committed acts or omissions detrimental to the Company vis-à-vis the imposable penalty for non-compliance per regulatory issuance.

#### **VIII. RELIANCE ON THIRD PARTIES AND SERVICE PROVIDERS**

The Company does not rely on any third party in conducting Customer Due Diligence. The personnel in Sales and Marketing and Credit are conducting due diligence procedures to the customer before establishing business relationship.

For name and sanction screening, the Company tapped the services of 64ai, Inc. and subscribed to use their Kaiser Check web database starting October 11, 2022.

The Company also acquired the services of the collection agencies/companies to collect from the customers. The Collection Agreement and Contract are being reviewed by the Legal and Compliance Department.

#### **IX. OUTSOURCING OF CONDUCT OF CUSTOMER IDENTIFICATION AND DUE DILIGENCE**

The Company does not outsource its conduct of customer identification and acceptance and performance of due diligence. This is the responsibility of the personnel of Sales and Marketing Group and Credit and Collection Department.

#### **X. CUSTOMER REFUSAL**

The Company shall deny relationship with the Client and immediately close the account of existing Client, in cases where:

- additional information cannot be obtained,
- any information or document provided is false or falsified, or
- the result of validation process is unsatisfactory

The Sales Associates (SA) shall verify the name of the prospective client against the Company's watchlist or other reliable financial institution sources. If the name matched on the watchlist, the SA shall investigate if the person on the watchlist and the client is the same. If the investigation reveals that the client and the person on the list is the same, the SA shall not open the account. The SA shall report the matter to the immediate Executive Officer in charge.

The Sales and Marketing personnel do not transact with the customers who are watchlisted and designated persons.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

Designated Custodians of KYC documents shall file and safekeep all pertinent documents for audit purposes.

### XI. PROHIBITED ACCOUNT

The following are the prohibited accounts of the Company:

- 1) Anonymous accounts;
- 2) Accounts under fictitious names/alias;
- 3) Numbered checking accounts
- 4) Other similar accounts

### XII. TARGETED FINANCIAL SANCTIONS (TFS) AND TFS TO PROLIFERATION FINANCING (PF)

The Company adheres to the 2021 Sanction Guidelines issued by the AMLC for Targeted Financial Sanctions (TFS) Related to Terrorism, Terrorism Financing and Proliferation Financing.

The Company will both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities including:

- (a) Any person or entity designated as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations Security Council Resolution or by another jurisdiction or supra-national jurisdiction;
- (b) Any person, organization, association, or group of persons designated under paragraph 3, Section 25 of the Anti-Terrorism Act of 2020 (ATA); and,
- (c) Any person or entity designated under UNSC Resolutions Nos. 1718 (2006) and 2231 (2015).

Financial sanctions are restrictions put in place by the United Nations and its Security Council, a supranational jurisdiction (e.g. European Union), another jurisdiction or by the Philippine government to achieve a specific foreign policy or national security objective

#### **Types of financial sanctions**

Financial sanctions come in many forms as they are developed in response to a given situation. The Terrorism Financing Prevention and Suppression Act (TF law) provides two (2) types of sanctions:

1.) **Targeted asset freezes:** these apply to named individuals, entities and bodies, restricting access to funds and economic resources. Someone subject to an asset freeze will be listed on the Consolidated List, designated or proscribed and posted under the AMLC or Anti-Terrorism Council (ATC) websites.

2.) **Prohibition against Dealing :** prohibits any person from (a) dealing, directly or indirectly, in any way and by any means, with any property or funds that he knows or has reasonable ground to believe is owned or controlled by a designated person, organization, association or group of persons, including funds derived or generated from property or funds owned or controlled, directly or indirectly, by a designated person, organization, association or group of persons; or



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

(b) makes available any property or funds, or financial services or other related services to a designated person, organization, association or group of persons.

**Filing a Return to the AMLC**

The Company will file a return:

- a. When there is a target match, i.e., the subject person or entity fully matches the description in the Consolidated List, list of designation or proscription, covered persons shall file a detailed electronic return within 24 hours from effecting the freeze.
- b. In cases where there is merely a potential target match, covered persons shall file a detailed electronic return within 24 hours from receipt of the AMLC's confirmation.
- c. For cases where the AMLC directs the freeze of the funds and other assets of a person or entity who, although not specifically included in the Consolidated List, was nevertheless found to be acting for and in behalf of or under the direction of those designated under the Consolidated List, list of designation or proscription, covered persons shall file the detailed electronic return within 24 hours upon discovery.

**XIII. COOPERATION WITH THE ANTI-MONEY LAUNDERING COUNCIL**

**1. AMLC DOCUMENTARY REQUIREMENTS FOR COVERED TRANSACTIONS (CT) AND SUSPICIOUS TRANSACTIONS (ST)**

The covered and suspicious transaction reports submitted to the AMLC shall become the basis for the Council to require customer's documentation, covered by a letter being received by mail. The Compliance Office/Department takes charge of requiring the documents (must be stamped with certified true copy and signature over printed name of Branch Head/Manager) from the branch where the account is maintained. The Compliance Department will then assure the personal delivery of the letter with the required documentation within the deadline set by the AMLC

**2. HANDLING OF FREEZE ORDER FROM AMLC**

A freeze order to an account/related account received by the Bank from AMLC or Court of Appeals must be immediately relayed to Legal Department for verification with the assistance of the Chief Compliance Officer.

Upon instruction from Legal Department, the concerned account/related account will be put on hold.

The Legal Department and Chief Compliance Officer will coordinate to the concerned personnel (e.g. branches, business units) and will ask to immediately notify the account holder on the details of the freeze order by phone or send letter of notification via registered mail.

Within 24 hours upon receipt of the freeze order, the Legal Department shall deliver to the concerned Court of Appeals and AMLC, a written return on the freeze order specifying all the pertinent and relevant information which shall include the following:

- The account numbers of the related accounts



### Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- The name(s) of the account holder(s)
- Outstanding balance(s) of related accounts(s) at the time they were frozen
- All relevant information as to the nature of the account(s) subject of the freeze order
- The date and time when the hold-out took effect

Possible related accounts will also be identified by responsible branch personnel/BU Heads concerned. Branch/BU involved shall coordinate with each other particularly when investigating, identifying and freezing related accounts maintained in different branches/BU and under different names. These accounts shall be reported to Compliance Department AML Section and evaluated by the AML Committee for disposition.

Related accounts pertain to accounts, funds and sources which originated from and/or are materially inked to the monetary instrument/s or properties under the name(s)/subject of the Freeze Order.

**Materially linked accounts** include but are not limited to the following (under Rule 3.e.3.a. of RIRR of R.A. 9160, as amended by R.A. 9194 and R.A. 10167):

- All accounts or monetary instruments belonging to the same person whose accounts, monetary instruments or properties are the subject of the Freeze Order;
- 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, whether such accounts are held, owned or controlled singly or jointly with another person;
- All accounts or monetary instruments the funds of which are transferred to the accounts, monetary instruments or properties subject of the Freeze Order without any legal or trade obligation, purpose or economic justification;
- All “In Trust For” (ITF) accounts where the person whose accounts, monetary instruments or properties are the subject of the Freeze Order is either the trustee or the trustor; and
- All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments or properties are the subject of Freeze Order.

### 3. FREEZING MECHANISM

The **period** of the freeze order is dependent on the circumstances of the case, but shall **not exceed 6 months**.

If **no case filed** against the owner of the asset frozen within the period determined by the court, the freeze order shall be **deemed ipso facto lifted**.

### 4. PROHIBITION AGAINST DISCRIMINATION

The **AMLA shall not be construed or implemented** in a manner that will **discriminate** against certain customer types, such as politically-exposed persons, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the **only basis to deny** these persons **access to the services** provided by the covered persons. Whenever a bank, or quasi-bank, financial institutions or whenever any person or entity commits said discriminatory act, the person or persons responsible for such violation shall be subject to sanctions as me be deemed appropriate by their respective regulators.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### 5. FORFEITURE OF EQUAL VALUE

The forfeiture shall include those other monetary instrument or property having an equivalent value to that of the monetary instrument or property found to be related in any way to an unlawful activity or a money laundering offense, when with due diligence, the former:

- cannot be located;
- has been substantially altered, destroyed, diminished in value or otherwise rendered worthless by any act or omission;
- has been concealed, removed, converted, or otherwise transferred;
- located outside the Philippines or has been placed or brought outside the jurisdiction of the court; or
- has been commingled with other monetary instrument or property belonging to either the offender himself or a third person or entity, thereby rendering the same difficult to identify or be segregated for purposes of forfeiture.

### 6. SHARING OF CUSTOMER INFORMATION AMONG EMPLOYEES

The Company allows the sharing of information among its branches and offices located nationwide only when conducting Customer Due Diligence provided the needed information shall be requested by the designated Compliance Office.

### 7. PENALTIES FOR VIOLATION OF THE ML/PF/TF SUPPRESSION ACT

Failure to adhere to this Manual may subject the Company's employees to disciplinary action up to the extent of termination of employment while the contracts or business relationships with accredited third party service providers may be suspended and if necessary, termination of the contract subject to prescribed notification requirements. Penalties for money laundering, terrorist financing and proliferation 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 ₱3,000,000 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, LDB risk losing their charters and/or licenses, and employees risk being subjected to AML criminal investigation.

- For knowingly transacting or attempting to transact any monetary instrument or property which represents, involves or relates to the proceeds of any unlawful activity (The money launderer himself)

Penalty      7 to 14 years imprisonment and a fine of not less than P 3 Million but not more than twice the value of the monetary instrument or the property.

- For knowingly performing or failing to perform an act in relation to any monetary instrument or property involving the proceeds of any unlawful activity as a result of which he facilitated the offense of money laundering (The person who assists the money launderer).

Penalty      4 to 7 years imprisonment and a fine of not less than ₱1.5 Million but not more than ₱3



Million

## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### ➤ Participation in the commission of ML

Penalty Imprisonment ranging from *four (4) to seven (7) years* and a fine corresponding to *not more than 200% of the value of the monetary instrument or property laundered* shall be imposed upon the covered person, its directors, officers or personnel who *knowingly participated* in the commission of the crime of money laundering.

### ➤ For knowingly failing to disclose and file with the AMLC any monetary instrument or property required to be disclosed and filed

Penalty 6months to 4 years imprisonment or a fine of not less than ₱100,000.00 but not more than ₱500,000.00 or both.

### ➤ Other Offenses under R.A. 9160, as amended

- **For failure to keep records** – Failure to maintain and safely store all records of transactions by any responsible official or employee of a covered institution, including closed accounts, for five (5) years from the date of the transaction/closure of the account.

Penalty 6months to 1 year imprisonment or a fine of not less than ₱100,000.00 but not more than-P 500,000.00, or both.

- **For malicious reporting** - Any person who reports or files completely unwarranted or false information relative to money laundering transaction against any person shall be held criminally liable.

Penalty 6 months to 4 years imprisonment and a fine of not less than ₱100,000.00 but not more than ₱500,000.00.

### ➤ **For breach of confidentiality** - When reporting covered or suspicious transactions to the AMLC, covered institutions and their officers and employees are prohibited from communicating directly or indirectly, in any manner or by any means, to any person or entity, the media the fact that a covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto. Neither may such reporting be published or aired in any manner or form by the mass media, electronic mail or other similar devices. In case of violation thereof, the concerned officer and employee of the covered institution and media (the responsible reporter, writer, president, publisher, manager, and editor-in-chief) shall be held criminally liable.

Penalty 3 to 8 years imprisonment and a fine of not less than ₱500,000.00 but not more than ₱1.0 Million

## 8. RULES OF PROCEDURES IN ADMINISTRATIVE CASES (RPAC)

Effective 26 July 2019, the Anti-Money Laundering Council (AMLC) has issued the Rules of Procedure in Administrative Cases under Republic Act No. 9160 or the Anti-Money Laundering Act of 2001, as Amended, and its Implementing Rules and Regulations, and Guidelines and Other Issuances of the Anti-Money Laundering Council and the Imposition of Administrative Sanctions (RPAC). The adoption of the RPAC supersedes the Rules on Imposition of Administrative Sanctions (RIAS). Salient features are as follow:



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

- **Application:** The RPAC is intended to apply to administrative cases for non-compliance with, or violations of the AMLA, as amended, and its implementing rules and regulations, and guidelines and issuances of the AMLC.
- **Coverage of administrative cases:** The RPAC covers not only administrative cases against covered persons, but also those against its individual officers, directors, and employees of the Bank.
- **Lower monetary sanctions:** Monetary sanctions under the RPAC are based on the covered person's asset size, and gravity of the violation/non-compliance, based on a graduated scale of the proportion or amount involved. For light violations of compliance with transaction reporting requirements, the minimum penalty that may be assessed is Php1,500.00 for non-compliance with covered transaction reporting requirements for the Bank with small asset sizes, on a per account basis.
- **Enumeration of covered persons:** Unlike the RIAS, the RPAC identifies the type of covered person subject of administrative cases.

### 9. SAFE HARBOR PROVISIONS

When reporting covered or suspicious transactions to the AMLC, covered institutions and their officers and employees shall not be deemed to have violated Republic Act No. 1405, as amended, Republic Act No. 6426, as amended, Republic Act no. 8791 and other similar laws

No administrative, criminal or civil proceedings shall lie against any person for having made a covered or suspicious transaction report in the regular performance of his duties in good faith, whether or not such reporting results in any criminal prosecution under this Act or any other law.

When reporting CT or ST to the AMLC, the Company and its officers and employees are not deemed to have violated:

- R.A. No. 1405, as amended,
- R.A. No. 6426, as amended,
- R.A. No. 8791 and
- other similar laws.

### KNOW-YOUR CUSTOMER RULE (KYC) AND CUSTOMER DUE DILIGENCE REQUIREMENTS FOR PURCHASERS OF THE BANK'S ACQUIRED PROPERTIES AND ASSETS AND LOAN BORROWERS

KYC/Customer Due Diligence as required by AMLA should be satisfactorily performed on Real and Other Properties Acquired (ROPA) disposals, with the following requirements:

- 1) Signed Bid Form and Customer Information Sheet of ROPA buyers, which shall be properly encoded in the company's database and shall be properly filled-up with minimum information such as Name, Present Address, Permanent Address, Date and Place of Birth, Nature of Work/Business, Contact Numbers TIN, SSS No. GSIS No. Specimen Signature, Source(s) of Funds, and Name of Beneficiaries in case of insurance contracts and whenever applicable.



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- 2) Check and verify the name of the buyer against the Watch list (OFAC List, List of Associated Persons in Taliban and Al Qaida, Her Majesty list and Internal Watchlist) via KaiserCheck and search via Google Search for enhance due diligence if the applicant has derogatory records and adverse information. Certification of name search shall be uploaded to the system as part of the KYC documentation as well the screenshot made via Google Search.
- 3) Accomplished AML Customer Risk Assessment Form (CRAF) for the assessment of the risk profile of the client with the corresponding due diligence performed.
- 4) Document the source of funds
- 5) Documentation of Sale (Deed of Sale)





Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

1.2 South Asialink Finance Corporation LOAN APPLICATION FORM Back Page

PRIVACY NOTICE AND CONSENT FORM

Here at **SOUTH ASIALINK FINANCE CORPORATION**, we take your privacy seriously.

The privacy and security of your personal data (the "Personal Information") which we collect from you is important to us. It is equally important that you understand how we handle this data.

In the course of conducting our business, we must collect "Personal Information" from you. The nature of the information that we collect will be strictly used to administer your account and to provide the products and services you have requested from us and to further meet your needs and the standard procedures of our business.

We will treat your "Personal Information" confidential. It will only be disclosed for the purpose of handling your account efficiently, effectively and to further assist you in your financial needs, to our affiliates such as credit bureaus, collection companies and other financial institutions. We have trusted relationships, with carefully selected third parties who perform services on our behalf. All service providers are bound by the contract to maintain the security of your personal information and to use it only as permitted by us. We guarantee that your personal information will be strictly kept in private.

Likewise, in order to attain your goals and financial goals, we might need to collect and gather information in relation to your loan application. In this regard, this will also serve as your consent in giving **SOUTH ASIALINK FINANCE CORPORATION**, ("SAFC" for brevity) the right to collect and gather information from any bank institutions, your employer, supplier, agencies, from your declared character references in the application form. You are also allowing **SAFC** to collect personal and sensitive information from your relatives up to 3rd consanguinity and vice versa, that we are allowed to disclose any personal information to the above-mentioned people and institutions in any case we cannot contact you to discuss your loan and your existing obligation, if any. You are also allowing **SAFC** to collect information from any institutions that you are connected with or related to in order to properly assess your loan application. Furthermore, you are allowing any of these above mentioned institutions and persons to disclose any information about you that will help us in ascertaining your loan application.

Furthermore, in any case of restructuring your loan obligation, you are giving consent and allowing **SAFC** to disclose and collect information from the above-mentioned institutions and people.

Here at **SOUTH ASIALINK FINANCE CORPORATION** we make sure that you are protected.

For further information regarding the privacy policy, you may visit our website at [www.southasialink.com.ph](http://www.southasialink.com.ph)

I hereby acknowledge that I have read, understand and agree to the terms of this document:

\_\_\_\_\_  
Borrower's signature over printed name

\_\_\_\_\_  
Co-Borrower's signature over printed name

\_\_\_\_\_  
Date



Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

2. South Asialink Finance Corporation CUSTOMER RISK ASSESSMENT FORM Front Page

**AML CUSTOMER RISK ASSESSMENT FORM**

CUSTOMER INFORMATION			
CUSTOMER'S NAME		<i>Last Name</i>	<i>First Name</i>
		<i>Suffix (if any)</i>	<i>Middle Name</i>
SOURCE OF FUND		NATURE OF WORK	
CUSTOMER TYPE <input type="radio"/> INDIVIDUAL <input type="radio"/> CORPORATION Beneficial Owner/s: (if any) _____ <input type="radio"/> OTHERS (Please Specify) _____			
BACKGROUND INFORMATION			
<b>NEGATIVE WATCHLIST FILE CHECK RESULT</b> from the OFAC and UN Sanctions Lists, Negative News and Advisories and other Derogatory Records		<input type="checkbox"/> Without Adverse Information <input type="checkbox"/> With Adverse Information Please Specify: _____	
<b>POLITICALLY EXPOSED PERSON (PEP)</b> (IF YES, DO NOT PROCEED TO RAF) including Family Members up to 2 <sup>nd</sup> Degree (Affinity/Consanguinity) and publicly known close associate of PEP		<input type="checkbox"/> NO <input type="checkbox"/> YES Please Specify: _____	
<b>LINKED TO HIGH RISK ACCOUNT</b> Persons connected or related to customers with High Risk Profile		<input type="checkbox"/> NO <input type="checkbox"/> YES Please Specify: _____	
RISK ASSESSMENT PROFILE (RAF)			
<input type="checkbox"/> <b>NORMAL RISK</b> *Indicate some details/specifications of the chosen item in the space provided.			
<b>INDIVIDUAL EARNINGS</b> <input type="radio"/> Salaried Employee <input type="radio"/> Pensioner/Retiree <input type="radio"/> OFW/Allottee <input type="radio"/> Foreign Individual	<b>SELF-EMPLOYED</b> <input type="radio"/> Store <input type="radio"/> Leasing Space <input type="radio"/> Trucking Business <input type="radio"/> PUV Operator	<b>PRIVATE PRACTITIONER</b> <input type="radio"/> Doctor <input type="radio"/> Lawyer <input type="radio"/> Accountant <input type="radio"/> Others _____	<b>AGRICULTURAL INDUSTRY</b> <input type="radio"/> Farmer/Fisher <input type="radio"/> Rice Dealer <input type="radio"/> LiveStock Dealer <input type="radio"/> Others _____
		<b>BUSINESS</b> <input type="radio"/> Wholesaler <input type="radio"/> Distributor <input type="radio"/> Manufacturing <input type="radio"/> Others _____	<b>OTHER SERVICES</b> <input type="radio"/> Construction <input type="radio"/> Food/Hospitality <input type="radio"/> Healthcare <input type="radio"/> Others _____
Please specify: _____			
<input type="checkbox"/> <b>HIGH RISK</b> *Indicate some details/specifications of the chosen item in the space provided.			
<b>HIGH VALUE GOODS</b> <input type="radio"/> Pawnshops <input type="radio"/> Jewelry Shop <input type="radio"/> Car Dealer <input type="radio"/> High Value Items <input type="radio"/> Vehicle Buy & Sell	<b>MONEY TRADINGS</b> <input type="radio"/> Foreign Exchange <input type="radio"/> Money Changers <input type="radio"/> Remittance Agent/Center <input type="radio"/> Lending Business <input type="radio"/> Money Transfers/Service <input type="radio"/> Private Banking	<b>NON-PROFIT ORGANIZATION</b> <input type="radio"/> Charities <input type="radio"/> Foundations <input type="radio"/> Religious Sect <input type="radio"/> Civic Organization <input type="radio"/> Cultural Associations <input type="radio"/> Cooperatives	<b>GAMBLING BUSINESS</b> <input type="radio"/> Casino Agent <input type="radio"/> Lotto Outlet <input type="radio"/> Online Gambling Franchise <input type="radio"/> Cock Fighting & Horse Race <input type="radio"/> Off-Shore Gaming <input type="radio"/> Other Gaming Services
		<b>SERVICE PROVIDERS</b> <input type="radio"/> Business trading via Internet <input type="radio"/> Virtual/Electronic Currencies <input type="radio"/> Private Armed Service Providers <input type="radio"/> Arms and Ammunition Dealers <input type="radio"/> Networking/Commission Based <input type="radio"/> Other Cash Incentive Activities	
Please specify: _____			
<input type="checkbox"/> OTHERS			
APPROVAL			
Assessed by:		Attested by:	
_____		_____	
Signature over printed name		Signature over printed name	
_____		_____	
Date		Date	
APPROVED BY:			
_____		_____	
Printed Name and Signature		Date	



Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

2.2 South Asialink Finance Corporation CUSTOMER RISK ASSESSMENT FORM Back Page

APPLICATION OF DUE DILIGENCE																																		
<input type="checkbox"/> INDIVIDUAL CUSTOMER <input type="checkbox"/> AUTHORIZED SIGNATORY																																		
<b>1. CUSTOMER INFORMATION SHEET (WITH COMPLETE ELEVEN MINIMUM INFORMATION)</b>																																		
<input type="checkbox"/> Name of Customer <input type="checkbox"/> Date and place of birth <input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner if applicable <input type="checkbox"/> Present address; <input type="checkbox"/> Permanent address; <input type="checkbox"/> Contact number or information; <input type="checkbox"/> Nationality; <input type="checkbox"/> Specimen signature or biometrics of the customer; <input type="checkbox"/> Nature of work, name of employer or nature of self-employment/business; <input type="checkbox"/> Source/s of funds; and <input type="checkbox"/> Tax Identification number (TIN) <input type="checkbox"/> Social Security System (SSS) number or Government Service Insurance System (GSIS) number as may be applicable																																		
<b>2. Presentation of Valid Identification Documents (IDs)</b>																																		
<b>3. Verify information provided in no. 1 based on official documents or other reliable, independent source documents.</b> Please specify: _____																																		
<input type="checkbox"/> CORPORATION AND JURIDICAL ENTITIES, PARTNERSHIP AND SOLE PROPRIETORSHIP																																		
<b>1. CUSTOMER INFORMATION SHEET WITH COMPLETE MINIMUM INFORMATION</b>																																		
<input type="checkbox"/> Name of Entity <input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner or beneficiary, if applicable, and authorized signatories <input type="checkbox"/> Official address; <input type="checkbox"/> Contact number or information; <input type="checkbox"/> Nature of business; <input type="checkbox"/> Specimen signature or biometrics of the customer;																																		
<b>2. IDENTIFICATION DOCUMENTS</b>																																		
<input type="checkbox"/> Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance and transfer companies; <input type="checkbox"/> Secondary license or certificate of authority issued by the supervising authority or other government agency <input type="checkbox"/> Articles of Incorporation/Partnership; <input type="checkbox"/> Latest General Information Sheet which list the names of directors/trustees/partners, principal stockholders owning at least twenty percent (20%) of the outstanding capital stock and primary officers such as the President and Treasurer; <input type="checkbox"/> Board or Partner's resolution duly certified by the Corporate/Partner's Secretary, or other equivalent document, authorizing the Signatory to sign on behalf of the entity; and <input type="checkbox"/> For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.																																		
Please provide list of banks where the client has maintained or maintaining an account/s																																		
1.	2.	3.	4.	5.																														
Please provide list of companies where the client is an officer, director or stockholder																																		
1.	2.	3.	4.	5.																														
For entities, shell companies etc. please provide each primary officers (President, Treasurer and authorized signatory/ies) name, present address, date and place of birth, nature of work, nationality and source of funds, stockholders owning at least 20% of the voting stock, and Directors/ Partners/ Trustees as well as their respective identification documents (Please provide additional sheet, if necessary)																																		
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Name of Primary Officers</th> <th style="width: 20%;">Position</th> <th style="width: 30%;">Present Address</th> <th style="width: 10%;">Nationality</th> <th style="width: 10%;">Ownership</th> </tr> </thead> <tbody> <tr><td>1.</td><td></td><td></td><td></td><td></td></tr> <tr><td>2.</td><td></td><td></td><td></td><td></td></tr> <tr><td>3.</td><td></td><td></td><td></td><td></td></tr> <tr><td>4.</td><td></td><td></td><td></td><td></td></tr> <tr><td>5.</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>					Name of Primary Officers	Position	Present Address	Nationality	Ownership	1.					2.					3.					4.					5.				
Name of Primary Officers	Position	Present Address	Nationality	Ownership																														
1.																																		
2.																																		
3.																																		
4.																																		
5.																																		
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Name of Directors/Partners/Trustees</th> <th style="width: 20%;">Position</th> <th style="width: 30%;">Present Address</th> <th style="width: 10%;">Nationality</th> <th style="width: 10%;">Ownership</th> </tr> </thead> <tbody> <tr><td>1.</td><td></td><td></td><td></td><td></td></tr> <tr><td>2.</td><td></td><td></td><td></td><td></td></tr> <tr><td>3.</td><td></td><td></td><td></td><td></td></tr> <tr><td>4.</td><td></td><td></td><td></td><td></td></tr> <tr><td>5.</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>					Name of Directors/Partners/Trustees	Position	Present Address	Nationality	Ownership	1.					2.					3.					4.					5.				
Name of Directors/Partners/Trustees	Position	Present Address	Nationality	Ownership																														
1.																																		
2.																																		
3.																																		
4.																																		
5.																																		
<b>For Individual Customers, Please state the validation procedures performed and secure/attached documentary proof. Please provide at least three (3)</b>																																		
<input type="checkbox"/> Presentation of Valid Identification Documents <input type="checkbox"/> Confirming the date and place of birth from a duly authenticated official document <input type="checkbox"/> Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters, Barangay Certifications or other documents showing address or through or other documents showing address or through on-site visitation <input type="checkbox"/> Contacting the customers by phone, email <input type="checkbox"/> Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by other means <input type="checkbox"/> Determining the veracity of the declared source of funds thru submission of Certificate of Employment (COE), Income Tax Return (ITR), Financial Statements or Statement of Assets, Liabilities and Networth (SALN), or Proof of Remittances																																		
<b>For corporate or juridical entities, Did you perform any of the following? If yes, please provide validation performed and secure/attached documentary proof. (Please provide at least three (3))</b>																																		
<input type="checkbox"/> Certificate of Registration (SEC/ DTI/ BSP/ IC) <input type="checkbox"/> Articles of Incorporation/ Partnership <input type="checkbox"/> Latest General Information Sheet (GIS) – Year _____ <input type="checkbox"/> Secretary's Certificate authorizing signatory/ies <input type="checkbox"/> Inquiring from the supervising authority the status of the entity <input type="checkbox"/> Contacting the entity by phone or email <input type="checkbox"/> Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address <input type="checkbox"/> Validating source of funds or source of wealth from reliable documents such as audited financial statements, bank references etc.																																		
<b>Assessed by:</b> _____			<b>Attested by:</b> _____																															



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

APPLICATION OF DUE DILIGENCE				
<input type="checkbox"/> INDIVIDUAL CUSTOMER	<input type="checkbox"/> AUTHORIZED SIGNATORY			
<b>1. CUSTOMER INFORMATION SHEET (WITH COMPLETE ELEVEN MINIMUM INFORMATION)</b>				
<ul style="list-style-type: none"> <li><input type="checkbox"/> Name of Customer</li> <li><input type="checkbox"/> Date and place of birth</li> <li><input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner if applicable</li> <li><input type="checkbox"/> Present address;</li> <li><input type="checkbox"/> Permanent address;</li> <li><input type="checkbox"/> Contact number or information;</li> <li><input type="checkbox"/> Nationality;</li> <li><input type="checkbox"/> Specimen signature or biometrics of the customer;</li> <li><input type="checkbox"/> Nature of work, name of employer or nature of self-employment/business;</li> <li><input type="checkbox"/> Source/s of funds; and</li> <li><input type="checkbox"/> Tax identification number (TIN)</li> <li><input type="checkbox"/> Social Security System (SSS) number or Government Service Insurance System (GSIS) number as may be applicable</li> </ul>				
<b>2. Presentation of Valid Identification Documents (IDs)</b>				
<b>3. Verify information provided in no. 1 based on official documents or other reliable, independent source documents.</b> Please specify: _____				
<input type="checkbox"/> CORPORATION AND JURIDICAL ENTITIES, PARTNERSHIP AND SOLE PROPRIETORSHIP				
<b>1. CUSTOMER INFORMATION SHEET WITH COMPLETE MINIMUM INFORMATION</b>				
<ul style="list-style-type: none"> <li><input type="checkbox"/> Name of Entity</li> <li><input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner or beneficiary, if applicable, and authorized signatories</li> <li><input type="checkbox"/> Official address;</li> <li><input type="checkbox"/> Contact number or information;</li> <li><input type="checkbox"/> Nature of business;</li> <li><input type="checkbox"/> Specimen signature or biometrics of the customer;</li> </ul>				
<b>2. IDENTIFICATION DOCUMENTS</b>				
<ul style="list-style-type: none"> <li><input type="checkbox"/> Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance and transfer companies;</li> <li><input type="checkbox"/> Secondary license or certificate of authority issued by the supervising authority or other government agency</li> <li><input type="checkbox"/> Articles of Incorporation/Partnership;</li> <li><input type="checkbox"/> Latest General Information Sheet which list the names of directors/trustees/partners, principal stockholders owning at least twenty percent (20%) of the outstanding capital stock and primary officers such as the President and Treasurer;</li> <li><input type="checkbox"/> Board or Partner's resolution duly certified by the Corporate/Partner's Secretary, or other equivalent document, authorizing the Signatory to sign on behalf of the entity; and</li> <li><input type="checkbox"/> For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.</li> </ul>				
Please provide list of banks where the client has maintained or maintaining an account/s				
1.	2.	3.	4.	5.
Please provide list of companies where the client is an officer, director or stockholder				
1.	2.	3.	4.	5.
For entities, shell companies etc. please provide each primary officers (President, Treasurer and authorized signatory/es) name, present address, date and place of birth, nature of work, nationality and source of funds, stockholders owning at least 20% of the voting stock, and Directors/ Partners/ Trustees as well as their respective identification documents (Please provide additional sheet, if necessary)				
Name of Primary Officers	Position	Present Address	Nationality	Ownership
1.				
2.				
3.				
4.				
5.				
Name of Directors/Partners/Trustees	Position	Present Address	Nationality	Ownership
1.				
2.				
3.				
4.				
5.				
For Individual Customers, Please state the validation procedures performed and secure/attached documentary proof. Please provide at least three (3)				
<ul style="list-style-type: none"> <li><input type="checkbox"/> Presentation of Valid Identification Documents</li> <li><input type="checkbox"/> Confirming the date and place of birth from a duly authenticated official document</li> <li><input type="checkbox"/> Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters, Barangay Certifications or other documents showing address or through other documents showing address or through on-site visitation</li> <li><input type="checkbox"/> Contacting the customers by phone, email</li> <li><input type="checkbox"/> Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by other means</li> <li><input type="checkbox"/> Determining the veracity of the declared source of funds thru submission of Certificate of Employment (COE), Income Tax Return (ITR), Financial Statements or Statement of Assets, Liabilities and Networth (SALN), or Proof of Remittances</li> </ul>				
For corporate or juridical entities, Did you perform any of the following? If yes, please provide validation performed and secure/attached documentary proof. (Please provide at least three (3))				
<ul style="list-style-type: none"> <li><input type="checkbox"/> Certificate of Registration (SEC/ DTI/ BSP/ IC)</li> <li><input type="checkbox"/> Articles of Incorporation/ Partnership</li> <li><input type="checkbox"/> Latest General Information Sheet (GIS) – Year _____</li> <li><input type="checkbox"/> Secretary's Certificate authorizing signatory/es</li> <li><input type="checkbox"/> Inquiring from the supervising authority the status of the entity</li> <li><input type="checkbox"/> Contacting the entity by phone or email</li> <li><input type="checkbox"/> Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address</li> <li><input type="checkbox"/> Validating source of funds or source of wealth from reliable documents such as audited financial statements, bank references etc.</li> </ul>				
Assessed by: _____			Attested by: _____	



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

APPLICATION OF DUE DILIGENCE																																		
<input type="checkbox"/> INDIVIDUAL CUSTOMER <input type="checkbox"/> AUTHORIZED SIGNATORY																																		
<b>1. CUSTOMER INFORMATION SHEET (WITH COMPLETE ELEVEN MINIMUM INFORMATION)</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Name of Customer</li> <li><input type="checkbox"/> Date and place of birth</li> <li><input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner if applicable</li> <li><input type="checkbox"/> Present address;</li> <li><input type="checkbox"/> Permanent address;</li> <li><input type="checkbox"/> Contact number or information;</li> <li><input type="checkbox"/> Nationality;</li> <li><input type="checkbox"/> Specimen signature or biometrics of the customer;</li> <li><input type="checkbox"/> Nature of work, name of employer or nature of self-employment/business;</li> <li><input type="checkbox"/> Source/s of funds; and</li> <li><input type="checkbox"/> Tax identification number (TIN)</li> <li><input type="checkbox"/> Social Security System (SSS) number or Government Service Insurance System (GSIS) number as may be applicable</li> </ul>																																		
<b>2. Presentation of Valid Identification Documents (IDs)</b>																																		
<b>3. Verify information provided in no. 1 based on official documents or other reliable, independent source documents.</b> Please specify: _____																																		
<input type="checkbox"/> CORPORATION AND JURIDICAL ENTITIES, PARTNERSHIP AND SOLE PROPRIETORSHIP																																		
<b>1. CUSTOMER INFORMATION SHEET WITH COMPLETE MINIMUM INFORMATION</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Name of Entity</li> <li><input type="checkbox"/> Name, present address, date and place of birth, nationality, nature of work and source of funds of beneficial owner or beneficiary, if applicable, and authorized signatories</li> <li><input type="checkbox"/> Official address;</li> <li><input type="checkbox"/> Contact number or information;</li> <li><input type="checkbox"/> Nature of business;</li> <li><input type="checkbox"/> Specimen signature or biometrics of the customer;</li> </ul>																																		
<b>2. IDENTIFICATION DOCUMENTS</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance and transfer companies;</li> <li><input type="checkbox"/> Secondary license or certificate of authority issued by the supervising authority or other government agency</li> <li><input type="checkbox"/> Articles of Incorporation/Partnership;</li> <li><input type="checkbox"/> Latest General Information Sheet which list the names of directors/trustees/partners, principal stockholders owning atleast twenty percent (20%) of the outstanding capital stock and primary officers such as the President and Treasurer;</li> <li><input type="checkbox"/> Board or Partner's resolution duly certified by the Corporate/Partner's Secretary, or other equivalent document, authorizing the Signatory to sign on behalf of the entity; and</li> <li><input type="checkbox"/> For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.</li> </ul>																																		
Please provide list of banks where the client has maintained or maintaining an account/s																																		
1.	2.	3.	4.	5.																														
Please provide list of companies where the client is an officer, director or stockholder																																		
1.	2.	3.	4.	5.																														
For entities, shell companies etc. please provide each primary officers (President, Treasurer and authorized signatory/ies) name, present address, date and place of birth, nature of work, nationality and source of funds, stockholders owning at least 20% of the voting stock, and Directors/ Partners/ Trustees as well as their respective identification documents. (Please provide additional sheet, if necessary)																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Name of Primary Officers</th> <th style="width: 15%;">Position</th> <th style="width: 30%;">Present Address</th> <th style="width: 10%;">Nationality</th> <th style="width: 15%;">Ownership</th> </tr> </thead> <tbody> <tr><td>1.</td><td></td><td></td><td></td><td></td></tr> <tr><td>2.</td><td></td><td></td><td></td><td></td></tr> <tr><td>3.</td><td></td><td></td><td></td><td></td></tr> <tr><td>4.</td><td></td><td></td><td></td><td></td></tr> <tr><td>5.</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>					Name of Primary Officers	Position	Present Address	Nationality	Ownership	1.					2.					3.					4.					5.				
Name of Primary Officers	Position	Present Address	Nationality	Ownership																														
1.																																		
2.																																		
3.																																		
4.																																		
5.																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Name of Directors/Partners/Trustees</th> <th style="width: 15%;">Position</th> <th style="width: 30%;">Present Address</th> <th style="width: 10%;">Nationality</th> <th style="width: 15%;">Ownership</th> </tr> </thead> <tbody> <tr><td>1.</td><td></td><td></td><td></td><td></td></tr> <tr><td>2.</td><td></td><td></td><td></td><td></td></tr> <tr><td>3.</td><td></td><td></td><td></td><td></td></tr> <tr><td>4.</td><td></td><td></td><td></td><td></td></tr> <tr><td>5.</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>					Name of Directors/Partners/Trustees	Position	Present Address	Nationality	Ownership	1.					2.					3.					4.					5.				
Name of Directors/Partners/Trustees	Position	Present Address	Nationality	Ownership																														
1.																																		
2.																																		
3.																																		
4.																																		
5.																																		
<b>For Individual Customers, Please state the validation procedures performed and secure/attached documentary proof. Please provide at least three (3)</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Presentation of Valid Identification Documents</li> <li><input type="checkbox"/> Confirming the date and place of birth from a duly authenticated official document</li> <li><input type="checkbox"/> Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters, Barangay Certifications or other documents showing address or through other documents showing address or through on-site visitation</li> <li><input type="checkbox"/> Contacting the customers by phone, email</li> <li><input type="checkbox"/> Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by other means</li> <li><input type="checkbox"/> Determining the veracity of the declared source of funds thru submission of Certificate of Employment (COE), Income Tax Return (ITR), Financial Statements or Statement of Assets, Liabilities and Networth (SALN), or Proof of Remittances</li> </ul>																																		
<b>For corporate or juridical entities, Did you perform any of the following? If yes, please provide validation performed and secure/attached documentary proof. (Please provide at least three (3))</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Certificate of Registration (SEC/ DTI/ BSP/ IC)</li> <li><input type="checkbox"/> Articles of Incorporation/ Partnership</li> <li><input type="checkbox"/> Latest General Information Sheet (GIS) – Year _____</li> <li><input type="checkbox"/> Secretary's Certificate authorizing signatory/ies</li> <li><input type="checkbox"/> Inquiring from the supervising authority the status of the entity</li> <li><input type="checkbox"/> Contacting the entity by phone or email</li> <li><input type="checkbox"/> Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address</li> <li><input type="checkbox"/> Validating source of funds or source of wealth from reliable documents such as audited financial statements, bank references etc.</li> </ul>																																		
<b>Assessed by:</b> _____			<b>Attested by:</b> _____																															



Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

3. Compliance Testing Template

AML COMPLIANCE TESTING

Branch/Business Unit: \_\_\_\_\_ Date Conducted: \_\_\_\_\_  
 Account Name: \_\_\_\_\_ PN No. \_\_\_\_\_

I. Customer Identification	Remarks
<b>1. Customer Application Form</b>	
a. Name	
b. Present Address	
c. Date and Place of Birth	
d. Nature of work, name of employer or nature of self-employment/business	
e. Contact details	
f. Source of funds	
g. Permanent address	
h. Nationality;	
i. TIN, SSS or GSIS	
j. Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, whenever applicable	
k. Specimen Signature	
l. Valid Identification Card	
<b>2. Risk Assessment Form</b>	
a. Background Information	
b. Risk Profile	
c. Risk Criteria	
d. Others	
<b>3.1 Reduced Due Diligence. Minimum Validation Procedure</b>	
a. Confirm date of birth from a duly authenticated official document	
b. Verify permanent address through evaluation of utility bills, bank or credit card statement or other documents showing permanent address or through on-site visitation	
c. Contacting the customer by phone, email or letter; and	
d. Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any means	
<b>3.2 Enhanced Due Diligence (EDD) for High Risk Customers:</b>	
a. Additional information other than the minimum information	
i. List of Banks where the individual has maintained or is maintaining an account/ List of companies where he is a director, officer or stockholder, banking services to be availed of	
b. Conduct validation procedures on any or all of the information provided	
c. Obtain senior management approval for establishing business relationship	
<b>3.3 Name and Sanctions Screening</b>	
a. United Nations Security Council List (UNSC)	
b. Office of Foreign Assets Control (OFAC)	
c. Kaiser Check Verification	
d. Others	
<b>II. Record Keeping, Retention and Digitization</b>	
a. Active Folder	
b. Digitized	
c. Archived	
d. Disposed	
<b>III. Covered and Suspicious Transactions</b>	
a. Covered Transactions	
b. Suspicious Transactions	
<b>IV. Training Program</b>	
a. AML/TF/FP Orientation	
b. AML Refresher Course	
c. Training on Risk Profiling	







Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

 <b>SOUTH ASIALINK FINANCE CORPORATION</b>	<b>REPORT ON ANTI-MONEY LAUNDERING COMPLIANCE TESTING No 2022-001</b>
---	---

Total Number of KYC Folder Tested	Total Number of Exceptions Found	Percentage	Impact	Likelihood	Rating

**C. Customer Due Diligence (CDD) including Sanctions Screening and Terrorist Financing**

--	--	--	--	--	--

*In conducting Customer Due Diligence, Customer may establish relationship under the true and full name of the account owner/s or customers upon presentation of an acceptable Identification Card and other official document such as proof of billing and proof of income. The branch/unit shall cross-check customer's name as well as the beneficiaries and authorized signatories against the negative watchlists (OFAC, UNSC, and other Local watchlist database).*

Total Number of KYC Folder Tested	Total Number of Exceptions Found	Percentage	Impact	Likelihood	Rating

**II. RECORDS KEEPING, RETENTION REQUIREMENTS & DIGITIZATION**

Account Name	PN No.	Findings/s	Status

*Section 6 of AMLC Regulatory Issuance (ARI) A, B, and C No. 2, Series of 2018, otherwise known as the Guidelines on Digitization of Customer Records (DIGICUR) covered persons as effectively implemented last 2018. All customer records should be fully digitized and uploaded in one (1) centralized database. The covered person shall maintain the records and transactions of the customer five (5) years from the date of transaction and closure of the accounts.*

Total Number of KYC Folder Tested	Total Number of Exceptions Found	Percentage	Impact	Likelihood	Rating

**III. COVERED TRANSACTIONS & SUSPICIOUS TRANSACTION REPORTING**

Account Name	PN No.	Finding/s	Status

*In accordance with Sections 7(1), 7(7), and 9(c) of Republic Act No. 9160, also known as the Anti-Money Laundering Act of 2001, as amended, in relation to Rule 22, Sections 1.1, 4, and 7, of its 2018 Implementing Rules and Regulations (IRR), the Council, in its Resolution No. 142, dated 22 June 2021, approved the adoption of 2021 AMLC Registration and Reporting Guidelines*



Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

<b>SOUTH ASIALINK</b> FINANCE CORPORATION	<b>REPORT ON ANTI-MONEY LAUNDERING COMPLIANCE TESTING No 2022-001</b>
--	---

Total Number of CTR Reported	Total Number of CTR Unreported	Percentage	Impact	Likelihood	Rating
	0/0	0%	-	-	-

**IV. TRAINING PROGRAM**

NAME	Designation	Branch	Status

*Rule 16 Section 4 of the 2021 ARRS requires all employees to attend AML/CFT/PF training.*

Total Number of Personnel	Total Number of Attendees	Percentage	Impact	Likelihood	Rating
-	-	-	-	-	-

*\*\*\*Please see attached list of attendees from Loans Documentation Department*

**Recommendations**

- 1.
- 2.

**Summary**

<p>Discussed with:</p> <p style="text-align: center;"><i>Loans Head</i></p> <p>Noted by:</p> <p style="text-align: center;"><i>Deputy COO- Operations</i></p>	<p>Prepared by:</p> <p style="text-align: center;"><i>Compliance Associate</i></p> <p>Approved by:</p> <p style="text-align: center;"><i>Chief Compliance Officer</i></p>
---	---



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### **PART 5 APPROVING AUTHORITY**

1. Roseshel Barrun      Chief Compliance Officer
2. Joel C. Cruz        President/Chief Operation Officer
3. Corporate Governance Committee
4. Board of Directors



## **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

### **PART 6 UPDATING OF MONEY LAUNDERING TERRORIST FINANCING PREVENTION PROGRAM (MTPP)**

This MTPP shall be reviewed/updated annually by the Compliance Office. The revised manual must incorporate changes in AML policies and procedures, latest trends in money laundering and terrorist financing typologies and latest pertinent SEC and AMLC issuances. Any revision or update in the MTPP shall likewise be reviewed by Corporate Secretary, confirmed by the Board of Directors and signed by any authorize signatory of the Corporation.

Memoranda, Circulars and other documents and updates issued by the Anti-Money Laundering Council, Securities and Exchange Commission and other supervising agencies incorporated with the MTPP and will be disseminated to the Board of Directors, Management and Employees of South Asialink Finance Corporation by means of circular emails, departmental meetings, ongoing trainings conducted by the Compliance Department, and Info-sheets provided by the Human Resource Department through its Intranet website.

Copy of the MTPP is disseminated to all personnel thru their official corporate email. It is also uploaded in the Human Resource Information System (HRIS) of the Company and SAFC Academy. An access shall be given to all personnel of the company.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)  
PART 7  
ANNEXES**

**ANNEX A  
ANTI-MONEY LAUNDERING (AML)  
PROCEDURES AND GUIDELINES ON COMPLIANCE TESTING**

**I. CUSTOMER DUE DILIGENCE**

- Review if the branch has conducted Due Diligence to identify the legal existence of the customer applying with the branch.
- Review the evidence obtained from reliable and independent source of the branch to properly establish such information in its records.
- Review if the branch has conducted enhanced customer due diligence which shall include obtaining more detailed information on the purpose of account opening, transaction and source of funds.

**Specific Procedures:**

1. Obtain the following information of clients customers of branch or unit;
  - Complete Name and Names Used
  - Present Address or residence, in the Philippines; or abroad, if customer is a non-resident
  - Permanent address, for both, resident and non-resident
  - Birthdate and birth place
  - Nationality
  - Nature of work of the customer e.g. attorney, cashier, physician (check if branch or unit used non-descriptive term such as business, employee, merchant, store owner (unless name of store is provided)
  - Name of Employer, if employed, and the complete address and telephone numbers of the employer
  - Nature of self-employment or business, or name of the single proprietorship and its complete address and telephone numbers
  - Customer's Tax Identification Number
  - Customer's Social Security Numbers or Government Services and Social Security Numbers
  - Sources of Funds
  - Complete name, address and contact information of beneficial owner
    - For broker dealers, whether the customer is an institutional customer
    - For broker dealers, the customer's investment objective
2. Verify if the branch or unit requires the following information in cases where the applicants are acting in representative capacity and legal capacity of the customer
  - a) Identify the principal owner or beneficiary, including data/information
  - b) If customer is a legal/juridical entity such as a corporation, the identity of the person authorized and beneficial owner, including information.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### A. REVIEW ON DOCUMENTATIONS

Verify that the branch's procedures and processes include comprehensive program for identifying customers who open an account.

#### Specific Procedures:

##### A.1 INDIVIDUALS AS CLIENTS

3. For purposes of No. 1, verify if the branch or unit requires from the customer the original copy of any of the following identification documents before opening of an account
  - a) Philippines passport or passport issued by a foreign government
  - b) Driver's license
  - c) PhilSys ID
  - d) Any official original identity card issued by the National Government of the Republic of the Philippines, its political subdivisions or instrumentalities, government owned or controlled corporations
    - PRC ID
    - NBI Clearance
    - Police Clearance
    - Postal ID
    - Voter's ID
    - Tax Identification Number
    - Barangay Certification
    - GSIS-ID Card
    - SSS Card
    - Senior Citizen Card
    - OWWA ID
    - OFW ID
    - Seaman's SCOK
    - Alien Certification of Registration / Immigrant Certificate of Registration
    - Government Office GOCC ID (e.g. AFP, HDMF IDs)
    - Certification from NCWDP
    - DSWD Certification
    - IBP ID and
    - Company IDs issued by private entities of institutions registered with or supervised or regulated either by the BSP, SEC or IC.
  
4. Verify if the branch or unit has obtained from the customer prior to the operating of an account the following:
  - a) Notarized special authorizations, for the representatives
  - b) Trust agreement, if acting as a trustee



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- c) Other pertinent and reasonable documents deemed necessary under the circumstances

#### **A.2 CORPORATE/PARTNERSHIP/SINGLE PROPRIETORS AS CLIENTS**

5. Verify if the branch or unit has obtained from your client copies of the following documents:
  - a) Certificate of registration issued by the SEC, for corporation or partnership, or by the Department of Trade and Industry, for single proprietorship including the articles of incorporation or partnership.
  - b) Latest General Information Sheet (GIS) and other Documents such as clearance from the SEC that the company is active and compliant with reportorial requirements.
  - c) Appropriate board resolutions
  - d) For clients or customers who are non-resident, verify if the branch or unit requires that the documents under no. 4 be duly authenticated by our Philippine Embassy or Consulate where said companies are located.

#### **B. REVIEW ON PROHIBITED ACCOUNTS**

6. Verify if the branch or unit has maintained accounts only in the name of account holders.
7. Verify if the branch or unit allow the opening, keeping or maintaining any of the following accounts:
  - Anonymous accounts
  - Fictitious name accounts
  - Incorrect name accounts
  - Account similar to the foregoing
8. Verify if the branch or unit refused opening of accounts under any of the following circumstances:
  - Those covered under No.7
  - Client fails to provide the requested evidence of identity

#### **C. REVIEW ON RENEWAL OF IDENTIFICATION**

9. Verify if the branch or unit regularly updates or renews identification of clients, particularly:
  - Changes of the applicable information required

#### **D. REVIEW ON AVERAGE CDD**

10. Verify if the branch or unit applies simplified or average customer due diligence to the following customers:



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

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

#### **E. REVIEW ON CORPORATE ACCOUNTS**

(11)

- a. Before establishing business relationship, verify if the branch or unit ensures that corporate client or other kind of business applicant has not been, or is not in the process of being dissolved, struck off, wound up, terminated.
- b. Review if the branch/business unit properly identified the ultimate beneficial owner (UBO) of the customers including the information and relevant documents.

#### **F. REVIEW ON TRUST, NOMINEES AND FIDUCIARY**

12. Verify if the branch or unit determines whether the client is acting in behalf of another person as trustee, nominee or agent.
13. Verify if the branch or unit establishes the identities of the agent/s and the authorized signatories, as well as the nature of their trustee or nominee's capacity and duties.
14. In case it is suspected that the trustee, nominee or agent is only dummy, verify if the branch or unit undertakes further verification to the business relationship between the parties.
15. In case satisfactory evidence of the beneficial owners cannot be obtained, verify if the branch or unit proceeds to:
  - Conduct or continue transacting with the client
  - Stop transacting with such account
16. For purposes of 15.1 Verify if the branch or unit undertakes the following:
  - Record any misgivings
  - Monitor said account

#### **G. REVIEW ON HIGH RISK CUSTOMERS**

Assess the adequacy of the branch to manage the risks associated with transactions involving politically exposed persons (PEPs) and other high risk accounts. Check the management's ability to implement effective due diligence, monitoring, and reporting systems.

#### **H. AREA OF RISKS**

In high-profile cases, PEPs have used banks as conduits for their illegal activities, including corruption, bribery, and money laundering. Banks that conduct business with dishonest PEPs face substantial reputation risk, enhanced scrutiny, and possible supervisory action.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### I. AUDIT PROCEDURES

- a) Obtain comprehensive due diligence information on PEPs and other high risk accounts
  - b) Review if the company has implemented policies, procedures, and processes pertaining to AML.
  - c) Check if the branch or unit provides greater scrutiny and monitoring of all PEP accounts and other high risk accounts
  - d) Check if the branch or unit has conducted enhanced due diligence to high risk customers
17. Verify if the branch or unit gives special attention to business relationship and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the Financial Action Task Force (FATF) Recommendations.
  18. Verify if the branch or unit establish the source of wealth of higher risk customers.
  19. Verify if the branch or unit seeks the approval of the senior management prior to business relationship with the high risk customers.

### II. MONITORING, RECORDING AND REPORTING

#### A. REVIEW ON MONITORING PROCESSES

20. Verify if the branch or unit conducts monitoring of the following business relationships and transactions
  - 1) Transaction involving trust, nominee and fiduciary accounts
  - 2) Transactions involving shell companies which have been allowed to transact after undertaking necessary verification Complex unusual large transactions or unusual patterns of Transactions
  - 3) Business relationships and transactions with persons, whether natural or juridical, from countries which do not or insufficiently apply the Financial Action Task Force Recommendations.
  - 4) Transactions which are suspected to be made by a person included in the list of suspected terrorist, or terrorist organizations that maybe furnished by the AMLC or by any other law enforcement agency or pursuant to internal policies and procedures.
  - 5) Transactions made by persons, whether individuals or corporate, who had been subjected to further verifications but nonetheless required to be monitored by the covered institution as part of its enhanced 'know-your-customer (KYC) application' of AMLA compliance procedure.
  - 6) Effectiveness of the transaction monitoring process in identifying, detecting and investigating unusual activities/transactions, and submit STR to the Compliance Department.



## Revised Money Laundering Terrorist Financing Prevention Program (MTPP)

### B. REVIEW ON RECORD KEEPING

21. Verify if the branch or unit maintains documentations on the following:
  - Customer relationship, identification and other pertinent data
  - Transactions
22. Verify if the branch or unit documentation is sufficient to permit reconstruction of individual transactions which will enable the AMLC to compile an audit trail should there be a report made pursuant thereto.
23. Verify if the branch or unit documentations include the information on the customer/beneficiary's name, address, nature and date of transactions, type and amount of currency involved, the type and identifying number of account, and information on whether a particular person is a customer or beneficial owner of the transactions.
24. Verify if the branch or unit documents referred to under Nos. 21 and 22 including recordings made under No. 16.1 and any analysis made to detect unusual or suspicious transactions available to the Commission and to the AMLC for its inspection.
25. Verify if the branch or unit apply the five (5) year retention period for the purpose of record keeping.
26. Verify if the branch or unit maintains a complete file on all transactions that have been brought to the attention of you Compliance Officer, including transactions that are not reported to the AMLC
27. Verify if the branch or unit requires the production of the original documents referred to herein and do you retain certified copies of aid documents, with the name of your employee certifying the documents clearly recorded.
  - a) if the original copies of the documents cannot be produced or certified copies cannot be retained, verify if the branch or unit records the reasons therefore.
28. Verify if the designated officer or staff authorized to keep or maintain the record referred to herein. (Specify the rank, office or designation)
  - a) Determine if the branch retains all records of customer's information and documents of transactions for at least five (5) years after the transaction has been completed or after the business relationship with the customer has ended such as:
    - Photo of individual customers
    - Customer information
    - Signature Card
    - Client Risk Assessment Form
    - Screenshot of Cross-checking with UN, Al Qaeda, OFAC, etc.)
  - b) Determine if the branch maintains Registry/LogSCOK for Closed Accounts



## **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- c) Determine if the branch conducts on-going customer due diligence to examine and clarify the economic background and purpose of any transaction or business relationship that appears unusual.
- d) Verify if all the KYC documents of the customers are scanned and uploaded in the Webloan system/ central database of the Bank so that the Compliance Officer may access the documents from time to time.

### **C. REVIEW ON REPORTING TO THE AMLC**

#### **C.1 GENERAL PROVISIONS**

- 29. Verify if the branch or unit has reported both covered transactions and suspicious transactions within five (5) working days from occurrence thereof.
- 30. Whenever any of branch officer or employee knows that the client has engaged in any of the predicate crimes under the AMLA, verify if the branch or unit promptly makes a report to the Compliance Officer.

#### **C.2 REVIEW ON COVERED TRANSACTION REPORTS**

- 31. Verify if the branch or unit reports to the AMLC transactions in cash or other equivalent monetary instrument involving a total amount in excess of the threshold of Five Hundred Thousand Pesos (P500,000.00) within one (1) day.

#### **C.3 REVIEW ON SUSPICIOUS TRANSACTION REPORTS**

- 32. Verify if the branch or unit reports to the AMLC transactions, regardless of the amount involved, where any of the following circumstances exists:
  - a) There is not underlying legal or trade obligation, purposes or economic justifications
  - b) The client is not properly identified.
  - c) The amount involved is not commensurate with the business or financial capacity of the client.
  - d) Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the AMLA, as amended.
  - e) Any circumstances relating to the transactions which is observed to deviate from the profile of the clients and/or the clients past transactions with the branch or unit.



### **Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

- f) The transactions is in any way related to an unlawful activity or offenses under the AMLA, as amended, that is about to be, is being or has been committed.

### **III. INTERNAL CONTROL AND PROCEDURES, COMPLIANCE AND TRAINING**

#### **➤ REVIEW ON INTERNAL CONTROL AND PROCEDURES**

- 33. Verify if the branch or unit follows bank's internal control and procedures aimed at preventing and impeding money laundering.

#### **E. REVIEW ON TRAININGS**

- 34. Verify if the branch officers and staff has attended trainings regardless of level of seniority.
- 35. Verify if the branch personnel has continuous trainings to but not limited to, identification of suspicious transactions, the procedures to be adopted when a transaction is deemed suspicious, and company's policy for dealing non-regular customers particularly where large case transactions or complex and unusual transactions are involved.
- 36. Verify if the branch manager has attended trainings but not limited to, offenses and penalties under the AMLA, the procedures relating to services of production and restrains, orders, internal reporting procedures, and the requirement for verification of identity and retention of records.
- 37. Verify if the branch officers and staff has attended, at least once a year, refresher trainings, but not limited to, updated or developments on money laundering techniques, methods and trends of money laundering and prevention aspects of the AMLA and obligations thereunder, the requirements on customer identification and due diligence, covered transactions and suspicious transactions reporting.

### **IV. VALIDATION/MONITORING OF AML CUSTOMER SELF-ASSESSMENT FORM QUESTIONNAIRES, HIGH RISK CUSTOMER, AML RELATED SYSTEMS AND DATABASES**

- 38. Validate the submitted AML Customer Self-Assessment Form Questionnaires of the branches/business units to the Compliance Department.
- 39. Check the monitoring of High Risk Customer of the branches/business units.
- 40. Check if the system/databases are updated.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**  
**ANNEX B**  
**AML COMPLIANCE TESTING RISK SCORING MATRIX**

The AMLC will ensure compliance by covered persons with these Guidelines through compliance checking or other modes that it may deem appropriate. Parallel to Section 5.a, the Supervising Authorities and Appropriate Government Agencies are enjoined to ensure that covered persons within their respective supervisory or regulatory authorities comply with these Guidelines by issuing and/or updating their respective circulars, or rules and regulations

The Following risk Level definitions shall be used by the AML Office in evaluating the individual risk issues noted during AML Compliance Testing.

Threat Probability		MINOR	MEDIUM	MAJOR
		IMPACT		
LIKELIHOOD	MOST	M	H	H
	MORE	L	M	H
	MUCH	L	L	M

RISK RATINGS / LEVEL OF RISK	
<b>HIGH</b>	If an issue is evaluated as a high risk concern, there is a strong need of corrective measures. Risk is almost sure or likely to happen and/or to have very serious/major consequences; therefore, a corrective action plan must be put in place as soon as possible.
<b>MODERATE</b>	If an issue is rated as moderate risk concern, risk could possible to happen and/or moderate consequences. Likewise, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
<b>LOW</b>	If an issue is described as low risk, risk is unlikely to happen and/or have minor or negligible consequences. However, regularization or certain adjustments are still necessary to mitigate the risk. Typically managed at operational level using routine procedures.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**IMPACT SCALE**

An impact scale refers to the seriousness of the damage (or otherwise) which could occur if the event (risk) happen. Impact of a ML/TF/PF risk could, depending on the financial institution (FI) and its circumstances, be rated or looked at from the point depending on FI's and its business circumstances, be rated or looked at from the point of view of:

- How it may affect the business (if though not dealing with risks properly, bank will suffers a financial loss from either crime or through penalties(sanction) given by the regulatory body (SEC and AMLC)
- The risk that a particular transaction may result in the loss of life or property through a terrorist act;
- The risk that a particular transaction may be involved in funds generated from the predicate crimes mentioned in the AML Manual.
- The risk that a particular transaction may be involved in financing or terrorism;
- Reputational risk – how it may affect bank if it is found to have (unknowingly) aided an illegal act, which may mean government sanctions and/or being ignored by the community of customers.
- How it may affect the wider community of customers if it is found to have aided an illegal act; the community may get a bad reputation as well as the business.
- Legal risk – How it may affect FI if it becomes a part of legal proceedings.
- All these impacts should be considered during measurements of impact scale.

**Impact Scale Table**

Consequence	Impact of an ML & TF risk
<b>MAJOR</b>	<ul style="list-style-type: none"> <li>• Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.</li> <li>• Material regulatory sanctions/penalties may arise due to serious non-compliance with the issued AMLC memorandum, circulars and other laws and regulations.</li> </ul>
<b>MEDIUM</b>	<ul style="list-style-type: none"> <li>• Moderate level of Money Laundering or terrorism financing impact</li> <li>• Minor regulatory sanctions/penalties may arise due to non-compliance with the issued AMLC memorandum, circulars and other laws and regulations</li> </ul>
<b>MINOR</b>	<ul style="list-style-type: none"> <li>• Minor or negligible consequences or effects</li> <li>• No expected or possible regulatory sanctions/penalties and can be managed on the operational level.</li> </ul>



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**LIKELIHOOD SCALE**

A Likelihood scale refers to the potential to potential of a ML/TF/PF risk occurring in the business for the particular risk is being assessed. Three (3) level of risk are show in the table below

**Likelihood Scale Table**

Frequency	Impact of an ML/TF/PF risk
<b>MOST</b>	<ul style="list-style-type: none"> <li>• 20% and above of the sampled accounts/transactions/documents have deficiencies or non-compliance</li> <li>• Non-performance of necessary actions for AML compliance occurring several times for the coverage testing period.</li> </ul>
<b>MORE</b>	<ul style="list-style-type: none"> <li>• Less than 20% to 10% of the sampled accounts/transactions/documents have deficiencies or non-compliance</li> <li>• Non-performance of necessary actions for AML compliance occurring seldom times for the coverage testing period.</li> </ul>
<b>MUCH</b>	<ul style="list-style-type: none"> <li>• Less than 10% of the sampled accounts/transactions/documents have deficiencies or non-compliance.</li> <li>• Non-performance of necessary actions for AML compliance occurring seldom times for the coverage testing period.</li> </ul>

**OVERALL REPORT RATING**

The following report rating definitions shall be used by the AML Office to draw an overall conclusion on the branch/unit’s compliance with the existing AML laws, rules and regulations, including internal policies and procedures:

<b>ABOVE ACCEPTABLE</b>	The level and quality of risk management is <b>ABOVE SATISFACTORY</b> for the branch/unit’s compliance to AML policies and procedures. <u>ZERO (0) or TWO (2) LOW RISK issues are noted in the AML testing preformed</u> and no unexpected materials findings from Internal Audit and Compliance Reviews
<b>ACCEPTABLE</b>	The level and quality of risk management is <b>SATISFACTORY</b> for the branch/unit’s compliance to AML policies and procedures. <u>THREE (3) or MORE LOW RISK issues or at least ONE (1) MODARATE RISK is noted in the AML testing preformed</u> and no unexpected materials findings from Internal Audit and Compliance Reviews
<b>BELOW ACCEPTABLE</b>	The level and quality of risk management is <b>INSUFFICIENT</b> for the branch/unit’s compliance to AML policies and procedures. There is inadequacy in the process and documents examined, requiring improvements in several AML Areas. <u>TWO (2) MODERATE RISK issues are noted in the AML testing performed</u> and occurrence of deficiencies can be addressed by regularization of cited accounts, submission of missing information/documents. If the deficiencies remain uncorrected, possible exposure to significant penalties may be imminent.
<b>UNACCEPTABLE</b>	The level and quality of risk management is <b>UNSATISFACTORY</b> for the branch/unit’s compliance to AML policies and procedures. <u>ONE (1) or more HIGH RISK issues are noted in the AML testing performed</u> and immediate and strict AML Compliance on the noted deficiencies must be taken due to a high probability of material sanctions/penalties form the regulations



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**  
**ANNEX C**  
**CUSTOMER RISK RATING METHODOLOGY**

## **I. INTRODUCTION**

In compliance with rule Section 9 of the 2018 Implementing Rules and Regulations (IRR) of Republic Act (R.A.) No.9160 otherwise known as Anti-Money Laundering Act of 2001, as amended in January 2021, South Asialink Finance Corporation developed the attached AML Customer Risk Assessment Form to determine the risk profile of our customer and assess the level of exposures and determine what customer due diligence procedures shall be applied.

The said form sets out the criteria in risk profiling wherein our personnel need to accomplish before establishing business relationship or opening of an account. This form also serves as the basis in assessing the inherent risk of the company in terms of customer type and due diligence pursuant to the requirement of the Institutional Risk Assessment (IRA) and Rule 18 of the IRR.

In order to insure appropriate procedures are in place to protect the Company from being used as a conduit for money laundering or terrorist financing, we must identify the customers, accounts and services that may be at higher risk for money laundering. When identified, appropriate monitoring procedures can be implemented to detect suspicious activity warranting further investigation.

### **I. FREQUENTLY ASKED QUESTION (FAQ)**

The following FAQ has been designed to help you understand our new customer risk rating and high risk customer monitoring process.

- 1. What are the risk rating codes and what do they mean?** Normal Risk and High Risk. Risk of the customer is classified based on their source of funds/wealth, public or high profile position, country of origin, etc.. This is also used to determine on what standard of customer due diligence procedures shall be applied, whether Average or Enhanced.
- 2. How do I determine the risk rating for my customer?** A form entitled, has been designed to assist you in the process. This form must be properly accomplished during onboarding/opening of account.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

RISK ASSESSMENT PROFILE (RAF)					
<input type="checkbox"/> <b>NORMAL RISK</b> *Indicate some details/specifications of the chosen item in the space provided.					
<b>INDIVIDUAL EARNINGS</b> <input type="radio"/> Salaried Employee <input type="radio"/> Pensioner/Retiree <input type="radio"/> OFW/Allottee <input type="radio"/> Foreign Individual	<b>SELF-EMPLOYED</b> <input type="radio"/> Store <input type="radio"/> Leasing Space <input type="radio"/> Trucking Business <input type="radio"/> PUV Operator	<b>PRIVATE PRACTITIONER</b> <input type="radio"/> Doctor <input type="radio"/> Lawyer <input type="radio"/> Accountant <input type="radio"/> Others _____	<b>AGRICULTURAL INDUSTRY</b> <input type="radio"/> Farmer/Fisher <input type="radio"/> Rice Dealer <input type="radio"/> LiveStock Dealer <input type="radio"/> Others _____	<b>BUSINESS</b> <input type="radio"/> Wholesaler <input type="radio"/> Distributor <input type="radio"/> Manufacturing <input type="radio"/> Others _____	<b>OTHER SERVICES</b> <input type="radio"/> Construction <input type="radio"/> Food/Hospitality <input type="radio"/> Healthcare <input type="radio"/> Others _____
Please specify: _____					
<input type="checkbox"/> <b>HIGH RISK</b> *Indicate some details/specifications of the chosen item in the space provided.					
<b>HIGH VALUE GOODS</b> <input type="radio"/> Pawnshops <input type="radio"/> Jewelry Shop <input type="radio"/> Car Dealer <input type="radio"/> High Value Items <input type="radio"/> Vehicle Buy & Sell	<b>MONEY TRADINGS</b> <input type="radio"/> Foreign Exchange <input type="radio"/> Money Changers <input type="radio"/> Remittance Agent/Center <input type="radio"/> Lending Business <input type="radio"/> Money Transfers/Service <input type="radio"/> Private Banking	<b>NON-PROFIT ORGANIZATION</b> <input type="radio"/> Charities <input type="radio"/> Foundations <input type="radio"/> Religious Sect <input type="radio"/> Civic Organization <input type="radio"/> Cultural Associations <input type="radio"/> Cooperatives	<b>GAMBLING BUSINESS</b> <input type="radio"/> Casino Agent <input type="radio"/> Lotto Outlet <input type="radio"/> Online Gambling Franchise <input type="radio"/> Cock Fighting & Horse Race <input type="radio"/> Off-Shore Gaming <input type="radio"/> Other Gaming Services	<b>SERVICE PROVIDERS</b> <input type="radio"/> Business trading via Internet <input type="radio"/> Virtual/Electronic Currencies <input type="radio"/> Private Armed Service Providers <input type="radio"/> Arms and Ammunition Dealers <input type="radio"/> Networking/Commission Based <input type="radio"/> Other Cash Incentive Activities	
Please specify: _____					
<input type="radio"/> <b>OTHERS</b>					

3. **What is Politically Exposed Person (PEP)?** PEP is a high-ranking official in the government, including his/her immediate family members up to second degree of consanguinity and affinity and closed associates. Please refer to the attached **Annex D** for the list of PEPs.
  
4. **Is PEP always considered as high-risk?** Once you establish that the customer is PEP, he/she is automatically considered as **high risk**. You do not need to fill out the Risk Assessment Profile. The CRAF should be **approved** by the Management and enhanced due diligence procedures should be performed before granting a loan and selling ROPA.
  
5. **What shall we do after we establish the risk rating of the customer?** If the customer falls under **Normal Risk**, it should be signed by **Preparer and Attestor ONLY**. On the other hand, once the customer is **PEP and High Risk**, it should be approved by the Management.
  
6. **What are the two (2) types of customers?** Individual and Corporation. Meanwhile, if the customer is the owner/manager/director/officer, it is individual. If the customer is the company itself, it should be corporation.
  1. **What shall we do if the customer is a corporation?** You also need to accomplish CRAF for **ALL** authorized signatories and beneficial owners.
  2. **Do we need to accomplish CRAF for guarantors and co-makers?** No. CRAF is only for principal borrower.
  3. **What does 'Linked to High risk Account' mean?** These are authorized signatories and beneficial owners of the corporation.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

4. **What shall we do in performing Customer Due Diligence?** First, you need to check if the applicant has adverse information/ derogatory records/ watchlisted in AML, OFAC, UN, Google search. Obtain ALL the data/information and documents/requirements from the applicant. Check the authenticity of the documents provided. Verify the information thru the documents submitted. Establish the proof of sources of funds and wealth. Require management approval for PEP and high risk applicant. Filled out the CRAF properly and completely.
5. **Shall I have to risk rate all of my new customers?** Yes. New customers shall be profiled and rate the risk started September 1, 2022. But eventually you will risk rate all existing customers during the record/file review.
6. **Can a customer's risk rating change?** Yes. You have to identify unexpected changes in customer activity that could signal a need to review the customer's account activity and possibly elevate the risk rating. This includes pre-termination of loans, and bulk payment of amortization and additional sources of funds. Certain high risk customers may qualify for normal risk rating (or reciprocally) based on a satisfactory relationship over a longer period of time.
7. **How often does a customer's risk rating have to be reviewed?** The frequency of the review process is shown below:

Task/Process	Frequency
PEP classification	Annual. Depending on the time a PEP assumed the office.
PEP Review	Mandatory Review every Three (3) years. Or every after election.
Reviewing factors for Risk Classification	Every 2 years for Normal Risk or due to Status update subject for reclassification.

8. **Why do we have to do this?** Anti-Money Laundering Council (AMLC) is closely monitoring the progress of covered persons as they establish programs to assess whether policies and practices as well as internal controls to prevent money laundering and terrorist financing are in place, well disseminated and effectively implemented.
9. **Will we receive any additional training?** Yes. We will be conducting training sessions on how to properly accomplish the CRAF and better understand the risk rating process.
10. **What if we failed to comply with this requirement?** The subject employee and his/her superior shall be given disciplinary actions in line with the Point System for Sales and Marketing (Audit Findings by CRD).



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**  
**ANNEX D**  
**LIST OF POLITICALLY EXPOSED PERSON**

**A. Elected Officials** - incumbent officials and former officials:

- President of the Philippines
- Vice President of the Philippines
- Senators
- Governors
- Vice Governors
- Provincial Board Member
- Congressmen
- Mayors
- Vice Mayors
- Councilors
- Barangay Chairman

**B. Appointed Officials** - incumbent officials and former officials:

- Cabinet Secretaries and Undersecretaries and other position of cabinet rank
- Supreme Court Justices
- Court of Appeals Justices
- Sandiganbayan Justices
- Officials of Constitutional bodies, i.e., Office of the Ombudsman, Commission on Election, Commission on Audit, etc.
- Regional Trial Court Judges
- Metropolitan Trial Court Judges
- City and Municipal Treasurers
- Provincial Treasurers
- Association of Barangay Chairmen (ABC) President to hold councilor-level position
- Sangguniang Kabataan Federation President to hold councilor-level position

**C. Officials of Government Owned and Controlled Corporations, Agencies, Commissions, and Bureaus**, whose rank are:

- President/ Administrator/ Commissioner/ Director/ Regional Director, or equivalent rank
- Vice President/ Deputy Administrator/ Deputy Commissioner/ Deputy Director/
- Deputy Regional Director, or equivalent rank
- Secretary/ Corporate Secretary
- Treasurer

*Note: The PEP definition under Item B includes those positions in an acting capacity (i.e., Acting DENR Secretary, Acting Deputy Director, Acting City Treasurer, Acting BIR Commissioner, etc.)*

- High ranking diplomats i.e., Permanent Representative (UN), Ambassador-at-Large, Resident Representative, Ambassadors, Charge d'affaires, Head of Mission, Consul, Resident Commissioner, Envoy.



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**D. Military and Police Officials** - includes incumbent, retired, and former military and police officials with the following ranks:

ARMY / AIRFORCE / MARINES / SCOUT RANGERS / PSG	NAVY / COAST GUARD	NATIONAL POLICE
1 <sup>st</sup> Lieutenant	Lieutenant Junior Grade	Police Inspector
Captain	Lieutenant Senior Grade	Police Senior Inspector
Major	Lieutenant Commander	Police Chief Inspector
Lieutenant Colonel	Commander	Police Superintendent
Colonel	Captain	Police Senior Superintendent
Brigadier General	Commodore	Police Chief Superintendent
Major General	Rear Admiral	Police Director
Lieutenant General	Rear Admiral	Police Director
Lieutenant General	Vice Admiral	Police Deputy Director General
General	Admiral	Police Director General

**E. Family members of the PEP**

- Spouse, common law husband/ common law wife
- 1st Degree  
 Consanguinity: father, mother, children (including adopted and illegitimate children)  
 Affinity: father-in-law, mother-in-law
- 2nd Degree  
 Consanguinity: grandparents, grandchildren, brothers, sisters  
 Affinity: grandparents-in-law, brothers-in-law, sisters-in-law



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)  
ANNEX E**

**CTR LOAN TRANSACTION CODES**

TXN TYPE	AML CODE	DESCRIPTION	REMARKS
LOAN RELEASE	LLNAC	Loan Availment (Regular/Foreign Currency Denominated Unit)	Cash Loan availed and released through cash
	<b>LLNAM</b>	<b>Loan Availment (Regular/Foreign Currency Denominated Unit)</b>	<b>MC/CC/OC Loan availed and released through manager's check/cashier's check.</b>
	LLNAP	Loan Availment (Regular/Foreign Currency Denominated Unit)	Mixed Payment Loan availed and released using two or more pay type
	LLNAW	Loan Availment (Regular/Foreign Currency Denominated Unit)	Wire Loan availed and released through wire
LOAN PAYMENT	LLPRC	Loan Payment (Regular/Foreign Currency Denominated Unit) - Cash	Payment of loan where settlement is made in cash
	LLPRM	Loan Payment (Regular/Foreign Currency Denominated Unit) - MC/CC/OC	Payment of loan where settlement is made by MC/CC or any other check
	LLPRP	Loan Payment (Regular/Foreign Currency Denominated Unit) - Mixed Payment	Payment of loan where settlement is made using two or more pay types (cash, checks, debit from account, wire)
	LLPRW	Loan Payment (Regular/Foreign Currency Denominated Unit)	Wire Payment of loan where settlement is made through wire
PRETERMINATION OF LOAN	LLTRC	Loan Pretermination (Regular/Foreign Currency Denominated Unit)	Cash Pretermination of loan where payment is made in cash
	LLTRM	Loan Pretermination (Regular/Foreign Currency Denominated Unit)	MC/CC/OC Pretermination of loan where settlement is made through manager's check/cashier's check
	LLTRP	Loan Pretermination (Regular/Foreign Currency Denominated Unit)	Mixed Payment Pretermination of loan where payment is made using two or more pay types (cash, checks, debit from account, wire)
	LLTRW	Loan Pretermination (Regular/Foreign Currency Denominated Unit)	Pretermination of loan where settlement is made through wire
OTHER LOAN TRANSACTIONS	<b>LLCAN</b>	<b>Loan Cancellation</b>	<b>Cancellation of an approved loan availed, call for cash for credit cards and similar transactions.</b>
	<b>LLRRW</b>	<b>Loan Renewal/Repricing</b>	<b>Takes place when a current loan is renewed, or its due date is extended before maturity date or its interest rates/outstanding obligation/periodic amortization is repriced whether a new promissory note is issued</b>
	LLRRE	Loan Restructuring (Regular/Foreign Currency Denominated Unit)	Takes place when a past due loan is renewed or its due date is extended after maturity date or its interest rates/outstanding obligation is repriced
	<b>LARSP</b>	<b>Sale Payment of Asset &amp; ROPA</b>	<b>Disposition of bank assets and ROPA either in cash or by installment and includes down payments, reservation fees and amortization.</b>

Transaction codes usually encountered by the Company for Generation of Covered Transaction Report



**Revised Money Laundering Terrorist Financing Prevention Program (MTPP)**

**ANNEX F**

**South Asialink Finance Corporation (SAFC)  
Anti-Money Laundering Committee**

**Chairman of the Committee:**

**Kevin John N. Cabanban  
President and CEO / AMLCOM**

**Members:**

**Roseshel M. Barrun  
Chief Compliance Officer**

**Ma. Theresa Medina  
Chief Finance Officer**

**Albert Gomez  
Credit and Collection Head**

**Cherry Ofielda  
Deputy COO for Sales and Marketing**

**Azenith S. Cabrera  
Deputy COO for Operations**

**[REDACTED]  
Legal Department Head**