MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM 2020

KASAGANA-KA
MUTUAL BENEFIT ASSOCIATION INC.
(Also known as KMBA)

KASAGANA-KA
MUTUAL BENEFIT ASSOCIATION INC.
(Also known as KMBA)

Money Laundering and Terrorism Financing Prevention Program (MTPP)

I. INTRODUCTION

The KASAGANA-KA MUTUAL BENEFIT ASSOCIATION, INC. (KMBA) is a non-stock, not-for-profit organization duly registered with the Securities and Exchange Commission ("SEC") and was granted the license to operate as a Mutual Benefit Association (MBA) by the Insurance Commission ("IC").

Pursuant to SEC Circular No. 12, Series of 2004 and IC Circular letter No. 32-2006, mandated all institutions including the MBA, where the SEC is vested by law the jurisdiction to regulate and supervise (the "Covered Institutions" or "Regulated Intermediaries"), to provide the basic and detailed framework of compliance with the Act.

This Operation's Manual on Money Laundering and Terrorism Financing Prevention Program ("MTTP Manual") aims to provide an appropriate framework and effective compliance policy for the MBA.

II. DESCRIPTION OF THE MONEY LAUNDERING

1. Money Laundering is a process intended to mask the benefits derived from serious offenses or criminal conduct as described under the Anti-Money Laundering Act, so that they appear to have originated from a legitimate source.

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

3. Money laundering is used also to hide the link between those who finance terrorism and those who commit terrorist acts.

4. Money laundering is also used to hide the link between those who finance terrorism and those who commit terrorist acts.

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

6. Generally, the process of money laundering comprises three stages, during which there maybe numerous transactions that could alert a regulated institution to the money laundering activity.

   a. **Placement** – the physical disposal of cash proceeds derived from illegal activity. The aim is to remove cash from the location of acquisition to avoid detection.

      Owing to the nature of insurance contracts or policies, payment of premiums as well as settlement of insurance claims, and all other forms of insurance transactions, are presently no longer predominantly cash based, thus covered institutions are less likely to be used in the placement stage than other financial institution.

   b. **Layering** – is the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy.

      The business of insurance is most likely to be used at the second stage of money laundering, the layering process, as they provide a potential avenue which may allow a dramatic alteration of the form of funds – from cash on hand to cash in bank, from money in whatever form to an entirely different asset such as securities, investment contracts, pension plans, insurance policies, stock certificates, pre-need plans, bearer and other negotiable instruments.

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

   c. **Integration** – the final stage is the process at which the money is integrated into the legitimate economic and financial systems and is assimilated with all other assets in the system. Integration of laundered money into the economy is accomplished by making it appear to have been legally earned. Thus, exceedingly difficult to distinguish between legal and illegal wealth.

      Insurance policies, particularly life insurance contracts, are treated not only as protection and savings instruments, but also as investment contracts and as such, insurance transactions incorporate added attraction to the launderer in that the alternative asset is normally highly liquid. The ability to liquidate investment portfolios containing both lawful and illicit proceeds, while concealing the criminal source of the latter, combined with the huge variety of investments and insurance products available, and the ease of transfer between them, offers the sophisticated criminal launderer an ideal route to effective integration into the legitimate economy. Due diligence

must therefore be exercised to prevent the use of insurance institutions as instruments of money laundering.

7. Due diligence, must therefore, be exercised to prevent the use of the Company as instrument for money laundering. The KMBA implements the following procedures to identify when it is being requested to "launder money".

   Member due diligence measures that shall be taken by the KMBA includes the following:

   a. Identifying the member and verifying the member's identity using reliable, independent source documents, data or information;
   b. Determining whether the member is acting on behalf of another person, and then taking reasonable steps to obtain sufficient identification data to verify the identity of that other person;
   c. Identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the KMBA is satisfied that it knows who the beneficial owner is. For legal persons and arrangements KMBA shall take reasonable measures to understand the ownership and control structure of the member;
   d. Obtaining information on the purpose and intended nature of the business relationship and other relevant factors;
   e. Conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the KMBA's knowledge of the member and/or beneficial owner, their business and risk profile, including, where necessary, the source of funds.

8. Any suspicion of such transactions should be communicated to the Compliance Officer. The following are some examples of suspicious transactions:

   a. Buying and selling with no discernible purpose or in circumstances which appear unusual;
   b. Instructions to credit benefit proceeds to an account different from that of the original source account or to a third party;
   c. Investors introduced by an overseas person, either of which are based in countries where production of drugs, drug trafficking, terrorism, or money laundering operations maybe present or prevalent;
   d. The use by a client of the SD/SB firm as a place to hold funds that are not being used to trade in securities;
   e. The entry of matching buys and sells in particular securities (wash sales) creating the illusion of trading. Such wash trading does not result in a bona fide market position and might provide a cover for a money launderer;
   f. Wash trading through multiple account maybe used to transfer funds through accounts by generating offsetting losses and profits in different

accounts. Transfer of positions between accounts that do not appear to be commonly controlled could also be a warning sign.

9. Tipping off refers to communicating, directly or indirectly, in any manner, or by any means, to any person, entity or media, including the customer himself, the fact an investigation is being contemplated or is being carried out.

   Employees are prohibited from disclosing to a client, or any other person or entity any information that has been passed to the Compliance Officer, to the management or to the regulatory authorities of anti-money laundering council which would likely prejudice its investigation on a suspicious transaction. To ensure confidentiality, a Non-Disclosure Agreement shall be executed by employees who are involved in the investigation.

10. Life insurance and non-life insurance including the MBA can be used in different ways by money launderers and terrorist financiers.

    a. Insurance Institution therefore shall take adequate measures to deter, detect and report money laundering and the financing of terrorism.

    b. The type of life insurance contracts that are vulnerable as vehicle for laundering money or terrorist financing are products, which includes: unit-linked single premium contracts, purchase of fixed and variable annuities, single provision life insurance policies that store cash value and (secondhand) endowment policies. Non-life money laundering or terrorist financing can be seen through inflated or totally bogus claims and through the use of reinsurance. An insurance policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins in the financial services sector.

III. BASIC PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING

The SEC and the IC seek to combat money laundering and financing of terrorism. KMBA places programs and systems which include the following:

1. "Know your Client" principle. The KMBA shall institute effective procedures for obtaining true identification of members. KMBA shall not keep anonymous accounts or accounts in obviously fictitious names and shall properly identify and record the true identity of its members when establishing business.

2. Compliance with laws. The KMBA management shall ensure that business is conducted in conformity with high ethical standards, laws and regulations are being adhered to and that the service is not provided where there is good reason to suspect that transactions are associated with money laundering activities.

3. Cooperation with AMLC and law enforcement agencies. Within the legal constraints relating to member confidentiality, KMBA shall cooperate fully with the Anti-Money Laundering Council, its Secretariat and law enforcement agencies and where there are reasonable grounds for suspecting money laundering, take appropriate measures which are consistent with the law.

   Disclosure of information by KMBA for the purposes of the Act regarding covered transaction reports and suspicious transaction reports shall be made to the General Manager, Anti-Money Laundering Council and Bangko Sentral Ng Pilipinas.

4. Dissemination of Policies and procedures. The policies and procedures to prevent and detect possible money laundering activities are properly disseminated to the Board of Trustees and management staff of KMBA which include its Compliance Officer registered with the SEC and/or IC.

   The extent and specific form of these measures may be determined following a risk analysis based upon relevant factors including the member, the business relationship and the transaction(s). Decisions taken on establishing relationships with higher risk members and/or beneficial owners shall be taken by the General Manager.

IV. Compliance Culture and Risk Ownership

1. The Compliance Office shall ensure that the Association is compliant to laws, rules and regulations related to money laundering and terrorism financing. This MTPP Manual shall serve as the internal policy of the Association describing its compliance culture specifically providing for the roles of the employees, the Officers, the Senior Management, and the Board of Trustees.

   Primary Roles of MTPP Key Persons:

   A. Board of Trustees
   - Ultimately responsible to the compliance on the law, rules and regulations on Money Laundering and Terrorism Financing.
   - Assess and set the Association's risk thresholds and appetite to inherent and potential risks on Money Laundering and Terrorism Financing.

   B. Senior Management
   - Establishes a culture of accountable and transparent management.
   - Have the oversight function on the daily initiatives against Money Laundering and Terrorism Financing activities.
   - Ensure that policies as provided in this MTPP Manual are in place.
   - Reports to the Board of Trustees Money Laundering and Terrorism Financing reports, updates and policies.

C. Compliance Officer

- Ensures that the Association has a sufficient, adequate, and well-maintained system that complies with the requirements of the latest AMLC reporting guidelines and current AML regulations and circulars for the accurate and efficient generation of alerts and reporting to the AMLC.
- Updates and ensure that all employees are well-trained and knowledgeable on regulatory related to ML TF

D. Internal Audit

- Ensures the effectiveness of the internal controls of the Association related to ML TF
- Periodically conducts compliance audit and assessment.

Three Lines of Defense

The three lines of defense of the Association are the following:

A. First Line of Defense – Business Unit Personnel

- Ensure compliance with this MTPP Manual.
- Ensure implementation of internal procedures for detecting and reporting suspicious transactions on its day-to-day transactions

B. Second Line of Defense – Compliance Office

- Monitors the Association's implementation of MTPP and compliance to related laws and regulations on money laundering and terrorism financing.
- Conducts review on AML compliance and provide recommendation thereof to the Senior Management and to the Board of Trustees.
- Inform the Senior Management on any red flags believed to be a non-compliance to this MTPP Manual and to laws and regulations related to money laundering and terrorism financing.
- Review Anti-Money Laundering alerts and reports covered transactions and suspicious transactions.

C. Third Line of Defense – Internal Audit

- An independent and adequately resourced audit shall be conducted to (a) evaluate the effectiveness of money laundering and terrorism financing risk management and controls.
- Reports to Audit Committee the result of its Compliance Audit

2. The Board of Trustees shall annually conduct Risk Assessment on money laundering and terrorism financing. The assessment shall be able to identify the following:

a. Inherent risk – the risk that is present in the Association's operations and management
b. Risk condition – the condition which specify if the risk is within the Association's appetite, limit or tolerance threshold.
c. Risk Controls – the existing internal controls at the present and its effectiveness
d. Residual Risk – the risk present despite existence of the controls.
e. Action Plan - the management action needed to address the residual risk.

The risk assessment shall result to the identification of the Association's risk indicators on money laundering and terrorism financing which shall be monitored by the Compliance Officer monthly and reported to Board of Trustees every quarter.

V. Client Due Diligence (CDD)

A. General

1. The Association shall strictly observe Client Due Diligence (CDD) to its clients or the beneficial owners of a company to which it transacts. It shall institute effective KYC procedures in identifying its clients and its service provider by securing its risk profiles.

2. As a regular part of the application process for insurance, KMBA shall obtain satisfactory evidence of the true and full identity of insurance applicants, which information include but not limited to:

   a. For individual policyholder, KMBA shall obtain the following minimum information:

      - Name;
      - Present address, with sketch map;
      - Permanent address, with sketch map;
      - Date and place of birth;
      - Nationality;
      - Nature of work and name of employer or nature of self-employment/business;
      - Contact number;
      - Tax identification number, SSS or GSIS number;
      - At least three specimen signature;
      - Source of fund(s);
      - Marriage contract, whenever applicable;
      - Birth certificates of covered/qualified dependents, whenever applicable
      - Names of beneficiaries, whenever applicable;
      - Proof of insurable interest, whenever applicable;

b. The members must provide photocopies of identifications and other applicable documents to KMBA and present the original documents for verification purposes, when deemed necessary. The acceptable identification cards, with specimen signature, are as follows:

- UMID
- SSS ID
- Passport
- TIN ID
- Company ID
- Postal ID
- Driver's License

c. While identification documents easily obtained in any name like, health or insurance cards, credit cards, provisional driving license and student identification cards may be used, the same shall not be accepted as the sole means of identification.

d. The names of beneficiaries, when applicable, to the insurance contract and the relationship to the policy owner.

- Duly notarized special authorizations for representatives.
- Other pertinent and reasonable documents as may be deemed necessary under the prevailing circumstances.

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

4. When KMBA acquires the business of another financial institutions or insurance institution, either in whole or as a product portfolio, it is not necessary for the identity of all existing members to be re-identified, provided that:

- All member account records are acquired with the business; and
- Due diligence inquiries do not raise any doubt as to whether the anti-money
- Laundering procedures previously adopted by the acquired business have satisfied AMLC requirements.

5. If during the business relationship, KMBA has reason to doubt:

a. The accuracy of the information relating to the member's identity;
b. The member as the beneficial owner;
c. The intermediaries' declaration of beneficial ownership, or
d. For reason of any sign of unreported changes, then KMBA shall take further measures to verify the identity of the member or the beneficial owner, when applicable. Such measures may include the following:

- Referral of names and other identifying information to criminal investigations authorities; and
- Review of disciplinary history and disclosure of past relevant sanctions.

5. Where the KMBA has already commenced the business relationship and is unable to comply with the verification requirements, it shall terminate the business relationships and consider making suspicious transaction report.

6. KMBA shall maintain accounts only in the true and full name of the account holder. It shall not open or keep anonymous accounts, fictitious name accounts, incorrect name accounts and all other similar accounts.

7. Verification without Face-to-Face Contact:

a. Whenever possible, prospective members shall be interviewed personally by an account officer or agent.

b. here may be cases where clients can open an account without going to the office but are well known to the Officer/Agent and he meets with them outside the office. In such cases, the accepting Investment Advisor/Agent/Consultant should sign the CAIF with the indication that he has conducted a face-to-face meeting with the client.

c. Customer identification procedures for non-face-to face verification is as the same as those for face-to-face verification. KMBA shall inform such clients that same measures shall apply to them.

d. The following are some counter checks being done by KMBA to verify identity of clients without face-to-face contact:

- Telephone contact with the applicant at an independently verified home or business number.
- Subject to the applicant's consent, telephone confirmation of the applicant's employment with the employer's personnel department at a listed business number.
- Submission of Income Tax Return duly stamped by BIR, and also bank statement or any proof of income and;

- Confirmation of the address through correspondence or presentation of proof of billing address like MERALCO bill, or any utility bill.

The above procedures should be strictly implemented when opening of accounts is coarsed via telephone, internet or by mail; especially if the client is just referred by another client or any of the staff. Such requirements should be done preferably prior to executing the initial transaction. If it cannot be avoided, ensure that above are conducted prior to the settlement of the client's initial transaction.

8. Customer identification and information of existing clients should be updated and/or amended at least once every five (5) years. This refers to change of residential or business address, new identification cards, new passport and additional business information. For any change of information before the said period, KMBA always request a letter or document pertaining to the changes being made.

9. No New Accounts shall be opened without face-to-face contact unless full compliance with the requirements of Section 6 is met and the original documents thereof are presented for verification purposes.

10. Bearing in mind the "know-your-customer" principle, KMBA should be in a position of no-doubt or no suspicions exist in our minds that the identities of our clients are questionable after a careful evaluation of all documents as enumerated in Section 7 are submitted to us and any other means used to come up with a satisfactory evidence on the identity of our clients. This should be all the more be very important where the client is not a Filipino and therefore more probing must be made on the purpose of the transaction and the sources of funds especially if it involves a significant amount, except, however, when such client is a long established and well-known customer

B. Corporation, Stock or Non-Stock and Partnership

1. Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company or its directors, or the business or its partners; a search or inquiry with the relevant Supervisory Authority/Regulatory Agency shall be made.

2. The following relevant documents shall be obtained in respect of corporate/other business applicants, which are subject to Philippine regulation.

   a. Copies of the Certificate of Registration, including Articles of Incorporation or Certificate of Partnership, as appropriate, copies of the By-laws and

Latest General Information Sheet, which list the names of directors/partners and principal stockholders and secondary licenses.

b. The name(s) and address(s) of the beneficial owner(s) and/or the person(s) or whose instructions the signatories on the account are empowered to act.

The originals or certified true copies of any or all of the foregoing documents, where required, shall be produced for verification.

c. Sworn statement as to existence or non-existence of beneficial owners.

d. Appropriate board resolutions and signed application forms authorizing the opening of the account or transaction together with the specimen signatures.

e. Where necessary, KMBA may also require additional information about the nature of the business of members, copies of identification documents of shareholders, directors, officers and all authorized signatories.

These requirements shall also apply in all cases involving holding companies.

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

C. Transactions with Shell Companies

1. Shell companies are legal entities, which have no business substance in their own right but through which financial transactions may be conducted. It is the policy of KMBA to be always cautious when dealing with these companies as these are often abused by money launderers. There must be a satisfactory evidence of the identities of the beneficial owners bearing in mind the "know-your-customer" principle.

D. Trustee Nominee and Agent Accounts

1. KMBA shall establish whether the applicant for insurance is acting on behalf of another person as trustee, nominee or agent. KMBA shall obtain satisfactory evidence of the identity of such agents and authorized signatories, and the nature of their trustee as nominee, capacity and duties.

2. Where the account is opened by a firm of lawyers or accountants, KMBA shall not be precluded from making reasonable inquiries about transactions passing through the subject accounts that give cause for concern or from reporting those transactions if any suspicion is aroused. If a Suspicious Transaction Report is made to the Council in respect of such members' accounts, the Council will seek information directly from the lawyers or accountants as to the identity of its

members and the nature of the relevant transaction, in accordance with the powers granted to it under the act and other pertinent laws.

VI. RECORD KEEPING

a. The KMBA shall prepare and maintain a record relative to its member relationships and transactions such that:
   - Requirements of the Act are fully met
   - Any transaction effected directly by KMBA can be reconstructed and from which the Council will be able to conduct an audit trail for suspected money laundering, when reports warrant the same.

b. KMBA can satisfy within a reasonable time any inquiry or order from the Council as to disclosure of information, including but not limited to whether a particular person is the member or beneficial owner of transactions.

2. The following document retention periods shall be followed:

   a. All documents and records of the policy holder, especially customer identification records, shall be maintained and safely stored for five (5) years from the dates of transactions.

   b. The documents, data or information collected under IC implementing rules process is kept up to date and relevant by undertaking reviews of existing records particularly for higher risk categories of members or business relationships.

   c. With respect to closed accounts, the records on member identification, account files and business correspondence, shall be preserved and safely stored for at least five (5) years from the date when they were closed.

   d. In case of long term insurance, records usually consist of full documentary evidence gathered by the KMBA or on the KMBA's behalf between entry and termination. If a member is terminated, responsibility for the integrity of such records rests with KMBA as product provider.

   e. KMBA, inclusive of agents or brokers shall follow the usual procedure and retain the records of those contracts which have been settled by maturity, claim or cancellation for a period of five (5) years after that settlement.

3. Transaction documents may be retained as originals or copies, on microfilms, or in electronic form, provided such forms are admissible in court, pursuant to the Revised Rules of Court and E-Commerce Act and its Guidelines.

4. if the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case had been closed.

VII. AUTOMATICALLY COVERED TRANSACTIONS AND SUSPICIOUS TRANSACTIONS

1. KMBA shall file before the Anti-Money Laundering Council, Covered Transaction Report (CTR) for all transaction in cash or other equivalent monetary instrument involving a total annual premium in excess of Five hundred thousand pesos (Php 500,000.00) (per AMLC Resolution No. 292, October 24, 2003) per day.

   The CTR in AMLA Form requires three (3) signatories from KMBA, to wit:

   a. The staff or officer who entertained or secured the account,
   b. The compliance officer, and
   c. A senior officer not less than the position of the Vice-President

   For online reporting thru electronic mail, it is the sole responsibility of the Compliance Officer to keep the report confidential and safe from public exposure.

2. As provided in the Act, the KMBA also file a Suspicious Transaction Report ("STR") before the Anti-Money Laundering Council, regardless of the amount involved, where any of the following circumstances exist:

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

   All covered transactions and suspicious transactions shall be reported by KMBA to the AMLC within ten (10) working days from occurrence thereof.

   Shall a transaction be determined to be both a covered transaction and a suspicious transaction, KMBA shall report the same as a suspicious transaction.

3. Any suspicious transaction, as a general principle, relates to any transaction wherein there is a feeling of apprehension or mistrust considering the unusual nature or circumstances of the transaction and the behavioral factors on the persons with whom the transaction is being dealt with and thereby bringing some suspicion that the transaction maybe connected with an unlawful activity. A list of examples of suspicious transactions is attached in Annex A hereof. The list is not exhaustive and it is left to the better judgment of KMBA to gauge the nature of each and every transaction that they would be involved in.

VIII. REPORTORIAL REQUIREMENTS

1. KMBA shall institute a system for the mandatory reporting of covered transactions and suspicious transactions by appointing the Compliance Officer who is registered with SEC, PSE and/or IC, who shall be responsible for reporting to the Council, after approval by the Board of Trustees. If an urgent disclosure is required when there is an on-going investigation, an initial notification by telephone should be made to the Executive Director, Anti-Money Laundering Council, Bangko Sentral ng Pilipinas.

2. Reporting of covered suspicious must be done by the Compliance Officer within five working days. Such reporting must be done within ten (10) working days after initial detection of facts that may constitute a basis for filing such reports.

3. Where reporting covered or suspicious transactions to the AMLC, KMBA and its 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 in form by the mass media, electronic mail, or other similar devices. In case of violation thereof, the concerned officer and employees of KMBA and media shall be held criminally liable.

4. Where any employee or personnel, director or officer of KMBA knows that the member has engaged in any of the unlawful activities under the Act, the matter must be promptly reported to the Compliance Officer within the Organization who, in turn, must immediately report the details to the Council.

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

5. KMBA shall maintain a complete file on all transactions that have been brought to the attention of the Compliance Officer, including transactions that are not reported to the Council.

6. Under Section 13 of the Act, where KMBA are required to disclose to an authorized officer knowledge, suspicion or belief that any fund, property or investment is derived from or used in any criminal conduct under the Act or any matter on which such knowledge, suspicion or belief is based, such disclosure shall not be treated as a breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct. Furthermore, under Section 13 of the Act, no administrative, criminal or civil proceedings shall lie against any person for having made a suspicious transaction report in the regular performance of his duties and in good faith, whether or not such reporting results in any criminal prosecution under this Act or any other Philippine law. KMBA, its directors and employees shall likewise not be liable for any loss, arising out of such disclosure, or any act or omission, in relation to the fund, property or investment consequence of the disclosure, where such is made in good faith and in the regular performance of their duties under the Act.

IX. INTERNAL CONTROL PROCEDURES

1. KMBA shall establish and implement internal control procedures aimed at preventing and impeding money laundering. Such procedures shall, among other things, ensure that KMBA and its employees are aware of the provisions of the law, its implementing rules and regulations, as well as all reportorial and compliance control and procedures that shall be established by the Council, the Supervising Authority and the KMBA itself.

2. KMBA shall issue a clear statement of policies in relation to money laundering, adopting the current regulatory requirements; this statement shall be communicated in writing to all management and relevant staff whether in branches, departments or subsidiaries and be reviewed on a regular basis.

3. KMBA shall see to it that its respective policies and procedures for dealing with money laundering and financing of terrorism reflecting the requirements under the Act and its implementing rules and regulations, are clearly set out and reflected in this Operating Manual.

4. Instruction Manuals shall set out the KMBA's policies and procedures for:
   a. selling insurance products including all types of bonds and contracts of suretyship
   b. member identification
   c. record keeping and maintenance
   d. acceptance and processing of insurance proposals

e. issuance of insurance policies
f. compliance with the requirements of the Act, and its revised implementing rules and regulations
g. cooperating with the Commission and other relevant authorities

5. KMBA shall establish written internal reporting procedures, which shall:
   a. Enable all its directors, officers, employees, all key staffs to know whom they shall
      report any knowledge or suspicion of money laundering activity.

   b. Ensure that there is a clear reporting chain under which suspicions of money laundering activity will be passed to the Compliance Officer, in accordance of reporting procedures of KMBA.

   c. Require the Compliance Officer to consider any report in the light of all relevant information available for the purpose of determining whether or not it gives rise to knowledge or suspicion of money laundering.

   d. Ensure that the Compliance Officer has reasonable access to any other information which may be of assistance in the determination as to whether or not suspicious transaction is to be filed.

   e. Require that upon determination of the suspicious nature of the report, the information contained therein.

   f. Maintain a record of all reports made to the Council, as well as all reports made by its own staff relative to covered and suspicious transactions, whether or not such were reported to the Council. Said register shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify relevant papers.

X. COMPLIANCE

1. KMBA shall appoint one or more senior persons, or an appropriate unit, to advise its management and staff on the issuance and enforcement of in-house instructions to promote adherence to the Act, its revised Implementing Rules and Regulations, its revised Operating Manual, including personnel training, reporting of covered and suspicious transactions, and generally, all matters relating to the prevention and detection of money laundering.

2. KMBA shall appoint a senior officer as the Compliance Officer. A compliance officer shall:

a. Be a senior officer with relevant qualifications and experience to enable him to respond sufficiently to inquiries relating to the relevant person and conduct of the KMBA's business.

He/She should at least:

- Be well versed in the different types of transaction which the KMBA handles and which may give rise to opportunities for money laundering;
- Has undergone an in depth training concerning relevant aspects of the AML Act, its revised IRR, and international standards
- Be responsible for establishing and maintaining a manual of compliance procedures in relation to the business of KMBA.
- Be responsible for ensuring compliance by the staff of KMBA with the provisions of the Act and its revised Implementing Rules and Regulations.
- Act as a liaison between KMBA and the Council in matters relating to compliance with the provisions of the Act and its revised implementing rules and regulations.
- Prepare and submit to the Council written reports on the KMBA's compliance with the provisions of the Act and its revised implementing rules and regulations, in such form and submitted at such time as the Council may determine.

XI. TRAINING OF STAFF

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

b. KMBA may, due to the scale and nature of its operations, assign the internal audit or training functions to another person (e.g. professional association, parent company or external auditors). Where KMBA delegates its responsibilities for audit and training, due to diligence is to be exercised to ensure that the person appointed are able to perform these functions effectively and the fact of such appointment must be relayed in writing to the Council.

c. Timing and content of training for various sectors of staff will be adopted by KMBA for its own needs. The recommended training programs are as follows:

   i. Provisions of the AMLA and the IRR
   ii. The KMBA's AMLA Manual
   iii. The KMBA's Internal Supervision, control and compliance procedures
   iv. The KMBA's Corporate Governance Manual
   v. Updates and changes on the AMLA
   vi. Updates and changes on Corporate Governance
   vii. Updates and changes on Internal Supervision, Control and compliance Procedures
   viii. Updates on BIR Regulations
   ix. Updates on PSE/SEC/IC Regulations

d. Refresher Training or orientations shall be made from time to time to constantly remind key staff of their responsibilities or if there are changes in the laws and rules in money laundering. A twelve- or six-monthly review of training or alternatively, a review of the instructions for recognizing and reporting covered transactions and suspicious money laundering transactions can be considered for the purpose.

XII. INTERNAL AUDIT

To test compliance with the KMBA's internal policies, procedures and controls, an audit function shall be in place. It is important that the audit function is independent and adequately resourced.

ANNEX "A"
COVERED TRANSACTION REPORT (CTR)

Who Must File.— Each covered institution must file SEC Form No. _____ (CTR) for each transaction by, through, or to the covered institution which involves a transaction in Philippine
currency or its equivalent in foreign currency of more than Php500,000.00. Multiple Transactions must be treated as a single transaction if the covered institution has knowledge that (1) they are by or on behalf of the same person, and (2) they result in currency received (Cash In) or currency disbursed (Cash Out) by the covered institution totaling more than Php500,000.00 in a series of transactions. A business day is a calendar day.

Identification Requirements. — This is important! All individuals conducting a reportable transaction(s) for themselves or for another person must be identified by means of an official document(s) from the covered institution as the person/s authorized to make such a report. In completing the CTR, the covered institution must indicate on the form the method, type, and number of the identification of the account holder or customer used in the transaction. Statements such as "known customer" or "signature card on file" are not sufficient for form completion.

When and Where To File.—File this CTR within five (5) days from which the transaction occurred to:

THE EXECUTIVE DIRECTOR
ANTI-MONEY LAUNDERING COUNCIL
BANGKO SENTRAL NG PILIPINAS
ROXAS BOULEVARD
PASAY CITY

Penalties.—Civil and criminal penalties are provided by the law for failure to file a CTR or to supply information or for filing a false or fraudulent CTR.

Specific Instructions

1. Because of the limited space of the CTR, it may be necessary to submit additional information on attached sheets. Submit this additional information on plain paper attached to the CTR. Be sure to put the covered institution's, individual's or organization's name and identifying number (e.g., items 2, 3, 4, and 6 of the CTR) on any additional sheets so that if it becomes separated, it may be associated with the CTR.

2. Amounts may be aggregated. The threshold limit for mandatory filing of a covered transaction report an amount in excess of Php500,000.00. This covers the following transactions:

    a. A single, series or combination of transactions a total amount in excess of Php500,000.00 or an equivalent in foreign currency based on the prevailing exchange rate where the client is not properly identified and/or the amount is

not commensurate with his business or financial capacity, or is without any underlying legal or trade obligation, purpose, origin or economic justification.

b. A single, series or combination or pattern of unusually large and complex transactions in excess of Php500,000.00 or an equivalent in foreign currency based on the prevailing exchange rate, especially cash deposits and investments having no credible purpose or origin, underlying trade obligation or contract.

3. Enter the full address of the covered institution where the transaction occurred. If there are multiple transactions, provide information on the office or branch where any one of the transactions has occurred.

4. The CTR shall be signed by the employee(s) who dealt directly with customer in the transaction and who made the initial internal report within the covered institution, the Compliance Officer of the covered institution, who made the necessary evaluation of the transaction and a senior official of the covered institution with a rank not lower than senior vice-president, who approved the filing of the CTR.

ANNEX " B"
SUSPICIOUS TRANSACTION REPORT (STR)

PART IV: Suspicious Transaction Information Explanation/Description

Explanation/description of known or suspected violation of law or suspicious transaction.

This section of the report is critical. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood. Provide below a chronological and complete account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account. If necessary, continue the narrative on a duplicate of this page.

a. Describe supporting documentation and retain for 5 years.
b. Explain who benefited, directly or indirectly, from the transaction, how much, and how.
c. Retain any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.
d. Retain any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.
e. Retain any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others.
f. Indicate where the possible violation took place (e.g., main office, branch, other).
g. Indicate whether the possible violation is an isolated incident or relates to other transactions.
h. Indicate whether there is any related litigation; if so, specify.
i. Recommend any further investigation that might assist law enforcement authorities.
j. Indicate whether any information has been excluded from this report; if so, why?
k. If you are correcting a previously filed report, describe the changes that are being made.
l. Indicate whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, letter of credit, domestic or international money order, stocks, bonds, traveler's checks, wire transfers sent or received, cash, etc.).
m. Indicate any account number that may be involved or affected.

Description of the Suspicious Transactions and Chronology of Events Leading to the Suspicion Using the Guidelines Enumerated Above

PART V: Suspicious Transaction Report Instructions

Safe Harbor Provisions of the Anti-Money Laundering Act of 2001, Republic Act No. 9169, under Section 9 © provides complete protection from criminal, civil and/or administrative liability for all reports of suspected or known criminal violations and suspicious activities to appropriate authorities, including supporting documentation.

Specifically, the law provides that a covered institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, shall not be liable to any person under any law or regulation of the Philippines

or any constitution, law, or regulation of any country or political subdivision thereof, for such disclosure or for any failure to notify the person involved in the transaction or any other person of such disclosure, when such reporting was done in good faith and in the regular performance of their duties and responsibilities under the Act.

The law further requires that a covered institution, and its directors, officers, employees and agents who, by means of a suspicious transaction report, report suspected or known criminal violations or suspicious activities may not notify any person involved in the transaction that the transaction has been reported. Any breach of this confidentiality provision shall render them criminally, civilly and administratively liable under the law.

In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the covered institution shall immediately notify, by telephone, appropriate law enforcement and covered institution supervisory authorities in addition to filing a timely suspicious transaction report.

WHEN TO MAKE A REPORT:

1. All covered institutions falling under Section 3 (a)(3) of the Anti-Money Laundering Act of 2001, Republic Act No. 9160 are required to make this report following the discovery of:

    a. Violations involving any amount. Whenever the covered institution detects any known or suspected violation of any the predicate crimes under the Act, or pattern of criminal violations, committed or attempted against the covered institution or involving a transaction or transactions conducted through the covered institution, where the covered institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the covered institution was used to facilitate a criminal transaction, and the covered institution has a substantial basis for identifying the suspect, which may include one of its directors, officers, employees, agents or other institution affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

    b. Violations aggregating PhP500,000.00 or more where a suspect can be identified. Whenever the covered institution detects any known or suspected predicate crime violation, or pattern of criminal violations, committed or attempted against the covered institution or involving a transaction or transactions conducted through the covered institution and involving or aggregating Php500,000.00 or more in funds or other assets, through one transaction or a series of transactions, where the covered institution reasonably believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the covered institution was used to facilitate a criminal transaction, and the covered institution has a

substantial basis for identifying a possible suspect or group of suspects, which may include one of its directors, officers, employees, agents or other institution-affiliated parties. If it is determined prior to filing this report that the identified suspect or group of suspects has used an alias, then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported.

c. A covered institution is required to file a suspicious transaction report no later than five (5) calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious transaction report. If no suspect was identified on the date of detection of the incident requiring the filing, a covered institution may delay filing a suspicious transaction report for an additional ten (10) calendar days to identify a suspect. In no case shall reporting be delayed more than twenty (20) calendar days after the date of initial detection of a reportable transaction.

HOW TO MAKE A REPORT:

1. Send each completed Suspicious Transaction Report to:

THE EXECUTIVE DIRECTOR
ANTI-MONEY LAUNDERING COUNCIL
BANGKO SENTRAL NG PILIPINAS
ROXAS BOULEVARD
PASAY CITY

2. For items that do not apply or for which information is not available, leave blank.
3. If more space is needed to report additional suspects, attach copies of PART IV to provide the additional information.
4. Identification Requirements for Persons Preparing and Making the Report. This is Important! All individuals conducting a reportable transaction(s) for themselves or for another person must be identified by means of an official document(s) from the covered institution as the person/s authorized to make such a report.

ANNEX "C"
EXAMPLES OF SUSPICIOUS TRANSACTION

The list of situations given below is intended mainly to highlight the basic ways in which money may be laundered. While each individual situation may not be sufficient to suggest that money laundering is taking place, a combination of such situations may be indicative of such a transaction. Further, the list is by no means complete or exhaustive and will require constant updating and adaptation to changing circumstance and new methods of laundering money. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

EXAMPLES OF SUSPICIOUS TRANSACTIONS:

I. Transactions Which Do not Make Economic Sense

2. Transactions not in keeping with the customer's normal activity, the financial markets in which the customer is active and the business which the customer operates.
3. Buying and selling of securities with no discernible purpose in circumstances which appear unusual.
3. Transactions not in keeping with normal practice in the market in which they relate, e.g., with reference to market size and frequency, or at off-market prices, early termination of products at a loss due to front end loading or early cancellation, especially where cash had been tendered and/or the refund check is to a third party.
4. Other transactions linked to the transaction in question which could be designed to disguise money and divert it to other forms or to other destinations or beneficiaries.
5. The entry of matching buys and sells in particular securities, wash sales, creating an illusion of trading. Such wash trading does not result in a bona fide market position and might provide "cover" for a money launderer.
6. Wash trading through multiple accounts of the same customer with the same or different broker(s) might be used

II. Transactions Involving Unidentified Parties

1. A personal customer for whom verification of identity proves unusually difficult and who is reluctant to provide details.
2. A corporate/trust customer where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.
3. Any transaction in which the counterparty to the transaction is unknown.
4. Settlement either by registration or delivery of securities to be made to an unverified third party.
5. Customers who wish to maintain a number of trustee or customers' accounts that do not appear consistent with their type of business, including transactions that involve nominee names.
6. A number of transactions by the same counterparty in small amounts relating to the same security, each purchased for cash, then sold in one transaction,

the proceeds being credited to an account different from the original account, the owner of which is unverified.

III. Suspicious Transactions Red Flags

a. Deviation from profile and/or past transactions
b. Structuring of transactions to avoid covered transaction reporting.
c. Amount involved not commensurate with the business or financial profile.
d. Client or beneficial owner is not properly identified.
e. Lack of underlying legal or trade obligation, purpose or economic justification.
f. Transaction is in any way related to an unlawful activity.

V. Miscellaneous

a. Large or unusual transactions in cash or bearer forms, remittances and transfers of funds.
b. The use of a customer of an intermediary to holds funds that are not being used to trade in securities.
c. A customer who deals with an intermediary only in cash or cash equivalents rather than through banking channels.
d. A customer who opens several accounts, in his own name or that of a nominee/s, trustee/s, agent/s, or dummy/ies, that do not appear to be consistent with their type of business.
e. The known background of the person conducting the transaction is not consistent with the transaction, and/or any unusual behavior in conducting the transaction;
f. The production of seemingly false identification in connection with any transaction, the use of aliases and a variety of different addresses;
g. A client with no discernible purpose for using the covered institution's service, where such service can easily be provided elsewhere with more convenience to