



**UNITED COCONUT PLANTERS LIFE
ASSURANCE CORPORATION
(Also known as COCOLIFE)**

**ANTI-MONEY LAUNDERING AND
COUNTER-TERRORISM FINANCING MANUAL**

(Revised as of March 28, 2025)

OUTLINE OF CONTENTS

I. Our Policy -----	3
II. Definition of Terms -----	3
III. Compliance Framework -----	11
a. Risk Assessment -----	11
b. Roles and Responsibilities -----	11
Board and Senior Management Oversight	
Compliance Officer	
Management/Officers	
c. Group-Wide AML/CTF Compliance -----	13
d. Implementation of Money Laundering and Terrorism-Financing Prevention Program -----	13
e. Internal Controls and Internal Audit Program -----	14
IV. Guidelines on Anti-Money Laundering and Terrorism-Financing	15
a. Client Acceptance -----	15
b. Customer Identification -----	16
c. Identification and Verification of Agents and Beneficial Owners -----	18
d. Risk-Based CDD Standards -----	20
e. Simplified or Reduced Due Diligence -----	21
f. Average Due Diligence -----	22
g. Enhanced Due Diligence -----	22
h. Customer Due Diligence Measures on Beneficiaries -----	23
i. Risk Assessment and Customer Risk Profiling -----	24
j. Targeted Financial Sanctions (Related to Proliferation of Weapons of Mass Destructions and Proliferation Financing) -----	25
k. Ongoing Monitoring of Customers, Accounts and Transactions -----	26
l. Ongoing CDD and Monitoring of Existing Customers -----	26
m. Customer Verification -----	27
n. Face To Face Contact -----	28
o. Politically Exposed Persons (PEPs) -----	28
p. Customer Acceptance Policy -----	29
q. Customer Refusal Policy -----	30
r. Tipping-Off Policy -----	30

s. Institutional Risk Assessment -----	30
t. Recruitment Process -----	30
V. Reportorial Requirements -----	30
a. Notification and Reporting of Suspected Criminal Activities -----	30
b. Duty to Report Transactions -----	31
c. Record Keeping -----	33
d. Document Retention -----	34
e. Record of Information on Covered and Suspicious Transaction Reports -----	34
VI. On-Going Training -----	34
VII. AML Compliance Unit -----	35

I. OUR POLICY

COCOLIFE is committed to cultivating ethical responsibility which is central to enhancing public trust, company morale and long-term success. Consistent with this policy, it shall observe the letter and spirit of the law on Anti-Money Laundering. COCOLIFE likewise supports the efforts of the Bangko Sentral ng Pilipinas, the Anti-Money Laundering Council (AMLC) and the Insurance Commission (IC) in combating money laundering and the terrorism-financing.

COCOLIFE shall observe the following principles throughout its business:

- a. Conform with high ethical standards and observe good corporate governance;
- b. Know sufficiently its customers to prevent any suspicious entity from transacting with or maintaining relationship with the Company;
- c. Adopt and effectively implement an anti-money laundering and counter-terrorism financing (AML/CTF) risk management system that identifies, monitors, and controls risks associated with money laundering and terrorist-financing;
- d. Comply with the existing laws and regulations aimed at combating money laundering and terrorist financing by making sure that officers and employees are aware of their respective responsibilities.

II. DEFINITION OF TERMS

- A. **Anti-Money Laundering Act (AMLA)** refers to Republic Act No 9160, as amended by Republic Act Nos. 9194, 10167, 10365 and 10927.
- B. **Anti-Money Laundering Council** refers to the financial intelligence unit of the Philippines which is the government agency tasked to implement the AMLA and The Terrorism Financing Prevention and Suppression Act (TFPSA).
- C. **Financing of Terrorism** is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (i) carry out or facilitate the commission of any terrorist act; (ii) by a terrorist organizations, association or group; or (iii) by an individual terrorist.
- D. **Person** refers to any natural or juridical person.
- E. **Transaction** refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered Person.
- F. **Competent Authorities** refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the AMLC; the authorities that have the function of investigating and/or prosecuting

money laundering unlawful activities and terrorist financing, and seizing/freezing and confiscating any monetary instrument or property that is in anyway related to an unlawful activity; Authorities receiving reports on cross-border transportation of currency & bearer negotiable instruments (BNIs); and authorities that have Anti-Money Laundering (AML)/Counter-Terrorism Financing(CTF) supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and Designated Non-Financial Business and Professions (DNFBPs) with AML/CTF requirements.

G. Covered Transaction refers to:

- a. A transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand pesos (Php500,000.00) or its equivalent in any other currency.
- b. A transaction, regardless of frequency of payment (monthly, quarterly, semi-annually or annually), where the total premiums/fees paid for a policy, plan or agreement for the entire year exceeds Five Hundred Thousand Pesos (Php500,000.00) or its equivalent in any other currency.

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

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

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

Other suspicious transactions include, but are not limited to:

1. Purchase of a single premium contract especially by a policyholder whose previous policies are with smaller regular modes of payment.
2. Payment by means of a third-party check or multiple blank checks or money order.

3. Payment in cash when, normally, this would be handled by checks.
4. Lump sum payments with foreign currency or foreign wire transfers.
5. Lump sum contributions to PDF or Fund Builder or large sum mutual fund placements, especially when client shows no concern for the performance of the investment, but much concern for the surrender or early cancellation of the contract.
6. Accelerating premium payments.
7. Borrowing from a single premium policy shortly after paying for it.
8. Early surrender of a single premium policy.
9. Applications for jumbo policies beyond the policyholder's apparent means, as in business coming from BIR or Customs personnel, military, policemen and politically exposed persons (PEPs).

I. **Customer/Client** refers to any person who keeps an account, or otherwise transacts business with the Insurance Commission Regulated Entities (ICRE). It includes the following:

1. Beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained or a transaction is conducted;
2. Transactors, agents and other authorized representatives of beneficial owners;
3. Beneficiaries;
4. A company or person whose assets are managed by an asset manager;
5. Trustor/grantors/settlors of a trust;
6. Insurance policy holder/owner, insured, pre-need plan holder, HMO client, or HMO enrolled member, whether actual or prospective: and
7. Juridical Person.

The term juridical person shall refer to an entity other than a natural person as defined under the civil code of the Philippines, including corporate clients who keep or maintain an account with COCOLIFE.

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

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

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

M. **Beneficial Owner** refers to any natural person who:

1. Ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or

2. Has ultimate effective control over a legal person or legal arrangement; or
3. Owns the same percentage as prescribed in the Guidelines on Identifying Beneficial Ownership and 2018 IRR, and its succeeding future amendments

Control includes whether the control is exerted by means of trusts, agreements, arrangements, understandings, or practices, and whether or not the individual can exercise control through making decisions about financial and operating policies.

N. Identification Document (ID) refers to any of the following evidence of identity:

1. For Filipino citizens: Those issued by any of the following official authorities:
 - a. PhilID;
 - b. Other identification issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities; and
 - c. Other identification documents that can be verified using reliable, independent source documents, data or information.
2. For foreign nationals:
 - a. PhilID, for resident aliens;
 - b. Passport;
 - c. Alien Certificate of Registration; and
 - d. Other identification documents issued by the Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities
3. For Filipino students:
 - a. PhilID;
 - b. School ID signed by the school principal or head of the educational institution; and
 - c. Birth Certificate issued by the Philippine Statistics Authority; and
4. For low risk customers: Any document or information reduced in writing which the covered person deems sufficient to establish the customer's identity.

O. Monetary Instrument shall include, but is not limited to the following:

1. Coins or currency of legal tender of the Philippines, or of any other country;
2. Credit instruments, including bank deposits' financial interest, royalties, commissions, and other intangible property;
3. Drafts, checks, and notes;
4. Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character, including those enumerated in Section 3 of the Securities Regulation Code;
5. A participation or interest in any non-stock, non-profit corporation;
6. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates' custodial receipts, or deposit substitute

instruments, trading orders, transaction tickets, and confirmations of sale or investments and money market instruments;

7. Contracts or policies of insurance, life or non-life, contracts of suretyship, pre-need plans, and member certificates issued by mutual benefit association; and
8. Other similar instruments where title thereto passes to another by endorsement, assignment, or delivery.

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

1. Personal property, including proceeds derived therefrom, or traceable to any unlawful activity, such as, but not limited to:
 - a. Cash;
 - b. Jewelry, precious metals and stones, and other similar items;
 - c. Works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;
 - d. Perishable goods; and
 - e. Vehicles, vessels, aircraft, or any other similar conveyance.
2. Personal property, used as instrumentalities in the commission of any unlawful activity, such as:
 - a. Computers, servers, and other electronic information and communication systems; and
 - b. Any conveyance, including any vehicle, vessel, and aircraft.
3. Real estate, improvements constructed or crops growing thereon, or any interest therein, standing upon the record of the registry of deeds in the name of the party against whom the freeze order or asset preservation order is issued, or not appearing at all upon such records, or belonging to the party against whom the asset preservation order is issued and held by any other person, or standing on the records of the registry of deeds in the name of any other person, which are:
 - a. derived from, or traceable to, any unlawful activity; or
 - b. used as an instrumentality in the commission of any unlawful activity.

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

R. **Monetary Instrument or Property Related to an Unlawful Activity** refers to:

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

- S. **Related Accounts** refers to those accounts, the funds and sources of which directly originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.
- T. **Materially-linked Accounts** shall include the following:
1. All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;
 2. All accounts or monetary instruments held' owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another Person;
 3. All "In Trust For" accounts where 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;
 4. All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;
 5. All accounts of juridical persons or legal arrangements that are owned, controlled or ultimately effectively controlled by the natural person whose accounts, monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control; and
 6. All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing.
- U. **Offender** refers to any person who commits a money laundering offense.
- V. **Unlawful Activity** refers to any act or omission, or series or combination thereof, involving or having direct relation, to the following:
1. *"Kidnapping for Ransom"* under Article 267 of Act No 3815, otherwise known as the Revised Penal Code, as amended;
 2. Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15 and 16 of Republic Act No. 9165, otherwise known as the *"Comprehensive Dangerous Drugs Act of 2002"*;
 3. Section 3 paragraphs b, c, e, g, h and i of Republic Act No. 3019, as amended, otherwise known as the *"Anti-Graft and Corrupt Practices Act"*;
 4. *"Plunder"* under Republic Act No. 7080, as amended;
 5. *"Robbery"* and *"Extortion"* under Articles 294, 295, 296, 299, 300, 301 and 302 of the Revised Penal Code, as amended;
 6. *"Jueteng"* and *"Masiao"* punished as illegal gambling under Presidential Decree No. 1602;
 7. *"Piracy on the High Seas"* under the Revised Penal Code, as amended, and Presidential Decree No. 532;
 8. *"Qualified Theft"* under Article 310 of the Revised Penal Code, as amended;
 9. *"Swindling"* under Article 315 and *"Other Forms of Swindling"* under Article 316 of the Revised Penal Code, as amended;

10. *"Smuggling"* under Republic Act No. 455, and Republic Act No. 1937, as amended, otherwise known as the *"Tariff and Customs Code of the Philippines"*;
11. Violations under Republic Act No. 8792, otherwise known as the *"Electronic Commerce Act of 2000"*;
12. *"Hijacking"* and other violations under Republic Act No. 6235, otherwise known as the *"Anti-Hijacking Law"*; *"Destructive Arson"*; and *"Murder"*, as defined under the Revised Penal Code, as amended;
13. *"Terrorism"* and *"Conspiracy to Commit Terrorism"* as defined and penalized under Sections 3 and 4 of Republic Act No 9372;
14. *"Financing of Terrorism"* under Section 4 and offenses punishable under Sections 5, 6, 7 and I of Republic Act No. 10168, otherwise known as the *"Terrorism Financing Prevention and Suppression Act of 2012"*;
15. *"Bribery"* under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, and *"Corruption of Public Officers"* under Article 212 of the Revised Penal Code, as amended;
16. *"Frauds and Illegal Exactions and Transactions"* under Articles 213, 214, 215 and 216 of the Revised Penal Code, as amended;
17. *"Malversation of Public Funds and Property"* under Articles 217 and 222 of the Revised Penal Code, as amended;
18. *"Forgeries"* and *"Counterfeiting"* under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code, as amended;
19. Violations of Sections 4 to 6 of Republic Act No. 9208, otherwise known as the *"Anti-Trafficking in Persons Act of 2003, as amended"*;
20. Violations of Sections 78 to 79 of Chapter IV of Presidential Decree No. 705, otherwise known as the *"Revised Forestry Code of the Philippines, as amended"*;
21. Violations of Sections 86 to 106 of Chapter VI of Republic Act No. 8550, otherwise known as the *"Philippine Fisheries Code of 1998"*;
22. Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the *"Philippine Mining Act of 1995"*;
23. Violations of Section 27(c), (e), (f), (g) and (i) of Republic Act No. 9147, otherwise known as the *"Wildlife Resources Conservation and Protection Act"*;
24. Violations of Section 7(b) of Republic Act No. 9072, otherwise known as the *"National Caves and Cave Resources Management Protection Act"*;
25. Violation of Republic Act No. 6539, otherwise known as the *"Anti-Carnapping Act of 1972, as amended"*.
26. Violation of Sections 1, 3, and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree *"Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives"*;
27. Violation of Presidential Decree No. 1612, otherwise known as the *"Anti-Fencing Law"*;
28. Violation of Section 6 of Republic Act No 8042, otherwise known as the *"Migrant Workers and Overseas Filipinos Act of 1995, as amended"*;
29. Violation of Republic Act No. 8293, otherwise known as the *"Intellectual Property Code of the Philippines, as amended"*;
30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the *"Anti-Photo and Video Voyeurism Act of 2009"*;

31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the "*Anti-Child Pornography Act of 2009*";
32. Violations of Sections 5, 7, 8, 9, 10 (c), (d) and (e), 11, 12 and 14 of Republic Act No. 7610, otherwise known as the "*Special Protection of Children Against Abuse, Exploitation and Discrimination*";
33. Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the "*Securities Regulation Code of 2000*";
34. Violation of Section 19 (A)(3) of Republic Act No. 10697, otherwise known as "*The Strategic Trade Management Act*", in relation to Proliferation of WMD and PF pursuant to UNSC Resolution Nos. 1718 of 2006 and 2231 of 2015;
35. Violations of Section 254 of Chapter II, Title X of the "National Internal Revenue Code of 1997", as amended, where the deficiency basic tax due in the final assessment is in excess of Twenty-Five Million Pesos (P25,000,000.00) per taxable year, for each tax type covered and there has been a finding of probable cause by the competent authority: Provided, further, that there must be a finding of fraud, willful misrepresentation or malicious intent on the part of the taxpayer: Provided, finally, that in no case shall the AMLC institute forfeiture proceedings to recover monetary instruments, property or proceeds representing, involving, or relating to a tax crime, if the same has already been recovered or collected by the Bureau of Internal Revenue (BIR) in a separate proceeding;
36. Felonies or offenses of a nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

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

W. Money Laundering is committed by:

1. Any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:
 - a. Transacts said monetary instrument or property;
 - b. Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
 - c. Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
 - d. Attempts or conspires to commit money laundering offenses referred to in (a), (b), or (c) above;
 - e. Aids, abets, assists in, or counsels the commission of the money laundering offenses referred to in (a), (b)' or (c) above; and
 - f. Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in (a), (b), or (c) above.

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

III. COMPLIANCE FRAMEWORK

1. RISK ASSESSMENT

COCOLIFE instituted the following processes in assessing their money laundering and terrorist financing (ML/TF) risks:

- i. The Compliance Officer shall conduct a sound risk management practice within COCOLIFE's operation by documenting its assessments and findings to ensure that risks associated with money laundering and terrorist financing such as counterparty, reputational, operational and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of these Guidelines, to the end that COCOLIFE shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.
- ii. Considering all the relevant risk factors, including the results of national and sectoral risk assessment before determining what is the level of overall risk and appropriate level and type of mitigation to be applied;
- iii. Keeping the assessment up-to-date through periodic review; and an annual review of the risk as through a Comprehensive Compliance Testing to manage the risk associated with transactions involving accounts considered as vulnerable to money laundering risk and ensure the conduct of enhanced due diligence procedures on all high-risk accounts.
- iv. All risk assessment and finding shall be kept by COCOLIFE's AML Secretary for submission to the Insurance Commission, as may be required.
- v. Ensure submission of the risk assessment information as may be required by the Insurance Commission.
- vi. It shall conduct an Institutional risk assessment once every two (2) years which will be headed by the AML Compliance Officer, or as often as the Board or Senior Management may direct, depending on the level of risks identified in the previous assessment, or other relevant AML/CTF developments that may have an impact on COCOLIFE's operation.

2. ROLES AND RESPONSIBILITIES

1. Active Board and Senior Management Oversight

The Board of Directors is ultimately responsible for ensuring compliance with the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) laws, their respective implementing rules and regulations, and other directives, guidance and issuances of the IC and AMLC.

The Board of Directors shall ensure that COCOLIFE will not be used as a site or a party of money laundering or financing terrorism.

The Board of Directors shall appoint a Compliance Officer that shall directly report as regards the day-to-day transaction or any concerns arising in relation to money laundering or financing of terrorism. Should the Board of Directors delegate audit, whether announced or unannounced, the auditor, both internal and external, shall directly report to the Board of Directors.

The Board of Directors shall approve manuals, prevention programs and policies, to strengthen the steps taken, in relation to money laundering and terrorism financing and shall exercise active oversight together with the Compliance Officer who will be the lead implementer. The manual and programs are also applicable and must be followed by all Branches.

Senior Management shall oversee the day-to-day management of COCOLIFE, ensure effective implementation of the AML/CTF policies approved by the Board and alignment of activities with the strategic objectives, risk profile and corporate values set by the board. Senior management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

2. Compliance Officer

COCOLIFE designated a compliance officer of senior management status with the authority and mandate to ensure day-to-day compliance with AML/CTF obligations of the Company.

The compliance officer shall also ensure that compliance measures reflect readily available information concerning new trends in ML and TF and detection techniques.

The Compliance Office has direct reporting line to the Board of Directors or any board-level or approved committee on all matters related to AML and CTF compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by senior management and the board, to wit:

- i. Ensure compliance by all responsible officers and employees with this Manual, the AML and CTF Laws, their respective implementing rules and regulations, other directives, guidance and issuances from the IC and AMLC. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of AML and CTF transaction monitoring system and record retention system through sample testing and review of audit or checking reports. It shall also report compliance findings to the Board;
- ii. Ensure that infractions, discovered either by internally initiated audits, or by special or regular compliance checking conducted by the IC and/or AMLC are immediately corrected;

- iii. Inform all responsible officers and employees of all resolutions, circulars and other issuances by the IC and/or the AMLC in relation to matters aimed at preventing ML and TF;
- iv. Alert senior management and the board of directors if it believes that COCOLIFE is failing to appropriately address AML/CTF issues; and
- v. Organize the timing and content of AML/CTF training of officers and employees including regular refresher trainings.

3. Management/Officers

Members of the Management/Officers are responsible for ensuring that staff adhere consistently to the AML/CFT policies and procedures to prevent money laundering and terrorist financing.

For this purpose, COCOLIFE shall devise guidelines detailing the duties and responsibilities of the Management, Officers and employees/staff in accordance with this Manual.

C. GROUP -WIDE AML/CFT COMPLIANCE

For the branches or offices located within the Philippines, the Compliance Officer, or its duly authorized representative, of COCOLIFE, shall oversee the AML/CTF compliance of the entire group with reasonable authority over the compliance officers of said branches or offices.

D. IMPLEMENTATION OF A MONEY LAUNDERING & TERRORISM-FINANCING PREVENTION PROGRAM (MTPP)

COCOLIFE shall implement internal policies, controls and procedures on the following:

- i. Risk assessment and management;
- ii. Detailed procedures of the ICREs' compliance and implementation of customer due diligence, record-keeping and transaction reporting requirements;
- iii. An effective and continuous AML/CTF training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under the AML and CTF laws, their respective implementing rules and regulations, the Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Guidelines for Insurance Commission Regulated Entities, and other applicable IC and AMLC issuances, their own internal policies and procedures, and such other obligations as may be required by the IC and/or the AMLC;
- iv. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personal with no criminal record or integrity-related issues are employed or contracted by COCOLIFE;

- v. Independent audit function to test the system. COCOLIFE shall specify in writing the examination scope of independent audits, which shall include evaluation or examination of the following:
 - a. Risk assessment and management;
 - b. MTPP;
 - c. Accuracy and completeness of customer identification information, covered and suspicious transaction reports, and all other records and internal controls pertaining to compliance with the AML and CTF Laws, their respective Implementing Rules and Regulations, the Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Guidelines for Insurance Commission Regulated Entities and other relevant IC and AMLC issuances.
- vi. A mechanism that ensures all deficiencies noted during inspection and/or regular or special compliance checking are immediately and timely corrected and acted upon;
- vii. Cooperation with the IC, AMLC and other competent authorities;
- viii. Designation of a Compliance Officer at the management level, as the lead implementer of the COCOLIFE's compliance program or creation of compliance unit;
- ix. The identification, assessment and mitigation of ML/TF risks that may arise from new business practices, services, technologies and products;
- x. Adequate safeguards on the confidentiality and use of information exchange, including safeguards to prevent tipping off;
- xi. A mechanism to comply with freeze, inquiry and asset preservation orders and all directives of the AMLC; and
- xii. A mechanism to comply with the prohibitions from conducting transactions with designated persons and entities, as set out in relevant United Nations Security Council Resolutions (UNSCRs) relating to the preservation and suppression of terrorism and terrorist financing and financing of proliferation of weapons of mass destruction.

The MTPP shall be regularly updated at least once every two (2) years to incorporate changes in the AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent IC and/or AMLC issuances. Any revision or update in the MTPP shall likewise be approved by the Board of Directors (BOD).

The compliance officer shall submit to the IC not later than fifteen (15) days from the approval of the BOD of the new/updated MTPP a sworn certification that a new/updated MTPP has been prepared, duly noted and approved by the BOD.

E. INTERNAL CONTROLS AND INTERNAL AUDIT PROGRAM

COCOLIFE shall establish internal controls to ensure day-to-day compliance with its AML/CTF obligations under the AML and CTF laws, their respective implementing rules and regulations, the Anti-Money Laundering/Counter-Terrorism Financing Guidelines for

Insurance Commission Regulated Entities, and other applicable IC and AMLC issuances, taking into consideration the size and complexity of its operations

COCOLIFE's internal audit program shall include periodic and independent evaluation of COCOLIFE's risk management, as well as the sufficiency and degree of adherence to its compliance measures. The auditors shall support a direct line of communication with the BOD.

To ensure periodic and independent evaluation of the COCOLIFE's risk management, as well as the sufficiency and degree of adherence to its compliance measure, an independent internal audit examination shall be conducted at least once every year or at such frequency as necessary, consistent with the risk assessment of COCOLIFE. The independent internal audit examination scope shall cover the accuracy of customer identification information, covered and suspicious transaction reports, and all other records and internal controls pertaining to compliance with AML/CTF obligations.

IV. GUIDELINES ON ANTI-MONEY LAUNDERING AND TERRORISM-FINANCING

Recognizing that money laundering empowers corruption and organized crime and that it is bad for the economy, the country's development, and business, COCOLIFE has adopted the following guidelines and procedures to prevent and impede money laundering.

A. CLIENT ACCEPTANCE

In order to comply with the requirements of AMLC as regards accepting clients, the following are the standards that shall be implemented by COCOLIFE in relation to accepting new clients or renewal of clients, businesses or partnership with COCOLIFE:

1. It shall be the policy of COCOLIFE for all clients, regardless of the nature of transaction, to require the risk-based and tiered policy;
2. In all instances, COCOLIFE shall document how a specific customer was profiled (low, normal or high) and what standard of CDD (reduced average or enhanced) was applied.
3. COCOLIFE shall require a more extensive due diligence for high-risk clients, such as those known in public as controversial personalities, those individuals holding prominent public position (Politically Exposed Persons);
4. Decisions to enter into business relationships with high-risk clients shall be taken exclusively by senior management officers or the Board of Directors, on case to case basis considering the risk;
5. It shall be the policy of COCOLIFE not to accept or enter into business relationship with clients who refuse to produce the required identification documents and to discontinue business relationship with clients, who after a series of follow up requests, failed to submit customer identification documents.

Further, COCOLIFE will not accept as customers or conduct transactions with persons or entities in the following circumstances:

- i. The customer has been identified by reliable sources as being a criminal or terrorist or being associated with criminal or groups;
- ii. The customer is involved in certain criminal or such other activities that are considered to be of high risk, given the nature of the source of funds;
- iii. The customer is from a jurisdiction which has been identified as an area/country of high risk by the financial intelligence unit and/or supervisory authority;
- iv. The customer is from a jurisdiction identified by reliable sources as one that has high levels of criminal or terrorist activities; and
- v. The employee has reason to believe, based on the behavior of the customer or other factors that the transaction may be related to money laundering or the findings of terrorism. In case where COCOLIFE form a suspicion of ML/TF and associated unlawful activities and reasonably believes that performing the CDD process would tip off the customer, COCOLIFE is permitted not to pursue.

B. CUSTOMER IDENTIFICATION

1. Establish and record the true and full identity of insurance applicants based on official documents. All policy contracts shall be issued only in the true and full name of the policy owner.
 - a. For **individual applicants**, the following identification information and identification documents should be obtained from the individual customers before establishing the business relationship:
 1. Full Name;
 2. Date and Place of birth;
 3. Present address;
 4. Permanent address;
 5. Contact number or information;
 6. Citizenship or nationality;
 7. Specimen signature or biometrics of the customer;
 8. Name, address, date and place of birth, contact number or information, sex, and citizenship or nationality of beneficiary and/or beneficial owner, whenever applicable;
 9. Proof of Identification and Identification Number;
 10. Nature of work and name of employer or nature of self-employment/ business, if applicable;
 11. Sources of funds or property; and
 12. PhilID or other identification document, as herein defined.

Ask them to produce original documents of identity issued by an official authority and bearing the photograph and signature of the client. (e.g. passport, SSS or GSIS ID, driver's license, company ID's, postal ID).

Photocopy the ID presented, certify to the authenticity of the photocopy and attach the same to the application form.

Note: Where the customer or authorized representative is a foreign national, COCOLIFE shall require said foreign national to present valid passport, Alien Certificate of Registration, Alien Employment Permit' or any government issued identification document bearing the photograph of the customer or beneficial owner, provided that COCOLIFE can be satisfied with the authenticity of the document.

b. For **new customers/clients** that are **juridical persons**, the following identification information and identification documents should be obtained before establishing business relationship:

1. Full Name;
2. Name of authorized representative/transactor/signer;
3. Current office address;
4. Contact number or information;
5. Nature of business;
6. Source of fund;
7. Specimen signature or biometrics of the authorized representative/transactor/signer;
8. Name, address, date and place of birth, contact number or information, sex and citizenship or nationality of beneficiary and/or beneficial owner, if applicable;
9. Certificates of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation or Partnership issued by the Securities and Exchange Commission (SEC) for corporations and partnerships, respectively, and by the Bangko Sentral ng Pilipinas (BSP) for money changers/foreign exchange dealers and remittance agents, and by the AMLC for covered persons;
10. Articles of Incorporation/Partnership;
11. Registration Data Sheet/Latest General Information Sheet;
12. Secretary's Certificate citing the pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity;
13. For entities registered outside of the Philippines, similar documents and/or information duly authenticated by a senior officer of the covered person assigned in the country of registration; in the absence of said officer, the documents shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered; and

For the identification documents of customers/clients that are juridical persons, the originals or true copies certified by the issuing government agency should be produced for verification.

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

- c. For **legal arrangements** (Trust or other similar arrangement), identify and verify the identity of the customer and understand the nature of business and its ownership and control structure through the following information:
1. Full name of legal arrangement;
 2. Current office address and country of establishment;
 3. Contact number or information; if any;
 4. Nature, Purpose and objects of the legal arrangement;
 5. The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement;
 6. Deed of trust and/or other proof of existence;
 7. Duly accomplished AML/CTF/KYC Questionnaire; and
 8. Other requirements for juridical persons, as applicable.
2. Additional verification measures should be undertaken if there is reason to doubt the accuracy of the information given on the application form or the veracity of the identification presented (e.g. telephone confirmation with client's employer, payroll slip, presentation of existing insurance policies). Record details of the additional checks.
 3. All applicants should be seen face-to-face and interviewed personally by the agent or the employee.
 4. In case the identification document presented does not bear any photo of the customer or authorized signatory, or the photo-bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory, COCOLIFE shall utilize its own technology to take the photo of the customer or authorized signatory.
 5. It is not necessary for Group Marketing and Healthcare to re-identify transferred accounts, provided all client records are acquired with the business and they are satisfied that the previous carrier or insurer has complied with AMLC procedures and requirements.
 6. Make clients aware of the Insurance Commission's policy that transactions will **NOT** be conducted with applicants who fail not only to provide evidence of their identity, but also to prove the purpose and intended nature of the insurance relationship. Furthermore, we shall file a suspicious transaction report with the Anti-Money Laundering Council regarding these cases.

C. IDENTIFICATION AND VERIFICATION OF AGENTS AND BENEFICIAL OWNERS

1. Identification and Verification of Agents
 - a. As general requirement, COCOLIFE 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.

- b. Where an account is opened or an occasional transaction in excess of the threshold is conducted by any person in behalf of another, COCOLIFE shall establish and record the true and full identity and existence of both the account holder or person purporting to act on behalf of the customer, and the beneficial owner or the principal on behalf the transaction is being conducted.
 - c. COCOLIFE 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.
- 2. Beneficial Ownership Verification (BOV)
 - a. As general requirement, COCOLIFE shall identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source such that COCOLIFE is satisfied that it knows who the beneficial owner is.
 - b. COCOLIFE shall the true nature of the beneficial owner's capacities and duties vis-à-vis his agent by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of CDD to be applied to both.
 - c. COCOLIFE shall verify the identity of the beneficial owner before or during the course of establishing a business or professional relationship, or conducting transactions for occasional customers in excess of the threshold. They may complete the BOV after the establishment of the business or professional relationship: Provided, that: a) this occurs as soon as reasonably practicable; b) this is essential not to interrupt the normal conduct of business; and c) the ML/TF risks are effectively managed.
- 3. Verification of Beneficial Ownership for Juridical Persons

For customers that are juridical persons, COCOLIFE shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

 - a. the identity of the natural persons if any, who ultimately have controlling ownership interest in a juridical person;
 - b. to the extent that there is a doubt under item (a) above, as to whether the persons with the controlling ownership interest are the beneficial owners or no natural person exerts control through ownership interests, the identity of the natural persons, if any, exercising control over the juridical person through other means: and
 - c. where no natural person is identified under items (a) and (b) above, the identity of the relevant natural persons who hold senior management positions.

4. Verification of Beneficial Ownership for Legal Arrangements
- For customers that are legal arrangements, COCOLIFE shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:
- a. For trust: the identity of the trustors/grantors/settlers, the trustees, the beneficiaries or class of beneficiaries, the protector, if any, and any other natural person exercising ultimate effective control over the trust agreement.
 - b. For beneficiaries of trust agreements that are designated by characteristics or by class: sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish the identity of the beneficiary at the time of payout or when the b intends to exercise vested rights.
 - c. For other types of legal arrangements: the identity of persons in equivalent or similar positions.

In determining the reasonableness of the identity verification measures, COCOLIFE shall consider the money laundering and terrorist financing risks posed by the customers and the business relationship.

D. RISK-BASED CDD STANDARDS

COCOLIFE shall undertake satisfactory CDD measures:

- a. Before establishing business relationship;
- b. There is any suspicion of Money Laundering or Terrorist Financing; and
- c. There is doubt about the integrity or adequacy of previously obtained customer identification information.

Provided, that where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, COCOLIFE may complete verification after the establishment of business relationship so as not to interrupt normal conduct of business. The verification of the identity of the customer shall be conducted during the duration of the policy/plan/agreement or at the time the customer files his/her claim, as the case may be.

1. CDD Standards

COCOLIFE shall implement the following standards of CDD:

- a. Identify and verify the identity of a customer using reliable, independent source documents, data or information. The **Application Forms** for respective customers shall be properly filled-up in order to identify the Customer.
- b. Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;

- c. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner based on official documents, or using relevant information or data obtained from reliable sources, such that COCOLIFE is satisfied that it knows who the beneficial owner is. COCOLIFE shall have a system to understand the nature of the customer's business and its ownership and control structure, in case of juridical persons or legal arrangements.

COCOLIFE shall keep records of the actions taken in order to identify the beneficial owner:

- a. Determine, understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship with the customers; and
- b. Conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with COCOLIFE's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

E. SIMPLIFIED OR REDUCED CUSTOMER DUE DILIGENCE (SDD)

The following measures shall apply where lower risks of ML/TF have been identified, through an adequate analysis of risk and based on the result of the institutional risk assessment:

- 1. a. For individual clients, upon presentation of acceptable identification card or official document as defined in this Manual or other reliable, independent source documents, data or information may avail of the products of COCOLIFE.
- b. For corporate, partnership, and sole proprietorship entities, upon submission of the required documents may avail of the products of COCOLIFE or may invest with COCOLIFE.
- 2. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
- 3. Reducing the frequency of customer identification updates;
- 4. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- 5. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified or reduced customer due diligence measures are not acceptable whenever there is suspicion of ML/TF, or where specific higher risk scenarios apply.

F. AVERAGE DUE DILIGENCE

COCOLIFE shall apply Average Due Diligence for medium/normal-risk clients:

COCOLIFE shall obtain at the time of insurance application all the minimum information and confirming this information with the valid identification documents hereof from individual clients before establishing any business relationship.

For new Corporate and Juridical Entity, COCOLIFE shall obtain the minimum information and/or documents and authorized signatory/ies of corporate and juridical entities before establishing business relationships.

G. ENHANCED DUE DILIGENCE (EDD)

COCOLIFE shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions, which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Where the risks are higher, COCOLIFE shall conduct EDD.

The EDD shall be employed if the Sales Force (Marketing Personnel) and Underwriting Department acquires any of the following information:

- a. Raises doubt as to the accuracy of any information or document provided by the customer or the ownership of the entity;
- b. Justifies re-classification of the customer from low or normal risk to high-risk;
- c. When establishing business relationship with any person from countries identified by the FATF or AMLC as having on-going or substantial ML/TF risks;
- d. Warrants the filing of a suspicious Transaction Report (STR) exists, including information that:
 - 1. The customer is transacting without any purpose, economic justification, or underlying legal or trade obligation;
 - 2. The customer is transacting an amount that is not commensurate to the business or financial capacity of the customer or deviates from the profile of that customer;
 - 3. The customer might have structured transactions to avoid being the subject of a Covered Transaction Report;
 - 4. The customer has been or is currently engaged in any unlawful activity; or
 - 5. Raises suspicions that an intermediary is being used to circumvent anti money laundering compliance measures.

1. Enhanced Due Diligence (EDD) Measures

Whenever EDD is applied as required by this Guidelines, customer acceptance policy, or where the risk of ML/TF are higher, COCOLIFE shall do all the following, in addition to profiling of customers and monitoring their transactions:

- a. Gather documents to support the:
 1. Sources of wealth and fund;
 2. Nature of occupation and/or business;
 3. Reason for intended or performed transaction; and
 4. Other identification information, which COCOLIFE deems necessary to verify the identity of the customer, and their agents and beneficial owners.
- b. Conduct additional validation procedures, such as:
 1. Verifying volume of assets, information available through public databases, internet and other records;
 2. Verifying the declared residence address and conducting face-to-face contact with the customers, and their agents and beneficial owners; and
 3. Other modes of validation, which COCOLIFE deems reliable and practical.
- c. Secure the approval of senior management to commence or continue transacting with the customer;
- d. Conduct enhanced ongoing monitoring including more frequent or regular updating of identification information and identification documents;
- e. Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and
- f. Such other measures as COCOLIFE may deem reasonable or necessary.

H. CUSTOMER DUE DILIGENCE MEASURES ON BENEFICIARIES

COCOLIFE shall conduct the following Customer Due Diligence measures on beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiary or beneficiaries are identified or designated, for a beneficiary:

- a. That is identified as specifically named natural or legal persons or legal arrangements, taking the name of the person;
- b. That is a legal arrangement or designated by characteristics or by category such as spouse or children, at the time the insured event occurs or by other means such as under a will, obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the pay-out but before funds are disbursed.

In both cases, the identity of the beneficiary should be verified at the time of the payout. The beneficiary, if known, should be part of the risk factors on the basis of which the life insurer or intermediary will determine if the relationship is higher risk and enhanced due diligence measures should be applied.

I. RISK ASSESSMENT AND CUSTOMER RISK PROFILING

COCOLIFE shall assess customers and ensure that the minimum Customer Due Diligence requirement was met. For this purpose, COCOLIFE shall classify its customers into Low-Risk, Medium-Risk or High-Risk, and shall establish criteria in classifying its customers. The following criteria relating to the product or service, the customer and geographical location, may be taken into account:

1. The customer risk (e.g. resident or non-resident, type of customer, occasional or one-off, legal person structure, types of occupation, PEP classification);
2. The nature of the service or product to be availed of by the customers;
3. The delivery channels, including cash-based, face-to-face or non- face-to face, or cross-border movement of cash;
4. The purpose of the transaction;
5. The amount of funds to be transacted by a customer or the size of transactions undertaken or to be undertaken;
6. The regularity or duration of the transaction;
7. The fact that a customer came from a high-risk jurisdiction;
8. The existence of suspicious transaction indicators;
9. The source of fund and source of wealth;
10. Nature of business and/or employment;
11. Country of origin and residence of operations, or the fact that a customer came from a high-risk jurisdiction or geographical area;
12. Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by the IC, 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; and
13. Such other factors COCOLIFE may deem reasonable or necessary to consider in assessing the risk of a customer to ML and TF.

These factors considered individually may not be an indication of higher risk in all cases. However, a combination of them may warrant greater scrutiny.

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

COCOLIFE shall document the risk profiling results, as well as how a customer was profiled and the standard of CDD applied.

Copies of the Risk Classification of the Company and the Financial Risk Analysis are attached hereto as Annexes "A" and "B", respectively.

J. TARGETED FINANCIAL SANCTIONS (RELATED TO PROLIFERATION OF WEAPONS OF MASS DESTRUCTIONS AND PROLIFERATION FINANCING)

COCOLIFE shall implement Targeted Financial Sanctions (“TFS”) relating to proliferation of weapons of mass destructions and its financing against all funds and assets that are owned or controlled, directly or indirectly, including those derived or generated therefrom by individuals or entities designed and listed under United Nations Security Council (UNSC) Resolution Nos. 1718 (2006)a (concerning the Democratic People’s Republic of Korea) and 2231 (2015) (concerning the Islamic Republic of Iran) and their successor resolutions under the UNSC Consolidated List.

COCOLIFE shall comply with the directives of the AMLC or other related government agencies relating to proliferation of weapons of mass destructions, including, but not limited to, the following:

- a. freeze the properties or funds of designated persons or entities or those whose identities match with all the information in the Consolidated List (Target Match); and freeze or put on hold (for a period not exceeding 36 hours) property or funds owned or controlled by persons or entities whose identity matches most, but not all, of the identifier information in said list (Potential Target Match);
- b. submit a return to the AMLC within twenty-four (24) hours from effecting the TFS;
- c. prohibit from dealing with properties or funds of designated persons or entities;
- d. file suspicious transaction report (STR) for attempted transactions or dealings;
- e. immediately inform the AMLC of any temporary freeze or hold against a potential target match in addition to the filing of an STR; and
- f. permit addition to the accounts frozen of interest or other earnings due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the TFS, provided that any such interest, other earnings and payments continue to be frozen.

COCOLIFE shall file a detailed return to the AMLC in the following cases:

1. When there is a target match, i.e., the subject person or entity fully matches the description in the UNSC Consolidated List, file a detailed electronic return within 24 hours from effecting the freeze.
2. In cases where there is merely a potential target match, file a detailed electronic return within 24 hours from receipt of the AMLC’s confirmation.
3. 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, United Nations Security Council Resolution No. 1988, par.1(a), file the detailed electronic return within 24 hours from receipt of the AMLC Resolution to freeze.

In all of the above cases, the detailed electronic return shall specify the following information:

For covered persons:

1. The account number(s);
2. The name(s) of the account owner(s) or holder(s);
3. The time of freezing of all subject accounts;
4. The balance of the account as of the time of freezing;
5. The related accounts, if any, including the balance thereof as of the time of freezing; and
6. Explanation as to the ground for the identification of related accounts.

For relevant government agencies:

1. The nature and description of the property;
2. The name(s) of the owner(s) and/or holder(s) of the property;
3. The mode and date of acquisition of the property by the owner(s); and
4. The location of the property.

K. ONGOING MONITORING OF CUSTOMERS, ACCOUNTS AND TRANSACTIONS

On-going monitoring of customers, accounts, and transactions is an essential aspect of effective KYC procedures. The front-line staff members of COCOLIFE, including senior management who are directly in contact with high-net worth clients shall have an understanding of the normal and reasonable account activity of the clients. The process of on-going monitoring of accounts includes the following:

1. Customer information and identification documents should be kept up to date once every three (3) years in conformity with the Revised Implementing Rules and Regulation (RIRR). A risk-and-materiality based on-going monitoring of customer's accounts and transactions is to be part of customer due diligence.
2. Timely information like reports on critical customer data not obtained/disclosed despite diligent follow up, or such reports on clients with unusual activities that may lead to suspicious transactions shall be provided to the appropriate department and copy furnished the Compliance Officer/Coordinator who will analyze and effectively monitor high risk customer accounts.
3. Members of senior management who are in direct contact with high net worth/important clients shall endeavor to know the personal circumstances of these clients and be alert to sources of third party information. Unusual activities of these types of clients that may put COCOLIFE at risk shall be reported to the AMLC Committee.

L. ONGOING CDD AND MONITORING OF EXISTING CUSTOMERS

COCOLIFE shall, on the basis of materiality and risk, conduct ongoing monitoring by establishing a system that will enable it to understand the normal and reasonable

account or business activity of customers, and scrutinize transactions undertaken throughout the course of the business relationship to ensure that the customers' accounts, including transactions being conducted, are consistent with COCOLIFE's knowledge of its customer, their business and risk profile, including where necessary, the source of funds.

COCOLIFE shall apply EDD on the customer/client if it acquires information in the course of its customer account or transaction monitoring that:

1. Raises doubt as to the accuracy of any information or document provided or the ownership of the juridical person or legal arrangement;
2. Justifies reclassification of the customer from low or normal risk to high risk pursuant to this manual; or
3. Indicates that any of the circumstances for the filing of a suspicious transaction report exists such as but not limited to the following:
 - a. Transacting without any underlying legal or trade obligation, purpose or economic justification;
 - b. Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his Profile;
 - c. Structuring of transactions in order to avoid being the subject of covered transaction reporting; or
 - d. Knowing that a customer was or is engaged or engaging in any unlawful activity as herein defined.

If COCOLIFE fail to satisfactorily complete the enhanced due diligence procedures or reasonably believes that performing the enhanced due diligence process will tip-off the customer, it shall file a suspicious transaction report, and closely monitor the account and review the business relationship.

COCOLIFE shall, on the basis of materiality and risk, ensure that pertinent identification 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. COCOLIFE shall ensure that beneficial ownership information are updated in case of any changes. Updating of records shall be mandatory when enhanced ongoing monitoring process is warranted. COCOLIFE shall document the actions taken in connection with updating of customer's record/information, and accordingly update the customer's risk profile.

M. CUSTOMER VERIFICATION

COCOLIFE shall implement and maintain a system of verifying the true identity of their clients, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, document, data or information.

For customers that are juridical persons or legal arrangements, COCOLIFE shall maintain a system of understanding the nature of the customer's business or

profession, and ownership and control structure, as well as the authority and identification of all persons purporting to act on their behalf. They shall verify the customer's identity through the following information:

- a. Name, legal form and proof of existence;
- b. The powers and other legal requirements or contracts that regulate and bind the juridical person or legal arrangement, as well as the names of the relevant persons having a senior management position or perform significant responsibilities in the juridical person or legal arrangement; and
- c. The address of the registered office and, if different, a principal place of business.

N. ~~FACE-TO-FACE CONTACT~~ CONDUCT OF SALE

COCOLIFE shall conduct face to- face contact at the time of establishment of the business 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 ML and TF risks are effectively managed, taking into consideration risk and materiality. Provided further, that no transaction shall be processed without conducting a face-to- face contact.

The use of Information and Communication Technology in the conduct of face-to-face contact may be allowed, provided that the COCOLIFE is in possession of and has verified the identification documents submitted by the prospective customer prior to the interview and that the entire procedure is documented.

In case of remote selling and sale through electronic commerce, COCOLIFE shall establish guidelines to ensure that remote selling and electronic commerce initiatives are not utilized in cross-border selling. It shall adopt measures to ensure that no-cross border selling shall occur at the time of conduct of the sale. All remote selling and electronic commerce initiatives of COCOLIFE shall comply with the relevant rules and regulations and shall require prior of approval of the IC.

O. POLITICALLY EXPOSED PERSONS (PEPs)

In addition to establishing the true and full identities of PEPs, COCOLIFE shall also establish and record the true and full identities of the immediate family members (spouse or partner; children and their spouses; and parents and parents-in-law), close relationships/associates and entities related to them and entities if publicly known to be related to the PEP.

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

- a. Take reasonable measures to determine whether a customer, and his agent and the beneficial owner are PEPs; and

- b. In cases when there is a higher risk business relationship, adopt the following measures:
 - 1) Obtain senior management approval before establishing or, for existing customers, continuing, such business relationships;
 - 2) Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
 - 3) Conduct enhanced ongoing monitoring on that relationship.

In relation to foreign, in addition to performing the applicable customer due diligence measures, COCOLIFE shall:

- a. Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
- b. Obtain senior management approval before establishing (or continuing, for existing customers) such business relationship;
- c. Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- d. Conduct enhanced ongoing monitoring on that relationship.

COCOLIFE shall apply the abovementioned requirements to family members and close associates for all types of PEPs.

P. CUSTOMER ACCEPTANCE POLICY

COCOLIFE shall have clear, written and graduated acceptance policies and procedures that will seek to prevent suspicious individuals or entities from transacting with, establishing or maintaining business relationship with them.

COCOLIFE will not accept as customers or conduct transactions with persons or entities in the following circumstances:

- a. The customer has been identified by reliable sources as being a criminal or terrorist or being associated with criminal or groups;
- b. The customer is from a jurisdiction identified by reliable sources as one that has high levels of criminal or terrorist activity/ies;
- c. The customer is involved in certain criminal or such other activities (e.g. sale of illegal drugs) that are considered to be of high risk, given the nature of the source of funds;
- d. The customer is from a jurisdiction which has been identified as an area/country of high risk by the financial intelligence unit and/or the supervisory authority; and
- e. The employee has reason to believe, based on the behavior of the customer or other factors (e.g. refuse/failure to disclose source of funds), that the transaction may be related to money laundering or the financing of terrorism.

Q. CUSTOMER REFUSAL POLICY

If the prospective customer is unable to comply with any of the CDD measures, COCOLIFE shall refuse to commence business relations or perform the transaction. If circumstances warrant, COCOLIFE should file an STR in relation to the customer with the AMLC.

R. TIPPING-OFF POLICY

In case where COCOLIFE form a suspicion of ML/TF and associated unlawful activities and reasonably believes that performing the CDD process would tip off the customer, COCOLIFE is permitted not to pursue the CDD process. In such circumstances, COCOLIFE may proceed with the transaction, immediately file a Suspicious Transaction Report with the AMLC, closely monitor the account, and review the business relationship

S. INSTITUTIONAL RISK ASSESSMENT

COCOLIFE shall conduct an Institutional Risk Assessment (“IRA”) to assess its own risk areas. The IRA shall conducted at least one every two (2) years.

The processes in the conduct of the IRA shall include the following:

1. Risk Identification;
2. Risk Analysis/Evaluation;
3. Treatment of Risk;
4. Evaluation of Residual Risk; and
5. Reporting of Results, Monitoring and Reassessment.

T. RECRUITMENT PROCESS

COCOLIFE shall ensure that all employees employed or recruited have undergone standard recruitment process. It shall ensure that prospective employees have no negative findings from their previous employer and shall require them to undergo background checking via external training provider.

V. REPORTORIAL REQUIREMENTS

A. NOTIFICATION AND REPORTING OF SUSPECTED CRIMINAL ACTIVITIES

COCOLIFE has a system of reporting all covered transactions and has a manner of reporting of suspicious transactions to avoid tipping off. Any member of the management or the staff who discovers or suspects fraudulent or other criminal activity/ies, including terrorist financing, must contact the compliance officer and complete a suspicious transaction report.

Any member of the management or the staff who reports suspicion or is aware that an investigation is being, or may be, conducted must take particular care at all times to avoid committing a tipping-off offense, that is, informing the customer or other parties that a report of suspicion has been provided to the compliance officer.

B. DUTY TO REPORT TRANSACTIONS

COCOLIFE shall report to the AMLC all covered transactions within **five (5) working days** from the occurrence thereof, unless the AMLC prescribes a different period not exceeding fifteen (15) days. Suspicious transactions shall be promptly filed within the next working day from the occurrence thereof which shall be the date of establishment of suspicion or determination of the suspicious nature of the transaction.

1. Suspicious Transaction

It is the duty of every employee to report any suspicious transaction/s or activity/ies to the compliance officer. Reporting should be done using the reporting procedures set out in this section.

- a. Suspicious Transaction/s shall cover all transactions, whether completed or attempted.
- b. Employees encountering suspicious and/or high risk transactions should immediately report the same to compliance officer using the Suspicious Transactions Report Form. The form shall be noted by their respective department heads.

Note: No administrative, criminal or civil proceedings shall lie against the employee reporting the suspicious transaction in the regular performance of his duties and in good faith. Neither shall such report be treated as a breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

- c. All internal reports must reach the compliance officer and must not be blocked at the department level.
- d. When the compliance officer receives a suspicious transaction report, he or she will log it, allocate a reference number, and acknowledge it. He will then undertake sufficient inquiries to determine whether, in his judgment, the concerned transaction is suspicious.
- e. The compliance officer will review:
 - The application form/KYC and CDD and other information obtained from the customer;
 - Historical transaction patterns; and
 - Suspicious transaction reports, if any.
- f. The compliance officer will evaluate and determine if reasonable grounds exist to report the same as a suspicious transaction. If so, have it reported

by the reporting officer to the AMLC within ten (10) working days after initial detection of facts that may constitute a basis for filing such reports.

- g. The compliance officer may discuss the report with:
 - Senior Management or members of the board level committee; or
 - Board of Directors
- h. If reasonable grounds do not exist, the compliance officer should record an opinion to that effect on COCOLIFE's STR Form and return the same to the reporting officer.

2. Covered Transactions

- a. All covered transactions **over** P500,000 or where the total premiums/fees paid for a policy, plan or agreement for the entire year exceeds Php500,000.00 or its equivalent in any other currency are already being captured by the electronic reporting system mandated by the AMLC; reports are automatically and routinely reported electronically as a Covered Transaction Report (CTR) with the AMLC within ten working days of the occurrence thereof .
- b. Transactions confirmed as suspicious by the compliance officer are likewise reported electronically as they occur, with hard copy furnished to the AMLC, within ten (10) working days of the occurrence thereof.
- c. If a transaction is deemed to be both a covered and a suspicious transaction, it shall be reported by the reporting officer as a **suspicious transaction** as well. In this regard, it shall be reported first as a covered transaction, subject to updating if it is finally confirmed to be reportable as a suspicious transaction.
- d. The reporting officer shall follow the filing and reporting of CTRs in accordance with the AMLC Registration and Reporting Guidelines (ARRG) and any amendments thereto.
- e. The reporting officer shall maintain complete electronic files of all automatically covered transactions and manual files of all suspicious transactions reported to him/her, even if there is insufficient ground to report the same to the AMLC. Copies of CTRs and STRs shall likewise furnish the compliance officer through its designated AML secretary.

IMPORTANT NOTE: DO NOT WARN OR NOTIFY CUSTOMERS WHEN INFORMATION RELATING TO THEM IS BEING REPORTED TO THE AMLC. ALSO, DO NOT LEAK SUCH REPORT TO THE MEDIA OR ANY OTHER PERSON. ANY VIOLATION OF THIS CONFIDENTIALITY PROVISION IS SUBJECT TO CRIMINAL, CIVIL AND ADMINISTRATIVE SANCTIONS.

- f. The CTR and STR shall be submitted to the AMLC in a secured manner, in electronic form and in accordance with the ARR. COCOLIFE shall provide complete and accurate information of all the mandatory fields required in the report. In order to provide accurate information, COCOLIFE shall regularly update customer identification information at least once every **two (2) years**.
- g. Electronic copies of CTRs and STRs shall be preserved and safely stored for at least five (5) years from the dates the same were reported to the AMLC.

C. RECORD KEEPING

- a. All records shall be created and maintained for each individual and corporate applicant or policy owner.
- b. All records transaction records should be maintained by the responsible unit or department. Transaction documents may be retained as originals, on microfilm, in electronic form or in such other forms sufficient to permit reconstruction of individual transactions so as to provide admissible evidence in court.
- c. All records of **inactive** files shall be maintained and stored safely by the responsible unit or department for at least five (5) years from dates of final transactions (i.e, date of NTO, cancellation, lapse, surrender, death claim, maturity or termination, PDF or FBR termination).
- d. COCOLIFE shall comply with the Guidelines on the Digitization of Customer Records issued by the IC or the AMLC.
- e. When money is **received from overseas customers**, regardless of amount, accomplish Foreign Currency Form to record the following and submit the same to COCOLIFE Reporting Officer/Customer Care Head:
 - 1. Transaction serial number;
 - 2. Currency and amount involved;
 - 3. Date and time received;
 - 4. Instruction details, if any;
 - 5. Name, identification cards or passport numbers;
 - 6. Telephone numbers and address of contact person;
 - 7. Bank accounts involved; and
 - 8. Date and time of delivery and receipt number, if any.
- f. COCOLIFE's Customer Care Head/Reporting Officer shall be responsible and accountable for all record keeping requirements under this Manual. Said personnel will also be responsible for making records of customer identification and transaction documents readily available.

D. DOCUMENT RETENTION

COCOLIFE shall maintain and safely store for at least five (5) years from the dates of transactions all records of customer identification and transaction documents, or as long as the business relationship exists. If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5) year periods, until, it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

COCOLIFE shall also maintain and safely store for at least five (5) years from the dates the accounts were terminated, all records of customer identification and transaction documents. The ICREs shall likewise keep the electronic copies of all covered and suspicious transaction reports for at least five (5) years from the dates of submission to the AMLC.

E. RECORD OF INFORMATION ON COVERED AND SUSPICIOUS TRANSACTION REPORTS

COCOLIFE shall maintain records concerning its internal reporting of CTRs and STRs, and decision-making whether to file or not to file said reports with the AMLC, for at least a period of five (5) years after the date of transaction.

VI. ON-GOING TRAINING

- a. COCOLIFE's anti-money laundering policy and procedures shall be included in all orientation programs for newly hired employees, officers and directors and Fast Start, COP, BLIC and mutual fund training programs for the sales force.
- b. The education and training programs shall include the following topics:
 1. Overview on ML/TF, and the AMLA and TFPsA;
 2. Roles of directors, officers and employees in ML/TF prevention;
 3. Risk Management;
 4. Preventive measures;
 5. Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC
 6. Cooperation with the AMLC and the IC; and
 7. International standards and best practices.
- c. In addition, higher level training will also be provided to COCOLIFE's Compliance and Reporting Officers, Internal Auditors, Administration and Operations managers and supervisors responsible for complying with the AMLA procedures and requirements.
- d. Attendance by COCOLIFE's directors, officers and employees in all education and training programs, whether internally or externally organized, shall be documented. Copies of AML/CTF continuing education and training programs, training certificates, attendance and materials shall be made available to the IC and the AMLC, upon request.

A refresher training course shall also be conducted every two (2) years which may include inviting outside resource persons for this purpose.

- e. This Manual on Anti-Money Laundering shall be posted on the intranet to ensure that all employees and sales force are aware of the provisions of the Anti-Money Laundering Act and its implementing rules and regulations. Updated guidelines and Specific Responsibilities with regard to implementation on threshold amounts, verification of customers' identification, determining sources of funds and reporting procedures, etc. will be issued by e-mail and likewise posted on the intranet to ensure that all employees and sales force do not forget their reportorial and compliance responsibilities.
- f. In cases where there are new developments brought about by new legislations, rules and regulations, and other IC and/or AMLC issuances, COCOLIFE shall immediately cascade these information to its responsible directors, officers and employees through the intranet system.

VII. AMLA COMPLIANCE TEAM

The AMLA Compliance Team of COCOLIFE reports directly to the Board of Directors thru the Corporate Governance Committee. The AML Unit is responsible for overseeing, coordinating and managing the proper and efficient implementation of the COCOLIFE's MTPP following a risk based approach, which included the implementation of the KYC policies, record retention policies, system of timely capturing and reporting of covered transactions, investigation of suspicious alerts and reporting, if warranted, provide a customized AML training programs to employees and the conduct of independent AML compliance checking program by the Internal Audit and Risk Management and Compliance Departments.

The AMLA Compliance Team shall have the following main functions, among others:

1. Serious Case Analytics – analyzing and evaluating high profile cases, process the filing and non-filing of suspicious transaction reports and conduct AML due diligence based on a submitted enhanced due diligence of the Sales Force and Underwriting.
2. Policy Development & Training – updating the company's AML policies and procedures in compliance with AML/CFT Act and provide trainings to all employees.
3. Transaction Monitoring – monitoring the daily operation of the CIS Life AML Monitoring System for covered transactions and evaluation of suspicious transactions for reporting to the Anti-Money Laundering Council.

The AMLA Compliance Team shall be headed by the designated AMLA Compliance Officer of the Company.