Capital Market Authority
Sultanate of Oman

Regulatory procedures manual for anti-money laundering for insurance companies, brokers and agents

Regulatory procedures manual for anti-money laundering for insurance companies, brokers and agents

Capital Market Authority
Sultanate of Oman
Po Box: 3359, Pc: 112
Tel 00698 24823100, Fax 00968 24816691
Web: www.cma.gov.om, e-mail: info@cma.co.om

1. INTRODUCTION:

Money laundering and terrorism financing crimes are economic crimes that require intensive efforts for combating them in the various sectors. Insurance sector can be used as a direct target for money laundering and terrorism financing operations.

This manual is based on Article (4) of Money Laundry Law promulgated by Royal Decree No (34/2002) which stipulates: "Institutions, natural and juristic persons shall verify their customers' identity and addresses, pursuant to the instructions issued by the competent supervisory authority before opening accounts, taking stocks, bonds or other securities for safe custody, granting safe deposit facilities or engaging in any other business dealings".

This manual aims at introducing money laundering operations and their role, measures that should be taken by insurance operators, policies that should be followed, suspicious transactions reporting measures and punishments. These would form effective measures and procedures to combat money laundering and terrorism financing.

2. MONEY LAUNDERING AND FINANCING OF TERRORISM

'Money Laundering' is a term used to describe a number of techniques, procedures or processes in which funds obtained through illegal and criminal activities are converted into other assets in such away as to conceal their true origin or ownership or any other factors that may indicate an irregularity, so that they appear to have originated from a legitimate source.
Article 2 of the Law of Money Laundering defines the offence of money laundering as under:
"Any person who intentionally commits any of the following acts shall be deemed to have committed the offence of money laundering:

(a) Transfer or movement of property or conducting a transaction with the proceeds of crime knowing, or with reason to know, that such property is derived directly or indirectly from a crime or from act or acts of participation in a crime, with the purpose of concealing or disguising the nature or source of such proceeds or of assisting any person involved in a crime

(b) The concealment, or disguise of the nature, source, location, disposition, ownership and rights in or with respect of proceeds of crime, knowing or with reason to know, that such proceeds were derived directly or indirectly from a crime or from act or acts of participation in a crime.

(c) The acquisition, receipt, possession or retention of proceeds of crime knowing, or with reasons to know, that it was derived directly or indirectly from a crime or from an act or acts of participation in a crime."

'Financing of terrorism' can be defined as the willful provision or collection, by any means,

directly or indirectly of funds with the intention that the funds should be used to facilitate or to carry our terrorist acts

"The Competent Authority" means "The Directorate General of Inquiries and Criminal Investigations of the Royal Oman Police"

"The Competent Supervisory Authority" for insurance licensees means "The Capital Market Authority"

3. MONEY LAUNDERING AND FINANCING OF TERRORISM IN INSURANCE

The insurance sector and other sectors of financial service industry are at risk of being misused for money laundering and financing of terrorism. Although, vulnerability of use of insurance sector for money laundering and financing terrorism is not as high as in other financial sectors like banking, the insurance sector (which includes insurers, reinsurance companies, brokers and agents) may be used as a possible target for money launderers and those seeking financing of terrorism as stated below:

A) Life Insurance

Life Insurance business is the predominant class of insurance business being used by money launderers.

The most common form of money laundering is to enter into a single premium contract or policy. The money launderer will then look to take back the monies by early surrender or by way of fraudulent claim.

Examples of life insurance contracts, which can be used for laundering money or terrorism financing are products, such as:

- Unit linked premium contracts which provide for withdrawals and unlimited top up premium
- Single premium life insurance policies where the money is invested in lump sum and can be surrendered at the earliest opportunity
- Fixed and variable annuities
- (Second hand) endowment policies
- When a life insurance policy matures or is surrendered, funds become available to the policyholder or other beneficiaries. The beneficiary under the contract may be changed before maturity or surrender in order that the payments are made by the insurer to a new beneficiary.

(B) General insurance

Money laundering or terrorism financing can be made through inflated and totally bogus claims,

e.g. by arson or other means to recover part of the invested illegitimate funds. Other examples include cancellation of policies for the return of premium by insurers' cheque, and the overpayment of premiums with request to refund the amount overpaid. Workmen compensation payments may be used to support terrorists awaiting assignments. Primary coverage and trade credit for transport of terrorist material may be provided.

(C) Reinsurers

Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious reinsurance companies or reinsurance brokers, fronting arrangements or by misuse of normal reinsurance transactions, for example the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers to disguise the source of funds.

(D) Insurance Intermediaries

Intermediaries are direct link to policyholders for distribution of insurance products, underwriting and claims settlement. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of or does not follow prescribed anti money laundering procedures or who fails to recognize and report information regarding suspicious transactions. Examples of money laundering involving insurance are provided in CMA's website.

4. CONTROL MEASURES AND PROCEDURES AGAINST MONEY LAUNDERING AND FINANCING OF TERRORISM

Every insurance licensee needs to have procedures and control measures preventing money laundering and terrorism financing which should include:

- Customer due diligence(Know your customer)
- Record keeping and ability to reconstruct a transaction
- Recognition and reporting of suspicious customers /transactions to the competent authorities
- Establishing and implementing internal policies, procedures and controls and appointment of competent officer at management level for implementation of such policies
- Establishing screening procedures when hiring employees and arranging on going training of employees and officers.

5. CUSTOMER DUE DILIGENCE (CDD)

5.1 Article 4 of the Law of Money Laundering, prescribes that

" Institutions and natural and juristic persons shall verify their customers' identity and addresses, pursuant to the instructions issued by the competent supervisory authority before opening

accounts, taking stocks, bonds or other securities for safe custody, granting safe deposit facilities or engaging in any other business dealings."

5.2 Insurance licensees shall undertake customer due diligence measures (CDD),* when:

(a) Establishing business relation i.e. when a person applies to do business with or through them.
(b) A significant or unusual transaction takes place or an occasional transaction above R.O. 6000 takes place in a single operation or in several operations that appear to be linked
(c) A change in policyholders' beneficiaries is made.
(d) There is a material change in the terms of insurance policy or the manner in which the. business relationship is conducted.
(e) Claims, commissions and other monies are to be paid to persons other than the policyholder.
(f) There is suspicion of money laundering or terrorism financing.
(g) The insurance licensee has doubt about the veracity or adequacy of previously obtained customer data.

5.3 Customer due diligence (CDD) measures

The following CDD measures should be taken by the insurance licensees:

(a) Obtaining sufficient and satisfactory evidence to establish the customers' identity and his legal existence.
(b) Determining whether the customer 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 as per para 5.4 and whether the customer is authorized to do so.
(c) Identifying the (ultimate) beneficial owner (especially for life and other investment related insurances) and taking measures to verify the identity of the beneficial owner.
(d) Obtaining information on the purpose and intended nature of business relationship.
(e) Conducting on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.

5.4. Methods of identification and verification

5.4.1. For individuals

If, customer is an individual, the insurance licensee must obtain and record the following information:

(a) Full name and any other names used
(b) Current permanent address including postal code, and current mailing address
(c) Date and place of birth

(d) Nationality
(e) Sex: Male/Female
(f) Current Passport number and/or current National Identity Card /Resident Card number/ Driving licence details
(g) Occupation and position held
(h) Employers name and address (If, self employed, the nature of self employment)
(i) Telephone number, fax number, e-mail address (where applicable)
(j) Signatures of the individual

The insurer must obtain supporting documents of the customer.

5.4.2. For Legal entities (companies and other legal arrangements)

If customer is a juristic entity, the insurance licensee should obtain and record the following information:

(a) the entity's full name
(b) date and place of incorporation and registration number
(c) legal form
(d) registered address and trading address
(e) names, nationalities and addresses of persons owning more than 10% of the capital.
(f) type of business activity
(g) telephone, fax, e-mail
(h) identification of the person/s purporting to act on behalf of the customer andverification that he person/s are so authorized

The information furnished shall be verified by obtaining certified copies of the following documents:

(a) certificate of incorporation/commercial registration
(b) memorandum of association
(c) articles of association
(d) partnership agreement
(e) copy of the latest annual report of the company
(f) board resolution providing the list of authorized signatories/ copies of power of attorney
(g) identification documentation of the authorized signatories.

5.4.3. Certification

Any document used for the purpose of identification/verification should be originaldocument. Where a copy of an original document is made by the insurance licensee, the copy should be

dated, signed and marked 'original sighted' by the authorized official of the insurance licensee. Any documents which are not obtained and certified by an authorized official of the insurance licensee should be certified and signed by any of the following from the country of residence of the customer:

(a) a registered notary
(b) a government ministry
(c) an official of an embassy or consulate
(d) a registered auditor
(e) a registered lawyer

5.4.4. Group life insurance policies

Where there are large number of policyholders (e.g. in case of group life insurance), it may be sufficient to carry customer identification on a limited group only, such as the principal shareholders, the main directors of the company and the holder of the master policy.

5.4.5. Keeping data up-to-date

Insurance licensees shall ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of the existing records.

5.4.6. Policy to insure life other than the proposer

Where a person applies for a policy to insure a life other than himself, it is the applicant for the policy whose identity has to be verified rather than the life to be insured.

5.5. CDD for existing customers and on business relationship and transactions throughout the course of relationship

(a) Business relationship with the customer shall be subjected to ongoing follow up and operations resulting of such relationship shall be verified.
(b) Customer particulars shall be reviewed and updated periodically.

Examples of transactions or 'trigger events' after establishment of the insurance contract are:

- A change in beneficiaries (for instance , to include non-family members, or a request for payment to be made to person other than the beneficiaries)
- A change/increase of the capital sum insured and /or of the premium payment (for instance, which appear unusual in the light of policyholders' income or where there are several over payments of policy premiums after which the policyholder requests that reimbursement is paid to a third party)

- Use of cash and/or payment of large single premiums
- Payment/surrender by a wire transfer from/to foreign parties
- Lump sum top up of existing life insurance contracts
- Request for prepayment of benefits
- Use of policy as collateral security (Unless required for financing mortgagee by a reputable financial institution)
- Change of the type of benefit (for instance, change from an annuity to lump sum payment)
- Early surrender of policy or change of duration (where this causes penalties) This list is not exhaustive.

5.6. Timing of identification and verification

The identification and verification of customers and beneficial owners should take place before or during the course of conducting transaction.

An insurance licensee may start processing the business while taking steps to verify the customers' identity. Pending receipt of required evidence, insurer shall "freeze" the rights attaching to the policy, and shall not issue documents of title. In case of failure by a customer to provide satisfactory evidence of identity, the transaction in question should not proceed further and relationship be terminated. The insurance licensee shall consider making a suspicious transaction report (STR) as this manual's requirements.

In case of life insurance, where a business relationship has been established after due verification of the policyholder, it is permissible to do the identification and verification of the beneficiary after the establishment of business relationship with the policyholder.
However, such identification and verification must occur before the time of payout to the beneficiary or before the time the beneficiary intends to exercise vested rights under the policy.

5.7. Classification of customers

Based on the customer and the product profile, the insurance licensee may classify the customers into low risk and high risk category.

5.7.1 Low risk category:

If the risk of money laundering or financing of terrorism is lower (based on insurance licensee's assessment), and if information on the identity of the customer or beneficial owner is publicly available, or adequate checks and controls exist elsewhere in the national systems it would be reasonable to apply, simplified and reduced CDD measures when identifying and verifying the identity of the customer or the beneficial owner.

Examples of customers, transactions or products where the risk may be lower is as under:

(a) Financial institutions—Banks and financial institutions regulated by the Central Bank of Oman.
(b) Companies listed on a stock exchange recognized by CMA
(c) Government administrations or government enterprises and companies where government is a major shareholder.
(d) Life insurance policies where annual premium is NO more than RO 500, or, a single premium of NO more than RO 1000 or equivalent.
(e) Insurance policies for pension schemes, if there is no surrender clause and policy cannot be used as security for loan.
(f) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a members' interest under the scheme.

Simplified CDD measures shall not apply, where the insurer suspects or has reason to suspect that the customer is engaged in money laundering or that transaction has been carried out on behalf of another person engaged in money laundering

5.7.2 Enhanced measures with respect to high risk customers

Enhanced CDD measures should apply to all business relationships, clients and transactions where the risk of money laundering is high.

Examples of high risk categories are:

(a) Non-resident customers
(b) High net worth individuals of non Omanis.
(c) Private banking
(d) Legal persons or arrangements such as trusts which are created for holding personal assets; charities and organizations.
(e) companies having closed family shareholding; firms with sleeping partners etc.
(f) Politically exposed persons (PEP*) i.e. the individuals who are or have held prominent public positions in a foreign country, for example head of state and government, senior politicians, senior government, judicial and military officials, senior executives of state owned corporations, important political parties officials.

With regard to enhanced due diligence, the following, additional measures should be taken, as required:

(a) Certification of documents by appropriate authorities and professionals
(b) Requisition of additional documents to complement those which are otherwise required
(c) Performance of due diligence on identity and background of the customer and/or beneficial owner, including the structure in the case of a corporate customer
(d) Performance of due diligence on source of funds and wealth
(e) Obtaining senior managements approval for establishing business relationship
(f) Conducting enhanced on going monitoring of the business relationship

For PEPs an insurance licensee must observe measures (d), (e) and (f) stated in the above para.

5.8. Complex, large and unusual transactions

Insurance licensees should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic purpose. The background of such transactions should be as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.
"Transactions" include enquiries and application for an insurance policy, premium payments, request for changes in benefits, beneficiaries, duration, etc

5.9. New and developing technologies.

New and developing technologies can be used to market insurance products.
E-commerce or sales through the internet is an example. Insurance licensees shall take particular care in accepting new business through internet, post or telephone.
Although, a non face-to-face customer can produce the same documentation as face-to-face customer, it is more difficult to verify their identity. Therefore, in accepting business from non face-to-face customer an insurer should use equally effective identification procedures as those available for face to face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk

Examples of such risk mitigating measures are:

- Certification by appropriate authorities and professionals of the documents provided
- Requisition of additional documents to complement these which are required for face-to face customers
- Telephone contact with the customer at an independently verified home or business number
- Requiring the first payment to be carried out through an account in the customers' name with a licensed bank in Oman.

5.10 Failure to satisfactorily complete CDD

Where an insurance licensee in unable to comply with the Customer Due Diligence criteria as this manual requires;

a) It should not establish insurance business relationship.

b) It should consider making suspicious transaction report (STR).

Where the insurance licensee has already commenced the business relationship and the insurance licensee is unable to comply with the CDD criteria (a) to (d) of para 5.3 it should terminate the business relationship and consider making a suspicious transaction report (STR).

5. 11 Reliance on Insurance Intermediaries for CDD measures

5.11.1 Insurance Brokers

The insurance companies may accept the customers introduced to them by the licensed brokers subject to the following conditions:

(a) Although, the insurance brokers are responsible for implementing all CDDmeasures, the ultimate responsibility for customer and/or beneficial owner identification and verification shall remain with the insurer relying on the insurance broker..

(b) Insurer shall obtain the necessary information concerning elements (a) to (d) of para 5.3 of the CDD measures from the broker.

(c) Insurer shall obtain a written confirmation from the broker that all CDD measures required by this manual have been followed and customers'/beneficial owners' identity has been established and verified. In addition, the confirmation must state that any identification documents and other customer due diligence material can be accessed by the insurer and copies of the documents and material shall be supplied to the insurer on request, without delay.

5.11.2 Insurance agents

Insurers shall be responsible for complying with the CDD measures for the business introduced by their agents and any third parties and for keeping records of the business introduced by them.

6. RECORD KEEPING

Article 5 of the Law on Money Laundering requires the institutions to maintain and hold documents of identification and addresses of customers and record of transactions for a period not less than ten years commencing the day following the finalization of transaction or closure of the account or termination of business relation , whichever is later.

Insurance licensees should, therefore, keep record on the

- risk profile of each customer and/or beneficial owner and the data obtained through the CDD process (i.e. copies of records of official identification documents like passport, identity cards, driving licenses or similar other documents), and
- the account files, business correspondence and record on business transactions for at least ten years after the end of business relationship i.e. at least ten years after the expiry of the policies and/or ten years after settlement of claims, surrender or cancellation. Such record should be sufficient to permit reconstruction of individual transactions so as to provide, if required, evidence for prosecution of criminal activity.

In situations, where the records relate to on-going investigations or transactions which have been subject to suspicious transaction reports, they should be retained until it is confirmed that the case has been closed.

7. SUSPICIOUS TRANSACTION REPORT (STR)

7.1 Reporting of suspicious transactions

Article 9, of the Law on Money Laundering prescribes that:

"Notwithstanding any provision relating to the confidentiality, institutions shall report to the competent authority on the transactions which are suspected to be in contravention of this Law. The report shall include all available information and documents relating to the transaction.

Institutions may be required by the public prosecution to submit any additional information relating to suspicious transactions. The information shall be submitted through the Central Bank or the competent supervisory authority".

7.2 Reporting suspicious transactions before finalization of the transaction

Article 11 of Law of Money Laundering, prescribes that:

" In the existence of information showing that the customer is not acting on his own behalf and the transaction is suspicious, the institutions shall immediately and before the finalization of the transaction , report such information and suspicions to the competent authority(Directorate general of Inquiries and Criminal investigations of the Royal Oman Police). Customers with profession such as lawyers or those with public powers of attorney may not invoke professional secrecy in order to refuse to disclose the true identity of the beneficiary"

Insurance licensees shall comply with the statutory obligation of reporting suspicious transactions.

7.3 Prohibition to tip off the customer

Article 8, of the Law of Money Laundering, prescribes that:

"Institutions and their directors and employees shall not advise their customers when reporting information relating to them or the existence of suspicions of contravention of this Law in their activities, to the competent authority."

Insurance licensees should note that 'tipping off "the customer about reporting to the competent authority is prohibited by the Law and is a punishable offence.

7.4 Recognizing suspicious transactions

(a) Suspicious transaction may fall into one or more of following examples of categories:

- Any unusual financial activity or transaction of the customer
- Any unusually linked transaction
- Any unusual or disadvantageous redemption of an insurance policy
- A claim made in suspicious circumstances.
- Any unusual method of payment
- Any involvement of any person subject to international sanctions.

An important condition for recognition of a suspicious transaction is for the insurance licensee to know enough about the customer and business relationship to recognize that a transaction or a series of transaction is unusual.

(b) When an insurance licensee is unable to complete CDD measures as required under Para 5 of this manual, it should consider making suspicious transaction report.
The process of verification of customers' identity, once begun, should be pursued either to a conclusion or to the point of refusal. If a prospective policyholder does not pursue an application, this may be considered suspicious in itself.

It is likely, that if an insurance licensee performs additional CDD because of suspicion, it could unintentionally tip off the policyholder or beneficiary of the suspicious transaction report. If the insurance licensee believes that performing the CDD process may tip off the customer, it may choose not to pursue that process and should file a STR.The insurance licensee should ensure that their employees are aware of and sensitive to these issues when conducting CDD. Examples of suspicious transactions may be found in CMA's website.

7.5 Internal Reporting

An insurance licensee must take reasonable steps to ensure that any member of staff who handles transactions which may involve money laundering makes a report promptly to the compliance officer, if he suspects that a customer or a person acting on behalf of a customer is engaged in money laundering and or that transaction is unusual or suspicious.

7.6 External Reporting

An insurance licensee shall ensure that any report required by para 7.5 above is considered by the compliance officer, and that if, having considered the report, he suspects that a person has been engaged in money laundering , he must make a report to the competent authority.

7.7 Suspicious Transaction Report (STR)

STR may be made as per form given in the Annexure-1.

8. ORGANIZATION AND STAFF

Article 6 of Law of Money Laundering states:

"Institutions shall establish internal control arrangements for detection and prevention of money laundering and shall further comply with the instructions issued by the competent supervisory authority.

Institutions shall develop programmes for combating money laundering. Such programmes shall include the following:

(a) Enhancing and implementing internal policies, procedures and controls including designation of competent officers at management level for implementation of such policies.

(b) Preparation of ongoing training programmes of concerned officials to keep them well informed on the latest developments in money laundering offences to enhance their abilities in detecting and combating such offences."

8.1 Establishing and implementing internal policy, procedures and controls

A detailed internal policy, procedures and control system for combating money laundering and terrorism financing shall include:

- procedures for customer due diligence (CDD;
- monitoring of transactions, identification and reporting of suspicious transactions;
- compliance management and appointment of compliance officer;
- standards for hiring employees and
- on going employee training programme.

The policy, procedures and controls shall be approved by the Board of insurance licensees who are companies incorporated in Oman, and by the senior management or head office in case of foreign branches and a copy shall be filed with the CMA.

8.2 Appointment of compliance officer

Article 5/15 of the 'Code of Corporate Governance for Insurance Companies' prescribes

the appointment of a senior manager of appropriate standing, knowledge and experience as compliance officer. The compliance officer appointed as per Article 5/15 of the 'Code of Corporate Governance' shall also be entrusted with the responsibility of monitoring AML and CFT measures and reporting suspicious transactions However, an insurance company may appoint an exclusive senior officer for AML/CFT measures and reporting of STRs if the work load so demands.

Insurance brokers shall also designate a senior and competent officer as compliance officer. The compliance officer should be well versed in different types of products and transactions which the insurance licensee handles and which may give rise to opportunities for money laundering and the financing of terrorism.

Name and particulars of the compliance officer shall be communicated to the CMA

8.3. Duties of compliance officer

The compliance officer shall have sufficient authority and resources to enable him to perform his duties which shall comprise of

- Establishing the insurance licensees' AML/CFT measures
- Ensuring the licensees' compliance with the Money Laundering Law and instructions issued by the CMA
- Verifying the internal reports and assessing CDD information
- Making external reports as per this manual to the Competent authorities
- Maintaining record of internal reports received and external reports made
- Arrangements for staff awareness and training by himself or someone else and keeping record of such training
- Making annual reports to senior management
- Having clear procedures for employees to immediately report cases suspicious as money laundering cases to the compliance officer.
- Compliance officer shall be aware of every related information including CDD information.
- Having clear verification methods and procedures for STR by the compliance officer, and reporting immediately and directly to the competent authority and competent supervisory authority without the need of any person's approval.
- All employees shall be aware to whom to report in case of any suspicious.
- Maintaining a record of all reports submitted by employees and all reports the compliance officer submitted to the competent authority.

8.4 Internal Audit

Insurance licensee's internal audit shall verify on a regular basis, compliance with the policy, procedures and controls relating to AML/CFT measures and submit its report to the audit committee.

8.5 Compliance monitoring

The Board of the insurance licensee/senior management shall review the effectiveness of its AML/CFT controls and procedures at least once each calendar year. The scope of review shall include:

(a) Number of internal reports made analytical breakdown of the results of those reports and their outcome

(b) Number of external reports made how many internal reports were not converted into external reports and reason for the same.

(c) Internal Auditors' report of sample testing of CDD measures and the quality and effectiveness of anti money laundering controls and procedures.

(d) Action plan to remedy deficiencies identified in the report.

8.6 Screening of staff

Insurance licensees are required to put in place screening procedures to ensure high standards of ability and integrity when hiring employees. Insurance licensees should identify the key staff within their organization with respect to AML/CFT and define fit and proper requirements which these staff should posses.

8.7 Training of staff

Each insurance licensee shall train its staff and agents in

- Nature and process of money laundering and terrorism financing, including current money laundering and terrorism financing techniques, methods and trends and new developments
- All aspects of Anti Money Laundering Law, regulations, guidelines on AML and CFT measures set out in this manual by CMA, and in particular, the requirements concerning CDD and suspicious transaction reporting and the company's commitment to that.
- Licencees' own AML/CFT policies and procedures for CDD, verification, record keeping, and reporting.
- The identity and responsibility of the compliance officer.

(a) "Front-Line Staff

"Front-line" staff who deal directly with public are first point of contact with the money launderers. They deal with:

- New business and the acceptance either directly or through agents and brokers
- Settlement of claims
- Collection of Premium and payment of claims.

In addition to the training in Para (a) above, they should be trained in:

- CDD measures , client acceptance policy and procedures for verification and record keeping
- Dealing with non regular customers when large transactions are involved
- Dealing with single premium and investment related life insurance policies
- Their responsibility under AML/CFT policies and procedures.

(b) supervisors/ Managers/ Senior Management and DirectorsA higher level of training covering all aspects of money laundering and AML/CFT measures should be provided. This should include:

- Offences and penalties arising from the Law
- Procedures relating to the service of production and restraint orders (to stop writing new business)
- Internal reporting procedures
- The requirements of verification and records

(c) Compliance OfficerThe compliance officer should receive in depth training concerning all aspects of the Money laundering Law, Regulations and instructions issued by the supervisory authorities and AML/CFT policies and procedures. In addition, the compliance officer shall require extensive initial and continuing instructions on the validation and reporting of suspicious transactions and on the feedback arrangements.

9. PENALTY STATED ACCORDING TO THE MONEY LAUNDERING LAW

Penalty stated in Money Laundering Law and its executive regulations are applied to any violation or incompliance to this manual's requirements.

ANNEXURE (1)

STR (Suspicious Transactions Report)

1. Reporting insurance licensee/ broker:

a. Name
b. Address
c. Phone
d. Fax/ e-mail

2. Reporting employee:

a. Name
b. Job
c. Report reference number

3. Customer's details:

a. Name
b. Passport/ identical card number
c. Nationality
d. Address
e. Phone/ fax/ e-mail
f. Profession
g. Type of activity

4. Policy's details:

a. Policy number
b. Policy type
c. Start date
d. Insured sum
e. Payment method: annual/ semiannual/ monthly
f. Premium required: regular/ one payment
g. Origin of cash
h. Agent's name
i. Agent's passport/ identical card number
j. Other business relations

5. Suspicious transactions:

Sum Date Transaction description

6. Suspicious reasons:
7. Other related information
8. Copy of attached documents

- Offer's sample
- Other communications
- Agent's report
- Related documents supporting suspicious transactions

Signature of employee:

Date

ANNEXURE (2)

PHONE AND FAX NUMBERS OF INSURANCE OPERATIONS DEPARTMENT, CMA

S	STATEMENT	OFFICE TELEPHONE
1	Director of Insurance Operations	24823440
2	Insurance auditor	24823122
3	Insurance auditor	24823328
4	Insurance auditor	24823114
5	Fax	24817383
6	e-mail	info@cma-oman.gov.om

PHONE AND FAX NUMBERS OF FINANCIAL INVESTIGATIONS UNIT

S	STATEMENT	OFFICE TELEPHONE
1	Director of Unit	24562856 - 24563372
2	Administration Affairs and Services	24569459
3	Phone exchange	24569601
4	Director's office fax	24569601
5	Administration Affairs and Services' fax	24569165
6	e-mail	ropfiu@omantel.net.om