Anika
Insurance Brokers

Sdn Bhd

(8286-D)

Anti-Money Laundering (AML) Manual

(Based on the AML Act 2001 and
BNM's JPI/GPI 27 Guidelines)

Anika Insurance Brokers Sdn Bhd – AML Procedural Manual

Table of Contents

Table of Contents

Appendices

Appendix I – Examples of Suspicious Transactions

Guidelines on Anti-Money Laundering (AML) Measures for Anika Insurance Brokers Sdn Bhd (AIB)

1) Introduction

Money laundering encompasses all activities, procedures or processes undertaken to legitimise funds obtained through illegal or criminal activities and to hide the origins of the proceeds of a criminal activity. It is recognised as one of the most serious issues facing the international community.

The wide variety of services and investment avenues in the insurance industry provide opportunities to launder money. Being a service-oriented industry, it is also critical that the integrity, trust and confidence the public has in the insurance system are maintained and the system is not utilised as a platform to legitimise proceeds obtained from criminal activities.

In the bigger scheme of things, allowing money laundering activities to go undetected would bring dire social and economic consequences, besides eroding the fabric of integrity and confidence in the Malaysian financial system.

2) The AML Guidelines

The AML Guidelines apply to all insurers (including their agents) and brokers. Insurance licensees should observe, report and comply with the requirements of the Guidelines and should cooperate and harmonise their respective AML measures with regard to their respective roles and business operations, to ensure that a tight AML framework is instituted and enforced in the insurance industry.

The purpose of the AML guidelines is to provide an AML Framework to guide the insurance licensees to put in place a set of transparent, explicit and clear policies, procedures as well as controls to implement and enforce effective anti-money laundering measures.

3) Description of Money Laundering

Money laundering comprises a sophisticated, intricate and complex web of transactions that is aimed to disguise or change the source, form or origins of illegally or criminally derived funds by infiltrating any part of the economic and financial sectors within and across national boundaries to render such funds legitimate or moving the funds to a place where they are less likely to attract attention.

Money Laundering may be summarised in the following three stages:

a) Placement

In the initial or placement stage of money laundering, the criminal introduces his illegal profits and ill-gotten gains into the financial system. This is the physical disposal or dealing of the initial proceeds derived from illegal activities. Examples would include the payment of premiums for policies, including top-ups especially for single premium policies.

b) Layering

After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the criminal engages in a series of conversions or movements of the funds to distance them from their source. The illicit proceeds are separated from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide an appearance of legitimacy as well as anonymity. Examples would include borrowing against insurance policies, termination of policies and sale of units in investment-linked products.

c) Integration

When layering succeeds, the criminal proceeds have been successfully laundered, i.e. cleaned and are regarded for all intent and purposes as legitimate funds and are then reintroduced, i.e. integrated back into the financial system through investment in businesses, purchase of assets, etc.

4) Forms of Money Laundering in the Insurance Industry

In the insurance system, money launderers may structure transactions, coerce employees to cooperate and they do not file proper reports, or establish apparently legitimate "front" insurance entities to launder money.

Money launderers predominantly target the life insurance business. The most common form is the purchase of single premium investments such as annuities, lump sum top-ups to an existing life insurance contract and lump sum contributions to personal pension contracts.

For the general insurance business, money laundering can be seen through bogus claims, ie. money launderers purchase legitimate businesses, then by arson or other means cause bogus claims to recover part of their investment. Another form of money laundering in the general insurance business is by the use of one or more reinsurers owned by the money launderers.

5) AML Act 2001 and BNM as the Lead Agency

International initiatives against money laundering started more than a decade ago, culminating in 1989 with the setting up of the Financial Action Task Force on Money Laundering (FATF) established by the Group (F7) Summit in Paris to develop a co-coordinated international response. The first task of the FATF was to determine measures to deter and detect money laundering which resulted in the publication of the 40 Recommendations. The FATF's 40 Recommendations cover three areas – legal, financial and law enforcement. Recognising the importance to address the issues of money laundering and the effective measures in legal, financial, regulatory and law enforcement areas require cooperation amongst members in the international arena.

Malaysia in 2000 became a member of the Asia/Pacific Group (APG) on Money Laundering, established in February 1997 in Bangkok. At the domestic front, the National Co-ordination Committee to Counter Money Laundering (NCC) has been established in April 2000 with Bank Negara Malaysia (BNM) as the lead agency. This reflects BNM's important role in coordinating and enforcing systematic anti-money laundering measures and in preventing the financial system from being used to further criminal activities.

The Anti-Money Laundering (AML) Act 2001 was gazetted on 5 July 2001 and came into force on 15 January 2002.

6) The FIU Department within BNM

BNM has established a new department called the "Financial Intelligence Unit" (FIU) to enforce the AML Act 2001 and to cooperate with other countries in the global fight against money laundering and other serious crimes. As part of its mission to implement Malaysia's national AML programme to ensure that the insurance industry is not in any way compromised by criminal activities associated with money laundering, the AML Guidelines (JPI/GPI 27) was issued in April 2001.

The AML Act 2001 and the Guidelines will have a profound impact on the practice of insurance in Malaysia. It makes it mandatory for insurance licensees and its staff (including agents) to report specific detailed information about certain client-related financial transactions to the FIU. This mandatory reporting scheme is to assist in the prevention, detection and deterrence of money laundering, and to facilitate the investigation and prosecution of money laundering offences.

7) Terrorist Financing

The latest amendments to the AML Act and the Penal Codes now extend to cover terrorist financing. The legislative amendments have already been passed by the Parliament on 20 November 2003 and gazetted as law on 25 December 2003. The amendments were made in order for Malaysia to accede to the UN Convention for the Suppression of the Financing of Terrorism.

The new legal provisions effectively extend the AML mechanism to include:

(i) The reporting of suspected terrorism financing activities.
(ii) Measures for the detection and prevention of terrorism financing.
(iii) Freeze, seize and forfeiture of terrorist property.

The above legislative measures as well as the revised FATF 40 Recommendations would translate into expansions to and the requirement of higher standards in the AML measures undertaken by the insurance licensees. The Guidelines call for high standards of vigilant care in the identification and verification of the licensee's clients as well as the identification of suspicious transactions. Business relations should not commence or should be terminated if the recommended measures could not be complied with.

8) Key AML Principles and a Duty of Vigilance

Money laundering is a major and serious threat to the good functioning of the insurance industry. The good name and public confidence of the insurance licensees may also be undermined or eroded if their entities are associated with laundering funds derived from crimes. As such, licensees should be constantly vigilant to deter criminals from making use of the insurance system for laundering ill-gotten money.

The insurance licensee's duty of vigilance, practiced and maintained in the form of its AML programme, should encompass the following key elements:

(i) Determining (or receiving confirmation of) the true identity of the prospective policy owners;

(ii) Keeping of records and the retention period;

(iii) Recognising and reporting of suspicious transactions to the relevant authority;

(iv) Establishing a system of procedures, controls and reporting system which includes designating a Compliance Officer who is responsible for the day-to-day compliance with current regulations;

(v) Training of staff, including intermediaries and agents, wherever located;

(vi) Assuring compliance with the relevant regulations by establishing a system of internal controls;

(vii) Liaise closely and cooperate with the relevant authorities on matters relating to vigilance policy and systems;

(viii) Ensuring that the internal audit and compliance departments regularly monitor the implementation and operation of vigilance systems;

(ix) Establishing high standards in all businesses and requiring compliance with laws and regulations; and

(x) Drawing up manuals detailing the whole due diligence duty of vigilance in terms of all policies and procedures to ensure the effective implementation of the licensee's AML measures.

9) AIB's AML Procedural Manual (Incorporating the AML Framework)

The AML Framework

The AML Framework aims to provide a set of transparent, explicit and clear policies, procedures and controls to guide the insurance licensees to implement and enforce effective AML measures.

The licensee should view these measures as **complementing** and **assisting** their business operations to secure a base of genuine policy owners and meet their policy owners' insurance needs as well as generate a long-term, sound and reputable insurance business.

AIB's AML Manual

AIB's AML manual aims to incorporate the prescribed AML Framework, while maintaining a duty of vigilance, into its AML manual and the accompanying set of procedures in carrying out its insurance broking business.

The Anti-Money Laundering Act 2001 (including any subsequent legislative amendments and extensions), together with BNM's JPI/GPI 27, should be the referencing sources and used in conjunction with the practice and application of this AML manual.

Anika
Insurance Brokers
Sdn Bhd
(8286-D)

ANIKA INSURANCE BROKERS SDN BHD'S CORPORATE POLICY ON ANTI-MONEY LAUNDERING MEASURES

Anika Insurance Brokers Sdn Bhd is fully committed to the fight in preventing its business operations from being used as an avenue for money laundering activities.

Anika will ensure it is in full compliance with the Anti-Money Laundering (AML) Act 2001 and Bank Negara Malaysia's Guidelines and Directives on AML measures.

COMPLIANCE POLICIES, PROCEDURES AND CONTROLS

1.0 Verification of Clients

We should verify and be satisfied with the identity of our customers and the nature and legitimacy of the insurance transactions to be undertaken. Verification is a cumulative process, which generally does not rely on any single piece of documentary evidence. The best possible evidence could mean that which is the most difficult to replicate or acquire lawfully because of its reputable and/or official origin.

We should maintain the '**Know Your Customer**' policy which is a critical precondition to recognise a suspicious or unusual transaction. This will aid the insurance licensees in their verification of potential insurance contracts and the financial flows and transaction patterns of existing policy owners.

1.1 Verification

- Before any policy is contracted, the identity and legitimacy of every verification subject relevant to the application for insurance business must be verified.

- Verification should be carried out primarily in respect of the parties entering into the insurance contract, any underlying principals that the policyholders are acting on behalf, and all the joint applications to the insurance contract. When there are underlying principals to any transaction, the true nature of the relationship between the principals and the policyholders should be established and appropriate enquiries performed on the former, especially if the policyholders are accustomed to act on their instruction (e.g. group policy).

- Where there are a large number of verification subjects (e.g. group policy) it may be sufficient to carry out verification on a limited group only, such as principal shareholders, the main directors of a company, etc.

- Where there are arrangements such as trust, nominee companies and fronting companies, verification should include an assessment of the substance of the arrangement, e.g. at the settlers, trustees and beneficiaries.

- If claims, commissions, and other monies are to be paid to persons (including partnership, companies etc) other than the policy holder then the proposed recipients of these monies should be the subject of verification.

- Any reinsurance on retrocession needs to be checked to ensure the monies are paid out to bona fide reinsurers for rates that commensurate with the risks underwritten.

- If it is necessary for sound business reasons to enter into an insurance contract before completion of verification, this shall be subject to stringent controls which shall ensure that any funds received are not passed to third parties. Alternatively, a senior officer of the company may give appropriate authority to proceed with the transactions. Any such decision shall be properly documented in the customer file.

1.2 Verification evidence:-

1.2.1 Individual

i) personal information should include:
   (a) full and correct name(s)
   (b) date and place of birth
   (c) nationality
   (d) current permanent address
   (e) telephone number, fax number and e-mail address
   (f) occupation and name of employer (if self-employed, the nature of the self-employment)
   (g) specimen signature of the verification subject.

ii) Some documents that may be considered the best possible to verify the above particulars of the individual are:
   (a) current valid passport; or
   (b) national registration identity card; or
   (c) armed forces identity card; or
   (d) driving licence which bears a photograph.

iii) Other documents that may be considered with some degree of care for the purpose of verification are birth certificates, an identity card issued by the employer of the application and credit cards (only if those listed in (ii) above are not available for any valid or reasonable reasons).

1.2.2 Corporate Client (including partnerships, clubs, societies & charities)

Certified copy of the:-

i) Certificate of incorporation or partnership agreement or other agreement establishing the unincorporated business.

ii) Memorandum and Articles of Association.

iii) Location of the registered office or agent.

iv) Resolution of the Board of Directors authorizing the person to contract the insurance business on the company's behalf.

v) Confirmation that the company has been struck off the register or is not in the progress or is not in the progress of being wound up.

vi) Names and addresses of all officers and directors.

vii) Names and addresses of all beneficial owners.

viii) Description and nature of the business including date of commencement of business.

ix) Products or services provided and location of principal business.

x) Purpose of the insurance contract.

xi) Source of funds.

xii) Nature of transaction.

xiii) Latest report and accounts.

xiv) Other official document and other information as is reasonably capable of establishing the structural information of the corporate entity.

1.2.3 Group Life and Pension Schemes

i) The principal shareholders and the main directors of the company or organisation.
ii) Beneficiaries, where they are not the policy owner.

1.3 Cases Exempted from Verification

Even though the following cases are exempted from verification, we must continually be vigilant and be guided by the fact where it knows or has reason to believe or suspect that money is being laundered, or that money laundering is, may or has occurred, the exemptions below are no longer applicable.

Examples of cases that can be exempted from verification are, as follows:-

- Where it is a switch and all the proceeds of a significant one-off transaction are paid directly into another insurance policy which in itself can, on subsequent surrender, only result in either:-

  (i) A further premium payment on behalf of the same customer.
  (ii) A payment being made directly to the customer and of which a record is kept.

- Where payments of one policy are used to fund premiums payable in another policy for the same customer. This is not regarded as entry into a business relationship, and as such do not require verification.

- Where third party evidence is required to support the exemption. Here, the introducer of the customer is a reliable party and submits a written introduction. This introducer may be:-

  (i) A reliable local institution, which is subsequently verified by the insurance entity and supplemented by appropriate enquiries, where necessary.
  (ii) A professional qualified person or an independent financial adviser operating from an acceptable jurisdiction, and whereby the insurance licensee is satisfied that the rules of his/her professional body regulator include ethical guidelines which together with the money laundering laws and regulations in his/her jurisdiction include requirements at least equivalent to those in the Guidelines.
  (iii) Where the introducer is reliable and has good standing introduction.
  (iv) Where the introducer is either an overseas branch or member of the same group as the receiving insurance licensee.

Details of the introduction should be kept as part of the records of the customer introduced.

A critical condition for the acceptability of such an introducer is that the terms of business between AIB and the introducer should require the introducer to complete verification of all customers introduced to AIB or to inform AIB of any unsatisfactory conclusion in respect of any such customer, to keep records in accordance with the Guidelines and to supply copies of any such records to AIB upon demand.

Where AIB is dissatisfied with any of the above conditions for the introducer, we should conduct its own verification of the customer and not regard it as an exempt case.

1.3.1 Where Third party Evidence is Not Required to Support the Exemption

- Where the customer is a licensed and/or supervised financial institution.

- Where there are small one-off applications, unless between entry and termination it appears that two or more one-off transactions are in fact linked and constitute a significant one-off transaction. In the absence of any contrary evidence, a period of **three months** or more of separation between one-off transactions are deemed as not linked.

- Where payments are made through post, credit card or electronically such as through the Internet, and such mode of payment is regarded reasonable, and where payment is from the customer's account held in another institution which is registered/ authorised/ exempt under local insurance (and banking) laws, the name(s) of the customer for business corresponds with the name(s) of the paying account holder, the receiving insurance licensee keeps a record of the customer's account with that other institution and there is no suspicion of money laundering. In such cases, it may be assumed that the other institution has completed the necessary verification.

1.4 Results of Verification

- Once verification has been completed (and subject to the records keeping requirements stipulated in this manual) no further evidence of identity is needed when transactions are subsequently undertaken. The file of each applicant for business should show the steps taken and the evidence obtained in the process of verification, or in appropriate cases, details of the reasons which justify the case.

- In the event of failure to complete verification of any verification subject and where there are no reasonable grounds for suspicion, any business relationship with or one-off transaction for the applicant for business should be suspended and any funds held to the applicant's order returned until verification is subsequently completed (if at all). Funds should never be returned to a third party but only to the source from where they came.

- If failure to complete verification itself raises suspicion, a report should be made and guidance sought from BNM or other law enforcement authorities as to how to proceed further.

2.0 Record Keeping

The company is required to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering. We should keep all the necessary records pertaining to its policy owners and their insurance transactions.

We should ensure that, minimally, they have adequate procedures and records to access:

i) The initial proposal documentation including, where completed the customer's financial assessment;
ii) The customer's needs analysis;
iii) Copies of regulatory documentation;
iv) Details of the payment method;
v) Illustration of benefits;
vi) Copy of documentation in support of verification by insurance licensees.
vii) All post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; AND
viii) Details of the maturing processing and/or claims settlement, including completed "discharge documentation".

2.1 The Records should have:-

- A description of the nature of all the evidence received relating to the identity of the verification subject or information on sourcing or on how to obtain a copy if the evidence itself or a copy of it is not readily available.

- The details of personal identity, including the names and addresses of the policy owner and any other parties connected to the insurance contract.

- The details of the transaction should also be recorded and should include the nature of the transactions, contract price(s) and valuation (for unit-linked policies), destination(s) of funds, memoranda of instruction(s) and authority(ies), book entries, the date of the transaction and the form (e.g. cash, cheque, etc.) in which premiums are paid.

- Especially in the case of long-term insurance, records should consist of full documentary evidence gathered by the insurance licensee between entry and termination of the policy. If there are terminations of policies, the record should include the maturity and any termination of a policy.

2.2 All Records Should Be Kept Properly

- Staffs are advised to maintain each client's information separately in one unique file as well as by each department.

- All relevant records are to be kept in readily retrievable forms and be accessible with ease. The records may be retained by way of original document, stored on microform, or as electronic data.

- Any records kept by third parties are regarded as readily retrievable only if AIB is reasonably satisfied that the third party is able and willing to keep such records and to disclose them when required.

- Maintain a separate register of all enquiries made to it by any law enforcement authority or their foreign equivalent. The minimum details of the register are the date and nature of the enquiry, the name and agency of the enquiring office, the powers being exercised and the details of the policies involved.

- The following data should be kept for a period of not less than **seven (7) years**:-

  i) Customer records, from the date the transaction has been terminated, whether due to early termination, surrender or expiry of a policy.

  ii) The account ledger records, from the date of entering the transaction into the ledger.

  iii) Records in support of entries in the accounts in whatever form they are used, eg. credit/debit notes/slips and cheques and other forms of vouchers, from when the records were created.

3.0 Recognition and the Reporting of Suspicious Customers / Transactions

To facilitate the recognition of suspicious customers/transactions, it is vital that AIB minimally observe the "Know Your Customer" principle, including sourcing relevant information about a customer's economic/financial background.

With a profile of the customer established, it will also facilitate AIB to vigilantly monitor the financial flows and transaction patterns of existing policy owners, particularly where there is a significant, unexpected and unexplained change in the behaviour of an account.

In determining a case of the possibility of money laundering and of criminal conduct, it is also more than the absence of certainty that some one is innocent, but rather an inclination to believe that for reasons that can be identified, there has been a criminal conduct. There is also an absence of factual information to negate any suspicious. "Suspicious" could also mean unusual in the context of that particular customer's profile.

3.1 The Three Separate Steps to be Taken in Deciding Whether a Suspicious Transaction Must be Reported:-

3.1.1 Step 1 – Do you engage in any of the activities that trigger reporting obligations?

- Only when staff member engage in the following specified activities on behalf of or for a customer, or when the staff member give instructions in relation to these activities, are their obligations to report suspicious transactions triggered:

  (i) Receiving premiums or paying claims, other than those received from or paid to policy holder/beneficiary.

  (ii) Consistently high activity levels of single premium business far in excess of any average company expectations.

  (iii) Unclear source of funds or inconsistent with client's apparent standing.

  (iv) Client reluctant to provide information to enable verification on insurance interest.

3.1.2 Step 2 – Has the transaction completed or still in its initial stage of business?

- The effort to recognise suspicious circumstances should commence with the request for insurance policy or when executing the initial transaction. The requirement to report a suspicious transaction applies not only to a completed transaction.

  Even during the initial stage of the business, or if the client, the staff member or the company, decides not to complete the transaction, there is still **obligation to report**.

- Note that in the context of dealing with the triggering activities the word "transaction" is used in both a specific and a general manner. It refers to both the specific triggering activity of receiving or paying funds, transferring funds, etc., and to the more general activity of completing a transaction on a specific matter for a client. Thus, there could be two or more reportable "transactions" in any matter that you handle for a particular customer.

  In this case, there would be multiple reportable transactions on a single customer matter, each of which would have to be detailed in separate pages or parts of a single suspicious transactions report for that particular matter.

3.1.3 Step 3 – Is the transaction "suspicious"?

- The more difficult question to answer is whether the transaction is "suspicious" within the meaning of legislation. Answering this question is dealt with in the following points.

- A "suspicious transaction" can involve any sum of money while a "threshold transaction" occurs when the significant one-off cash transactions exceed the prescribed threshold of RM10,000 (please refer to the specific section below for more details).

- A suspicious transaction may involve several factors that may seem individually insignificant, but together may raise suspicion that the transaction is related to the commission of a money laundering offence. To identify a suspicious transaction, all circumstances surrounding the transaction need to be considered.

- The company shall be alert to the implications of financial flows and transaction patterns of existing policyholders, particularly if there is a significant, unexpected and unexplained change in the behavior of the policyholders' accounts, such as borrowing against the policy, early surrender, etc.

3.2 The Assessment of Whether a Transaction is Suspicious

3.2.1 Against some patterns of legitimate business, suspicious transactions should be recognisable as falling into one or more of the following categories:-

- Any unusual financial activity of the customer in the context of his own usual activities.
- Any unusual transaction in the course of some usual financial activity.
- Any unusually-linked transactions.
- Any unusual or disadvantageous early redemption of an insurance policy.
- Any unusual employment of an intermediary in the course of some usual transaction or financial activity, eg. payment of claims or high commission to an unusual intermediary.
- Any unusual method of payment.

3.2.2 The company staff, reviewing all information about a potentially suspicious transaction must consider:

- What a money laundering offence is.
- Whether a suspicion is reasonably based.
- The General and Specific Indicators of suspicious transactions compiled by BNM (please refer to Appendix I for the indicators and examples).

3.3 Recognition

Transactions may give rise to reasonable grounds to suspect that they are related to money laundering regardless of the sum of money involved. **There is no monetary threshold for making a report on a suspicious transaction**. A suspicious transaction may involve several factors that may seem individually insignificant, but together may raise suspicion that the transaction is related to the commission of a money laundering offence. As a general guide, a transaction may be connected to money laundering when you think that it (or a group of transactions) raises questions or gives rise to discomfort apprehension or mistrust.

The context in which the transaction occurs is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. As a reporting person or entity, or a staff of a reporting person or entity, you should evaluate transactions in terms of what seems appropriate and is within normal practices in your particular line or class of business. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering.

An assessment of suspicion should be based on a reasonable evaluation of relevant facts, including the knowledge of the customer's business, financial history, background, behavior and pattern of transaction. Also, it could be the consideration of many factors – not just one factor – that will lead you to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission of a money laundering offence. All circumstances surrounding a transaction should be reviewed.

Specific examples of suspicious transactions are listed in Appendix I. These examples are not intended to be exhaustive. The list however provides some examples and guide on some of the ways in which money can be laundered in the insurance industry.

3.4 Reporting of Suspicious Customers/Transactions

3.4.1 AIB's Reporting Guide and Procedures

- All transactions that are regarded by a staff as suspicious must be reported immediately to the Departmental Head within 24 hours. A written memo that sets out the facts and circumstances that lead to the conclusion the transaction was suspicious must be prepared together to the Departmental Head.

- Departmental Head must report immediately to the Compliance Officer within 24 hours after receiving the memo.

- The Compliance Officer and the responsible manager will review any memo from the responsible staff member who prepared it.

- The Compliance Officer, to whom all cases of suspicious transactions are reported to, is in turn responsible to report such transactions to the FIU in BNM within 48 hours after receiving the written memo.

- The Compliance Officer is required to report immediately any suspicious transactions to FIU using the reporting form in Appendix II. In the event that urgent disclosure is required, especially where the suspicious transaction is related to an on-going investigation, an initial notification should be made by fax/phone to FIU or any other person designated by him.

FINANCIAL INTELLIGENCE UNIT (FIU)
BANK NEGARA MALAYSIA
JALAN DATO' ONN
50480 KUALA LUMPUR

Tel: 03 - 2698 8044 (ext 8071 / 7376)
Fax: 03 - 2693 3625

BNM's website: http://www.bnm.gov.my/

- To ensure that the Board of Directors (BOD) and the Senior Management team are kept fully informed of any attempts to use AIB as an avenue to launder money which may undermine its soundness and integrity, the Compliance Officer should inform the BOD and the Senior Management team immediately via memo or e-mail. Further discussions will be carried out in the next scheduled BOD Meeting and monthly Management Meeting.

- For such cases reported from the branches, the staff should report to the branch head within 24 hours with the similar necessary factual memo and the latter in turn to immediately inform the Compliance Officer at the KL Head Office within 24 hours.

- The respective department shall maintain a complete file on all transactions that have been reported to the Compliance Officer, including any transactions that are not reported to BNM.

- However, any information or details relating to the facts surrounding the suspicions triggered or the report made to the FIU or any other law enforcement agencies (including the acknowledgement of receipt of the report made) should not be kept in the customer's file. Instead, the information and documents/reports should be separately retained in a classified AML compliance or report file.

- Where a further investigation of the customer is required following the reporting of a suspicious transaction to BNM, care should be taken to ensure that the customer is not aware that such a report has been made to BNM, or any other law enforcement agencies so as not to jeopardise any further investigation attempts (please refer to the "prohibition on disclosure" and 'tipping-off' sections below for more details on this).

3.5 Organisational Chain of Implementation, Roles and Responsibilities

3.5.1 Roles of Compliance Officer, Responsible Manager and Staff/Agent

- The Compliance Officer should be familiar with the different types of transaction which the insurance licensee handles and which may give rise to opportunities for money laundering.

- The Compliance Officer should also be a source of reference and information and be able to advise the reporting personnel whether a particular case is a suspicious transaction.

- The Compliance Officer, the responsible manager and any staff member working on matter that involves a potentially reportable transaction will be involved in the process of determining, upon advice of senior management, whether a suspicious transaction report must be completed.

- The Compliance Officer, the responsible manager and staff member have primary responsibility for determining whether a particular transaction is suspicious and needs to be reported. Therefore, if any staff member becomes aware of information about a possible suspicious transaction, then that staff member must communicate that information to the respective manager, who will in turn report it to the Compliance Officer.

3.6 Penalties for Non-Compliance with the Obligations to Report a Suspicious Transaction and Other Major Requirements of the AML Guidelines

The penalties for the licensee, its BOD members and management personnel as well as the staff member failing to meet the suspicious transaction reporting and other compliance obligations are very serious.

3.6.1 Penalties and Specific Actions

The AML Act 2001 provides for the following specific penalties and enforcement actions to be taken against the above parties for non-compliance (without any just or reasonable excuse) with the AML Guidelines or other obligatory requirements:

i) BNM is empowered to take the necessary actions to prevent or avoid having any person who is unsuitable from controlling, or participating, directly or indirectly, in the directorship, management or operation of the licensee;
ii) BNM is also empowered to revoke or suspend the licensee's licence;
iii) A court order may be obtained against any or all of the officers or employees of the licensee to forcibly enforce satisfactory compliance with such obligations;
iv) Any person within the licensee company may also be liable, upon conviction, to a fine up to RM100,000 and/or to imprisonment for a term up to six (6) months, with provisions for further fines for a continuing offence.

3.6.2 Immunity and Protection of Persons Reporting

In general, a responsible staff member who has met the AML Guidelines and Obligations, in particular the prompt and proper reporting of any suspicious transactions in good faith according to the prescribed procedures and requirements, are immune from the relevant disciplinary proceedings, including any civil or criminal liabilities.

S24 of the AML Act 2001 provides for such a protection for any reporting person, unless the information supplied or the reporting was disclosed or supplied in bad faith. S24 further states that, "*In proceedings against any person for an offence under [the Act], it shall be defence for that person to show that he took all reasonable steps and exercised all due diligence to avoid committing the offence.*"

3.6.3 Restriction on Revealing Disclosure of A Suspicious Transaction Reporting

The staff members or any officers of the licensee are prohibited from informing or revealing any information or details of a suspicious transaction report to anyone, including the client or suspect parties, or even the fact that a report has been or will be made. This is to ensure the investigation is not jeopardised, harmed or impaired. This prohibition applies whether or not a criminal investigation has begun.

S6 of the AML Act 2001 provides for the specifics to the restrictions mentioned above, as well as the possible penalties that may ensue following a breach to the Act.

3.6.4 Tipping-off

It is an offence for anyone who knows, suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting, or are proposing to act, in connection with an investigation into money laundering, to prejudice an investigation by so informing the party or the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action.

Preliminary enquiries of a customer in order to verify his identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger tipping-off offence before a suspicious transaction report has been submitted in respect of that customer unless the staff member is aware that an investigation is underway or the enquiries are likely to prejudice an investigation.

Where it is known or suspected that a suspicious transaction report has already been disclosed to the FIU/BNM, the Police or other authorised agencies and it becomes necessary to make further enquiries, great care should be taken to ensure that the customer do not become aware that his/her name has been brought to the attention of the authorities.

- Penalties for Tipping-off: On conviction, a fine of up to RM1,000,000 and/or an imprisonment term up to one (1) year.

3.7 Can the Company/Licensee Continue to Transact with the Customer?

The professional responsibility issues concerning the customer as well as the legal/enforcement authorities that may arise once a report is made could be complicated. The licensee or its staff members are strictly prohibited from assisting the customer knowingly in any fraud or illegal conduct following the report made.

If a report is made, or if a report would have been necessary but for the fact that the transaction was not completed, there must have been some conduct or transaction of concern, and the licensee should consider the future of the business relationship with the customer.

When a suspicious transaction report has been made or is being made, the AML Guidelines has suggested that the licensee and its responsible staff members to continue dealing or to transact with the customer in the normal or usual way (on the surface) unless instructed otherwise by FIU or any other law enforcement agencies. This is necessary so as not to jeopardise or impair any investigation on the customer.

3.8 When and How to Withdraw from a Transaction with the Customer

After a suspicious transaction is triggered and a report has been made, and if the licensee determines that it is in an unresolvable conflict and decides that it cannot continue to act for the customer, the licensee and its staff members are prohibited from disclosing the fact that a report has been made and from disclosing the contents of the report.

Given the prohibition against disclosure, the licensee cannot be specific in stating the reason for withdrawal. The licensee is required to consult with the FIU/BNM prior to withdrawing from dealing with a customer under these circumstances.

The Compliance Officer will note down the fact of the withdrawal from the transaction in the AML compliance records file, together with the advice received from BNM and the reasons for the withdrawal.

3.9 "Threshold" or "Large Cash Transactions"

AIB determines and adopts RM10,000 as its cash transactional threshold for the AML reporting purpose. Thus, for a single or one-off cash transaction or payment of RM10,000 and above by a new or existing customer, a 'threshold report' must be made to the Compliance Officer, who will in turn reports the transaction to the FIU/BNM, regardless whether there is any evidence to classify the transaction as suspicious or otherwise.

For the purpose of this part, multiple cash transactions in the domestic or foreign currency which, in aggregate, amount to RM10,000 and above shall be treated as though it is a single transaction if they are undertaken by or on behalf of any one person or party during the course of one (1) day.

4.0 Training

4.1 The Objective of Training

The effectiveness of the vigilance system in the company depends on the extent to which the staffs of AIB comprehend the issues surrounding money laundering, their respective obligations under AML the Framework, as well as their obligations to comply with both the Guidelines and any relevant legislation. These can be achieved by a conscious and systematic effort to build an environment and culture of awareness and vigilance of money laundering activities at all levels within AIB.

4.2 Training Schedule

The training schedule of any AML courses or briefings (new, updates or refreshers) shall be built into the Company's Annual Training Programme at the beginning of each year.

4.3 Topics and Elements Covered by the Training Programme for the Following Categories of Staff:

4.3.1 New Employees

The beginner's training or orientation should generally include:-

- A description of the nature and processes of money laundering.
- An explanation of the staff's obligations under the Guidelines and any legal obligations contracted in the relevant legislation.
- An explanation of the vigilance policy and system, with particular emphasis on verification, the recognition of suspicious transactions and the need to report such suspicions to the departmental/branch head and the Compliance Officer.

4.3.2 Broking Staff / Technical Personnel

These are personnel who deal directly with the public and are the first persons of contact with money launderers. Thus, their efforts are vital to the implementation of the vigilance policy. They need to be aware of their obligations under the Guidelines, their legal responsibilities and the vigilance systems in place, in particular in relation to the obligation to identity and report suspicious transactions. These staff should be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Compliance Officer in accordance with the vigilance system, regardless whether the funds are accepted or the transaction proceeded with.

4.3.3 Management Staff and the BOD

A higher level of briefing and training encompassing all aspects of the Guidelines, vigilance policy and systems should be provided to those with the responsibility for supervising or managing staff. The training should include briefings on the relevant laws and any offences and penalties arising from any relevant legislation, procedures relating to the service of production and restraint orders, internal reporting procedures and the requirements for verification of identity and the retention of records.

4.3.4 Compliance Officer

- In-depth and thorough training on all aspects of the Guidelines, the relevant laws, vigilance policy and the AML Framework are essential for the Compliance Officer. In addition, there should be extensive instruction on verification, record keeping and reporting of suspicious transactions, besides feedback arrangements and liaison with the relevant authorities.

- Refresher and update training should be given at regular intervals, best achieved on six-monthly review of training, especially in areas such as the recognition and reporting of suspected money laundering transactions to ensure that key staff remain familiar with and are updated as to their responsibilities. There should also be regular updates in the administrative and legal requirements and obligations.

5.0 Accountabilities

5.1 Role of the Senior Management and Compliance Officer

The senior management of the company has the overall broad mandate and responsibility for overseeing the effective implementation of compliance regime policies and procedures throughout the company. The management team shall endeavour and be responsible in ensuring they provide all the necessary support and assistance to the Compliance Officer in ensuring the Company's commitments on AML measures and obligations are met and maintained at all times.

The Compliance Officer is appointed to monitor and assist the senior management to oversee the implementation of the vigilance system, periodically reviewing those policies and procedures, and training key staff members. In that capacity, the Compliance Officer and the responsible managers will be involved in the review of all transactions identified by other key staff members as possibly requiring reporting under the legislation. The Compliance Officer, with consultation from the senior management, will have the primary responsibility for reviewing the available information and determining whether a transaction needs to be reported. The managers who worked on the matter may be involved in reviewing the available information and determining whether the transaction needs to be reported as explained above ("Organisational Chain of Implementation, Roles and Responsibilities").

The Compliance Officer and the managers are responsible for maintaining the compliance records file. This file physically separate from the customer file and contains all customer-related information, worksheets, records and documents pertaining to compliance with the legislation.

Any key staff member who receives any correspondence regarding money laundering from FIU/BNM must direct the correspondence to the Compliance Officer for reference or further actions immediately.

5.2 Role of the Department, Branch or Servicing/Broking Manager

The manager should understand the principles of anti-money laundering as outlined in the Act and Guidelines, so that he/she can assist in creating awareness of money laundering at the respective department or branch.

He/She will assist in detecting, recognising and monitoring suspicious transactions and ensure that reporting procedures are observed by all the staff under his/her supervision.

In order to ensure full understanding of anti-money laundering issues by all the staff, the department or branch manager will coordinate training of staff (including agent), disseminate information, policies or procedural matters and to provide day-to-day guidance to staff (including agent) regarding compliance with the Anti-Money Laundering Act and Guidelines.

He/She may also act as point of reference or advice for any matter regarding money laundering in his/her department or branch.

6.0 Review of Policies and Procedures

6.1 Internal Audit

The objective of the Company's review will be to assess whether the company's policies and procedures are in place, are being adhered to, and whether the procedures and practices comply with the guidelines and legislation.

The review may involve:-

- Reviewing how staff members handle transactions to determine their knowledge of the legislative requirements and policies and procedures in place.
- Reviewing the criteria and process for identifying and reporting suspicious transactions.
- Testing the validity and reasonableness of exceptions made to reporting transactions.

On an annual basis, the audit may be conducted by independent qualified personnel such as internal auditors, who shall evaluate and review the efficacy of these policies and procedures.

The internal auditors doing the review will document all the findings, and identify and announce the findings deficiencies to the Compliance Officer. The Compliance Officer, in turn, will consult with the senior management for a response indicating corrective actions and a timeline for implementing such actions. This information will be kept in the Compliance Officer's records.

EXAMPLES OF SUSPICIOUS TRANSACTIONS

A Examples of Common Indicators of Suspicious Transactions

1 Knowledge of Money Laundering Reporting

- Customer does not want correspondence sent to home address.
- Customer admits or makes statements about involvement in criminal activities.
- Customer appears to have accounts with several financial institutions or contracting many policies with several insurance companies in one area for no apparent reason.
- Customer repeatedly used an address but frequently changes the names involved.
- Customer is accompanied and watched.
- Customer shows uncommon curiosity about the Company's internal systems, controls and policies.
- Customer has only vague knowledge of the nature and amount assured of a policy.
- Customer presents confusing details about transaction.
- Customer over justifies or explains the transaction.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, not in keeping with the transaction.
- Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after the policy is contracted.
- Customer is involved in activity out-of-keeping for that individual or business.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the customer's presentation of the transaction.
- Customer attempts to develop close rapport with staff.
- Customer uses aliases and a variety of similar but different addresses.
- Customer uses a post office box or general delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Customer offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- Customer suggests an unusual method of payment.
- Customer engages an unusual intermediary in the course of some usual transactions or financial activity.
- Customer appears to be living well beyond his or her means in light of his or her employment, profession or business.

- Customer is reluctant to discuss his or her financial affairs when this type of behavior is inconsistent with the ordinary business practice of the client, or out of context with the nature of the transaction being conducted.
- Customer requests anonymity.
- Customer attempts to convince you not to complete any documentation required for the transaction.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer seems very conversant with money laundering issues.
- Customer is quick to volunteer that funds are "clean" or "not being laundered".

2 Identity Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents (no originals sighted).
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customers' supporting documentation lacks important details such as a phone number and photograph.
- Customer inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.

3 Cash Transactions

- Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past.
- Customer uses notes in dominations that are unusual for him/her, when the norm in that business is much smaller or much larger denominations.
- Customer pay premium by notes that are packed or wrapped in a way that is uncommon for the client.
- Customer pays relatively large premiums by musty or extremely dirty bills.

- Customer makes cash transactions (engage a series of small policy contract) of consistently rounded-off large amounts (e.g., RM20,000, RM15,000, RM9,900, RM8,500, etc.).
- Customer consistently makes cash transactions (payment of premium) that are just under the reporting threshold (RM10,000).
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently requests return of premium on policy redemption that is paid for purchases of traveler's cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the customer.
- Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.

4 Economic Purpose

- Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically viable for the customer.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.

5 Transactions Involving the Policy

- Contracting the policy when the customer's address is outside the local service area.
- Contracting policy in other people's names.
- Contracting policy with names very close to other established business entities'.
- Attempting to open or operating accounts under a false name.
- Account with a large number of small policies and small number of large cash redemptions.
- Customer frequently uses many contracting locations outside of the home branch location.
- Customer makes multiple transactions on the same day.
- Inactive or dormant policy suddenly sees significant and active activity.
- Multiple premium payment is made on behalf of a customer by third parties.

6 Transactions Involving Areas Outside Malaysia

- Customer and other parties to the transaction have no apparent ties to Malaysia.
- Transaction crosses many international lines.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.
- Transaction involves a country known for highly secretive banking and corporate law.
- Transaction involves a country known or suspected to facilitate money laundering activities.
- Use of a credit card issued by a foreign bank that does not operate in Malaysia ("shell" bank) by a customer that does not live and work in the country of issue.

7 Transactions Related to Offshore Business Activity

- Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas account or accounts.
- Happen to know that the customer frequently requests for traveler's cheques, foreign currency draft or other negotiable instruments.
- Know that the customer obtained loans secured by obligations from offshore banks.
- Know that the customer loans to or from offshore companies.
- Offers of multimillion-dollar premium form a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic fund transfers by customer on an in-and-out basis for payment of premium and redemption of policy.
- Know that customer uses letter of credit and other methods of trade financing to move money between countries when such trade is inconsistent with his/her business.

B Examples of Specific Indicators for Suspicious Transactions:-

1 Brokerage and Sales

(i) New Business

- A personal lines customer for whom verification of identity proves unusually difficult, who is evasive or reluctant to provide full details.

- A corporate/trust customer where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

- A customer with no discernible reason for using the insurer's service, e.g. customers with distant addresses who could find the same service nearer their home base, or customers whose requirements are not in the normal pattern of or inconsistent with the insurer's business and could be more easily serviced elsewhere.

- A customer introduced by an overseas broker, affiliate or other intermediary, when both customer and introducer are based in countries where production of drugs or drug trafficking may be prevalent.

- Any transaction in which the insured is unknown (e.g. treaty reinsurance, business introduced under binding authorities, etc.)

(ii) Abnormal Transactions or which do not make economic sense

- Proposals from an intermediary not in keeping with normal business introduced.

- Proposals not in keeping with an insured's normal requirements, the markets in which the insured or intermediary is active in and the business which the insured operates.

- Early cancellation of policies with returns of premium, with no discernible purpose or in circumstances which appear unusual.

- A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time, the return of premium being credited to an account different from the original account.

- Any transaction in which the nature, size or frequency appears unusual, e.g. early termination or cancellation, especially where cash had been

tendered and/or the refund cheque is to a third party or a sudden purchase of a lump sum contract from an existing customer whose current contracts are small and of regular payments only.

- Assignment of policies to apparently unrelated third parties.

- Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to size or class of business.

- Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

- Willingness to pay high premium on high risks which have a likehood of regular claims being made.

2 Settlement

(i) Payment

- A number of policies taken out by the same insured for low premiums, each purchased for cash and then cancelled with return of premium to a third party.
- Large or unusual payment of premiums or transactions settlement by cash.
- Overpayment of premium with a request to refund the excess to a third party or to a different country.
- Payment by way of third party cheques or money transfers where there is a variation between the account holder, the signatory and the prospective insured.

(ii) Disposition

- Payment of claims to a third party without any apparent connection to the policy owner.
- Abnormal settlement instructions, including payment to apparently unconnected parties or to countries in which the insured is not known to operate.

(iii) Claims and Reinsurances

- Strong likelihood of risks occurring, resulting in substantial claims, with consequently high premium.
- Claims paid to persons other than insured.
- Claims which, while appearing legitimate, occur with abnormal regularity.
- Regular small claims within premium limit.
- Treaty reinsurance with high incidences of small claims.
- Regular reinsurance claims paid overseas to third parties.
- Recent change of ownership/assignment of policies just prior to a loss.
- Abnormal loss ratios for the nature and class of risk bound under a binding authority.

APPENDIX II

Money Laundering in the Insurance Industry
- Reporting of Suspicious Transactions to Bank Negara Malaysia

Report No. (xxx/yyyy): _____
(serial number/reporting year)

A. Details of Reporting Insurance Entity 1/

1. Reporting Institution: _____

2. Address: _____
_____
_____
_____

3. Telephone No.: _____

4. Fax. No.: _____

B. Details of Reporting Officer/Compliance Officer

1. Name: _____

2. Designation: _____

3. Telephone: _____

4. E-mail Address: _____

C. Customer's Particulars 2/

1.Name : _____

2. Birthdate/
Registration date* : _____

3. Nationality/
Country of Registration*: _____

MASTER COPY

4. NRIC/ Passport/
   Registration No. *: _____

5. Address: _____

6. Telephone No. : _____

7. Fax. No.: _____

8. Occupation/Designation/
   Business Activities * : _____

9. Name & Address
   of Employer/
   Own Office * : _____

D. Policy Details
(contracted, or otherwise – to complete where appropriate)

1. Policy No.: _____

2. Type of Policy: _____

3. Date of
   Commencement: _____

4. Name of Agent: _____

5. Agent's NRIC/
   Passport No.: _____

6. Contact Address: _____

7. Agency Name/
Address: _____

8. Sum Insured: _____

9. Payment mode: _____
(Yrly/half-yrly/quarterly/monthly/lump sum)*

10. Premiums payable in:-
- original currency: _____
- RM equivalent: _____

11. Name of
beneficiary: _____

12. Customer's relationship
with beneficiary: _____

13. Address of
beneficiary: _____

D. Details of the Suspicious Transactions 3/

1. Amount involved: _____

2. Date of transaction
regarded suspicious: _____

3. Source of funds: _____

4. Destination of funds: _____

5. Nature/ type of
transaction: _____

MASTER
COPY

6. Reason (s) for suspicion: _____

7. Other relevant information: _____

Details of authorised officer 4/:-

Name: _____
Designation: _____

Signature:

Insurance Entity: _____

Company stamp:

Date: _____

MASTER COPY

Anti-Money Laundering Act 2001

Revised Verification Procedures – BNM's JPI: 20/2004

- 23 August 2004

Effective 1 October 2004

JPI: 20/2004 – Revised Verification Procedures

- The revision came about after the dialogue session between IBAM & BNM
- JPI: 20/2004 was issued to facilitate compliance with S16(2) of AMLA (verification requirements)
- The circular supersedes JPI: 34/2003 (19.12.03)
- Procedures applicable to both insurers and insurance brokers
- Effective from 1 October 2004

FOR INDIVIDUAL APPLICANTS – Verification to be performed at the Point of Sale

- Sight the original NRIC, and verify against the details of the applicant; **OR**
- Sight the original current valid passport, and verify against the details of the applicant.

FOR INSTITUTIONAL APPLICANTS (incl. companies, partnerships, trusts and societies) – Verification to be performed at the Point of Sale

- Sight the relevant documents which can be used to establish the authenticity of the business, eg. Certificate of registration, M&A, audited annual accounts, etc; **AND**
- Verify against the details of the applicant.

OR

- We'll conduct a search on the applicant with the ROC/CCM or ROB/ROS

FOR INSURANCE POLICIES (both single and annual premium policies) with premiums exceeding RM50,000 and RM100,000 per annum in respect of individual and group policies respectively:

- A copy of the documents verified (spare original or photostat) should also be retained by the licensee.

In line with S16(3) of AMLA, verification of **BOTH** the applicant and beneficiary is required, where the beneficiary under a policy is different from the applicant.

Verification should be performed at the **Point of Sale (POS)**, except in the following circumstances:

(i) The verification procedures for the following may be performed at or before the time the benefits are paid out (this includes payments of sums insured, claims surrender values under life policies, and on the first withdrawal of units held under investment-linked policies):

- Policies sold with premiums not exceeding RM5,000 in aggregate per annum;
- Verification of beneficiaries (where different from the applicant); and
- Verification of individual members covered under group policies (verification of the group policy owner should be carried out at the POS).

Verification should be performed at the **Point of Sale (POS)**, except in the following circumstances:

(ii) For insurance policies sold **without face-to-face contact** (eg. through call centres, internet, direct mailing and telemarketing), verification may be performed at or before the time the benefits are paid out if the premiums do not exceed RM5,000, in line with the previous exception.

Verification for insurance policies sold without face-to-face contact with premiums exceeding RM5,000 shall be performed as soon as possible before the insurance cover is issued.

The customer identification procedures used to verify the identity of an non face-to-face customer should follow that used for face-to-face relationships and, at a minimum, should include a requirement for the insured to produce a certified copy of the identification documents.

INSURANCE BROKERS may rely on intermediaries or reliable third parties (eg. business introducers or employers who purchase group insurance policies for their employees) to perform the verification procedures.

- In such cases, insurance brokers should take adequate steps to satisfy themselves that a copy of all identification documents relating to verification performed will be made available by the intermediaries and third parties upon request and without delay.
- In such cases, insurance brokers shall be responsible to ensure that adequate customer due diligence is performed by the intermediary or third party.
- Insurance brokers should undertake and complete their own verification of the customers if they have any doubt of an intermediary or third party's ability to undertake appropriate customer due diligence.

FOR LOW-RISK INSURANCE APPLICATIONS (having regard to the type of customer, business relationship and nature of transaction), the following simplified procedures are permitted:

(i)

- for policies sold to a Government agency, financial institution as defined under the AML Act, public educational institution or company listed on Bursa Malaysia, the licensee is only required to ascertain that the institution falls within these categories;

FOR LOW-RISK INSURANCE APPLICATIONS (having regard to the type of customer, business relationship and nature of transaction), the following simplified procedures are permitted:

(ii)

- for policies sold via financial institutions to the institutions' customers, verification by licensees is not required if prior verification has been conducted by the financial institutions;

FOR LOW-RISK INSURANCE APPLICATIONS (having regard to the type of customer, business relationship and nature of transaction), the following simplified procedures are permitted:

(iii)

- for renewal and reinstatement of policies with no significant changes to the terms and conditions of the policy (including benefits under the policy), licensees may rely on prior verification performed, unless doubts arise concerning the veracity of information previously obtained for verification; and

FOR LOW-RISK INSURANCE APPLICATIONS (having regard to the type of customer, business relationship and nature of transaction), the following simplified procedures are permitted:

(iv)

- for reinsurance transactions, verification is not required where the ceding company is an insurer licensed under the Insurance Act 1996 or the Offshore Insurance Act 1990, or a takaful operator licensed under the Takaful Act 1984. Apart from these, reinsurers should take the necessary steps to verify that the ceding company is authorised to carry on insurance business in its respective jurisdiction, and that the jurisdiction is one which enforces anti-money laundering standards at least equivalent to that in Malaysia.

The extent of verification measures should be appropriate to the level of risk attached to the customer, business relationship or transaction. Enhanced due diligence should be undertaken for higher risk categories. For institutional applicants considered to be high-risk, additional due diligence measures should include verifying the identity of the individuals with controlling interests in, or having management control of, the business.

FACTORS TO CONSIDER in determining whether a customer belongs in the higher risk category:

- Customer type and background;
- Geographical origin of customer;
- Geographical sphere and nature of the customer's activities;
- Means and mode of payment;
- Unusual arrangements of payments to be made to third parties or other bearer arrangements; and
- Suspicion or knowledge of money laundering, financing of terrorism or other crime.

LICENSEES should have appropriate mechanisms in place to check and ensure that adequate verification procedures have been performed by their officers or intermediaries.

- In the event of failure to complete verification, licensees should not conclude an insurance contract, perform a transaction (eg. payment of benefits), or should terminate the business relationship. Licensees should also consider making a suspicious transaction report if there are grounds to believe that a suspicious transaction may have taken place.

Please refer to the distributed CHECKLIST relating to the AML verification procedures

THE END

ANIKA INSURANCE BROKERS SDN. BHD.

Anti-Money Laundering & Anti-Terrorism Financing Manual
- Revised Verification Procedures **Effective 1 October 2004**
- (BNM JPI: 20/2004 dated 23 August 2004)
- This circular supersedes the BNM circular JPI: 34/2003 issued on 19 December 2003

Revised verification procedures effective 1 October 2004:

1. FOR INDIVIDUAL APPLICANTS – Verification to be Performed at the Point of Sale:

   (i) Sight the **original** NRIC, and verify against the details of the applicant; OR
   (ii) Sight the original current valid passport, and verify against the details of the applicant.

2. FOR INSTITUTIONAL APPLICANTS (incl. companies, partnerships, trusts and societies) – Verification to be Performed at the Point of Sale:

   (i) Sight the relevant documents which can be used to establish the authenticity of the business, eg. Certificate of registration, memorandum and articles of association, audited annual accounts, etc., AND verify against the details of the applicant.

3. FOR INSURANCE POLICIES (both single and annual premium policies) WITH PREMIUMS EXCEEDING RM50,000 AND RM100,000 PER ANNUM IN RESPECT OF INDIVIDUAL AND GROUP POLICIES RESPECTIVELY:

   (i) A copy of the documents verified (spare original or photostat) should also be retained by the licensee.

4. In line with S16(3) of the AML Act, verification of **BOTH** the applicant and beneficiary is required, where the beneficiary under a policy is different from the applicant.

5. Verification should be **performed at the Point of Sale (POS)**, except in the following circumstances:

   (i) The verification procedures for the following may be performed at or before the time the benefits are paid out (this includes payments of sums insured, claims surrender values under life policies, and on the first withdrawal of units held under investment-linked policies):

      (a) Policies sold with premiums not exceeding RM5,000 in aggregate per annum.

      (Eg. A licensee may opt to perform the verification of an existing policy owner who had purchased a policy with an annual premium of RM4,000 at the time the benefits will be paid out instead of at the POS. However, the licensee will be required to perform the verification at the POS if the policy owner subsequently purchases another policy with the same licensee with combined premiums for both policies exceeding RM5,000.)

      (b) Verification of beneficiaries (where different from the applicant); and

      (c) Verification of individual members covered under group policies (verification of the group policy owner should be carried out at the POS); and

5. (Contd.)

(ii) For insurance policies sold without face-to-face contact (eg. Through call centres, internet, direct mailing and telemarketing), verification may be performed at or before the time the benefits are paid out if the premiums do not exceed RM5,000, in line with No. 5 (i) above.

Verification for insurance policies sold without face-to-face contact with premiums exceeding RM5,000 shall be performed as soon as possible before the insurance cover is issued.

The customer identification procedures used to verify the identity of an non face-to-face customer should follow that used for face-to-face relationships and, at a minimum, should include a requirement for the insured to produce a certified copy of the identification documents.

6. Insurance brokers may rely on intermediaries or reliable third parties (eg. business introducers or employers who purchase group insurance policies for their employees) to perform the verification procedures.

(i) In such cases, insurance brokers should take adequate steps to satisfy themselves that a copy of all identification documents relating to verification performed will be made available by the intermediaries and third parties upon request and without delay.

(ii) In such cases, insurance brokers shall be responsible to ensure that adequate customer due diligence is performed by the intermediary or third party.

(iii) Insurance brokers should undertake and complete their own verification of the customers if they have any doubt of an intermediary or third party's ability to undertake appropriate customer due diligence.

7. For low-risk insurance applications (having regard to the type of customer, business relationship and nature of transaction), the following simplified procedures are permitted:

(i) for policies sold to a Government agency, financial institution as defined under the AML Act, public educational institution or company listed on Bursa Malaysia, the licensee is only required to ascertain that the institution falls within these categories;

(ii) for policies sold via financial institutions to the institutions' customers, verification by licensees is not required if prior verification has been conducted by the financial institutions;

(iii) for renewal and reinstatement of policies with no significant changes to the terms and conditions of the policy (including benefits under the policy), licensees may rely on prior verification performed, unless doubts arise concerning the veracity of information previously obtained for verification; and

7. (Contd.)

(iv) for reinsurance transactions, verification is not required where the ceding company is an insurer licensed under the Insurance Act 1996 or the Offshore Insurance Act 1990, or a takaful operator licensed under the Takaful Act 1984. Apart from these, reinsurers should take necessary steps to verify that the ceding company is authorised to carry on insurance business in its respective jurisdiction, and that the jurisdiction is one which enforces anti-money laundering standards at least equivalent to that in Malaysia.

8. The extent of verification measures should be appropriate to the level of risk attached to the customer, business relationship or transaction. Enhanced due diligence should be undertaken for higher risk categories. For institutional applicants considered to be high risk, additional due diligence measures should include verifying the identity of the individuals with controlling interests in, or having management control of, the business.

Factors to consider in determining whether a customer belongs in the higher risk category:

- *customer type and background;*
- *geographical origin of customer;*
- *geographical sphere and nature of the customer's activities;*
- *means and mode of payment;*
- *unusual arrangements for payments to be made to third parties or other bearer arrangements; and*
- *suspicion or knowledge of money laundering, financing of terrorism or other crime.*

9. Licensees should have appropriate mechanisms in place to check and ensure that adequate verification procedures have been performed by their officers or intermediaries.

In the event of failure to complete verification, licensees should not conclude an insurance contract, perform a transaction (eg. payment of benefits), or should terminate the business relationship. Licensees should also consider making a suspicious transaction report if there are grounds to believe that a suspicious transaction may have taken place.

ANIKA INSURANCE BROKERS SDN. BHD.

Anti-Money Laundering and Anti-Terrorism Financing Guidelines
(Bank Negara Malaysia's Surat Pekeliling JPI: 20/2004 dated 23 August 2004)

VERIFICATION PROCEDURES - CHECKLIST

For more details, please refer to your latest copy of Anika's AML & ATF Manual.

[Please complete the form accurately and tick the applicable boxes, before sending it together with the debtors code creation form to the Finance department]

1. Name of client: _____

   Debtor code: _____
   (Please fill in once created)

   Date: _____

   Checklist completed by: _____
   (Anika's employee)

   Designation: _____

   Department: _____ Initial: _____

   Reviewed by: _____ Initial: _____

   Date: _____

   Approved by
   Compliance Officer: _____ Initial: _____

   Date: _____

---

2. Type of Clients/Applicants:

☐ Individual applicants – Go to Section 3

☐ Institutional applicants (including companies, partnerships, trusts and societies) – Go to Section 4

☐ Applicants under Group Policies – Go to Section 5

☐ Insurance policies sold without face-to-face contact (eg. through call centres, internet, direct mailing and telemarketing) – Go to Section 6

☐ Government agency, financial institution (as defined under the AML Act), public educational institution or company listed on Bursa Malaysia – Go to Section 7

☐ Policies sold via financial institutions to the institutions' customers – Go to Section 8

☐ Renewals and reinstatement of policies for existing clients with no significant changes to the terms and conditions of the policy (incl. benefits under the policy) – Go to Section 9

☐ Ceding company (reinsurance transactions) – Go to Section 10

---

3. Individual Applicants:

Verification to be performed at the Point of Sale:

☐ Sighted original NRIC AND verified against details of applicant; OR

☐ Sighted original current valid passport AND verified against details of applicant.

☐ Discrepancies noted:

_____

_____

_____

_____

_____

_____

_____

☐ Yes ☐ No Does the single & annual premium policies exceed RM50,000 p.a.? If yes, retain a copy (spare or photostat) of the documents verified.

Verification may be performed later for the following cases:

☐ Yes ☐ No Is the beneficiary under the policy different from the applicant? If yes, then verification of both the applicant and beneficiary is required. However, verification of the beneficiary may be performed at or before the time the benefits are paid out.

☐ Policies purchased with premiums not exceeding RM5,000 in aggregate p.a.
– Verification may be performed at or before the time the benefits are paid out.

---

4. Institutional applicants (including companies, partnerships, trusts and societies):

Verification to be performed at the Point of Sale:

☐ Sighted relevant business documents AND verified against details of applicant (eg. certificate of registration, M&A, audited annual accounts)

Document/s sighted: _____

☐ Discrepancies noted:

_____
_____
_____
_____
_____
_____
_____

☐ Yes ☐ No Does the single & annual premium policies exceed RM50,000 p.a. and RM100,000 p.a. in respect of individual and group policies respectively?
If yes, retain a copy (spare or photostat) of the documents verified.

Verification may be performed later for the following cases:

☐ Yes ☐ No Is the beneficiary under the policy different from the applicant?
If yes, then verification of both the applicant and beneficiary is required. However, verification of the beneficiary may be performed at or before the time the benefits are paid out.

☐ Policies purchased with premiums not exceeding RM5,000 in aggregate p.a.
– Verification may be performed at or before the time the benefits are paid out.

---

5. Applicants under Group Policies (companies who purchase policies for subsidiaries or other companies/parties within their group, or employers who purchase policies for their employees):

Verification to be performed at the Point of Sale:

☐ Sighted relevant business documents AND verified against details of group policy owner. (eg. certificate of registration, M&A, audited annual accounts)

Document/s sighted: _____

☐ Discrepancies noted:

_____

_____

_____

_____

_____

_____

_____

☐ Yes ☐ No Does the single & annual premium policies exceed RM50,000 p.a. and RM100,000 p.a. in respect of individual and group policies respectively?
If yes, retain a copy (spare or photostat) of the documents verified.

Verification may be performed later for the following cases:

☐ Yes ☐ No Is the beneficiary under the policy different from the applicant?
If yes, then verification of both the applicant and beneficiary is required. However, verification of the beneficiary may be performed at or before the time the benefits are paid out.

☐ Verification of individual companies/members covered under group policies
– Verification may be performed at or before the time the benefits are paid out.

☐ Policies purchased with premiums not exceeding RM5,000 in aggregate p.a.
– Verification may be performed at or before the time the benefits are paid out.

---

6. Insurance policies sold without face-to-face contact (eg. through call centres, internet, direct mailing and telemarketing) – Applicable only to individuals:

Verification to be performed as soon as possible before the insurance cover is issued:

☐ Sighted original NRIC AND verified against details of applicant; OR

☐ Sighted original current valid passport AND verified against details of applicant.

☐ Discrepancies noted:

_____

_____

_____

_____

_____

_____

_____

☐ Yes ☐ No Does the single & annual premium policies exceed RM50,000 p.a.?
If yes, retain a copy (spare or photostat) of the documents verified.

Verification may be performed later for the following cases:

☐ Yes ☐ No Is the beneficiary under the policy different from the applicant? If yes, then verification of both the applicant and beneficiary is required. However, verification of the beneficiary may be performed at or before the time the benefits are paid out.

☐ Policies purchased with premiums not exceeding RM5,000 in aggregate p.a.
– Verification may be performed at or before the time the benefits are paid out.

---

7. Government agency, financial institution (as defined under the AML Act), public educational institution or company listed on Bursa Malaysia:

The client has been ascertained to fall under the category of a:

☐ Government agency.

☐ Financial institution (as defined under the AML Act).

☐ Public educational institution.

☐ Company listed on Bursa Malaysia.

---

8. For policies sold via financial institutions to the institutions' customers, verification by insurance brokers is not required if prior verification has been conducted by the financial institutions.

---

9. For renewals and reinstatement of policies for existing clients with no significant changes to the terms and conditions of the policy (incl. benefits under the policy), insurance brokers may rely on prior verification performed, unless doubts arise concerning the veracity of information previously obtained for verification.

---

10. For reinsurance transactions, verification is not required where the ceding company is an insurer licensed under the Insurance Act 1996 or the Offshore Insurance Act 1990, or a takaful operator licensed under the Takaful Act 1984.

Apart from these, reinsurers should take the necessary steps to verify that the ceding company is authorised to carry on insurance business in its respective jurisdiction, and that the jurisdiction is one which enforces anti-money laundering standards at least equivalent to that in Malaysia.

Performance Management System