REPUBLIC  **OF CYPRUS**

INSURANCE COMPANIES CONTROL SERVICE

Orders for Life-Insurance Companies and Life-Insurance Intermediaries in accordance with Article 59(4) of the PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007-2013

(FOURTH ISSUE)

APRIL 2014

CONTENTS

1. INTRODUCTION

1.1 The Republic of Cyprus enacted the appropriate legislation and has taken effective regulatory and other measures by putting in place suitable mechanisms for the prevention and suppression of money laundering and terrorist financing activities. Moreover, Cyprus is committed to apply all the requirements of international treaties and standards in this area and, specifically, those deriving from the European Union Directives.

1.2 On 13/12/2007 the House of Representatives enacted "The Prevention and Suppression of Money Laundering Activities Law" (hereinafter to be referred to as "the Law") by which the former Laws on the prevention and suppression of money laundering activities of 1996-2004 were consolidated, revised and repealed. Under the current Law, which came into force on 1 January 2008, the Cyprus legislation has been harmonised with the Third European Union Directive (2005/60/EC) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

1.3 The present Orders are issued for Life - Insurance Companies and Life - Insurance Intermediaries in accordance with Article 59(4) of the Law 2007-2013 (subsequent amendments of the Basic Law, 58(I)/2010, 80(I)/2012, 192(I)2012, 101(I)/2013), and aim at laying down the specific policy, procedures and internal controls that the above should implement for the effective prevention of money laundering and terrorist financing so as to achieve full compliance with the requirements of the Law. It is emphasized that the Law explicitly states that Orders are binding and compulsory to all persons to whom they are addressed. Furthermore, the Law assigns to supervisory authorities, including the Superintendent of Insurance, the duty of monitoring, evaluating and supervising the implementation of the Law and the Orders issued to supervised entities.

2. THE MAIN PROVISIONS FOR THE PREVENTION AND SUPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007-2013

2.1 Purpose

The main purpose of the Prevention and Supression of Money Laundering Activities Law of 2007-2013 (hereinafter to be referred to as "the Law") is to define and criminalise the laundering of proceeds generated from all serious criminal offences including terrorist financing offences and provide for the confiscation of such proceeds aiming at depriving criminals from the profits of their crimes. It also places special responsibilities upon life insurance companies and life insurance intermediaries for the conclusion of life insurance, other financial institutions and professionals which are required to take preventive measures against money laundering and terrorist financing by adhering to prescribed procedures for customer identification, record keeping, education and training of their employees and reporting of suspicious transactions. The main provisions of the Law, which are of direct interest to Life Insurance companies (hereinafter to be referred as 'Insurance Companies'), and Life insurance Intermediaries (hereinafter to be referred as 'Intermediaries') are as follows:

2.2 Prescribed offences (Article 3 of the Law)

The Law has effect in respect of offences which are referred to as "prescribed offences" and which comprise of:

(i) money laundering offences; and

(ii) predicate offences.

2.3 Money Laundering offences (Article 4 of the Law)

Under the Law, every person who knows or at the material time ought to have known that any kind of property constitutes proceeds from a predicate offence, is guilty of an offence, if is engaged in any of the following:

(i) converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of a predicate offence to evade the legal consequences of his actions;

(ii) conceals or disguises the true nature, source, location, disposition, movement, rights with respect to property or ownership of this property;

(iii) acquires, possesses or uses such property;

(iv) participates in, associates, co-operates or conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above;

(v) provides information with respect to investigations that are being performed for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence.

Commitment of the above offences is punishable on conviction by a maximum of fourteen (14) years imprisonment or a fine up to 500.000 euro or both of these penalties, in the case of a person knowing that the property is proceeds from a predicate offence or by a maximum of five (5) years imprisonment or a fine up to 50.000 euro or both of these penalties, in the case he ought to have known.

2.4 Predicate offences (Article 5 of the Law)

Predicate offences are:

a) All criminal offences punishable with imprisonment exceeding one year from which proceeds were generated that may become the subject of a money laundering offence as defined in Article 4.

b) Terrorist financing offences as defined in Article 4 of the Ratification Laws of the United Nations Convention for Suppression of the Financing of Terrorism of 2001 and 2005, as well as the collection of funds for the

financing of persons or organizations associated with terrorism.

c) Offences for drug trafficking as defined in article 2 of the Law.

With regard to the terrorist financing offences it should be noted that on 22 November 2001, the House of Representatives enacted the Ratification Laws of the United Nations Convention for Suppression of the Financing of Terrorism. As a result of the above, terrorist financing is considered to be a criminal offence punishable with 15 years imprisonment or a fine of EUR 1,7 million or both of these penalties. Furthermore, the above Law contains a specific Article which provides that terrorist financing and other linked activities are considered to be predicate offences for the purposes of Article 5 of the Law. Consequently, suspicions of possible terrorist financing activities or collection of funds for terrorism financing should be immediately disclosed to MOKAS under Articles 27 and 69 of the Law.

For the purposes of money laundering offences, it does not matter whether the predicate offence was committed abroad and, consequently, is not subject to the jurisdiction of the Cyprus courts (Article 4(2) of the Law).

2.5 Defenses for persons assisting money laundering and duty to report (Article 26 of the Law)

It is a defense, under Article 26 of the Law, in criminal proceedings against a person in respect of assisting another to commit a money laundering offence that he intended to disclose to the Unit for Combating Money Laundering (hereinafter to be referred to as "MOKAS") his suspicion or belief that the agreement or arrangement related to proceeds from a predicate offence and that his failure to make the disclosure was based on reasonable grounds. Also, under Article 26 of the Law, any such disclosure made in good faith, should not be treated as a breach of any restriction imposed by contract that insurance companies and intermediaries have on their customers and it does not involve any kind of responsibility from the person that makes the disclosure.

In the case of employees of persons whose activities are supervised by one of the authorities established under Article 59, the Law recognizes that the disclosure may be made to the Money Laundering Compliance Officer (MLCO) in

accordance with established internal procedures and such a disclosure shall have the same effect as a disclosure made to MOKAS.

2.6 Reports to MOKAS (Article 27 of the Law)

It is an offence for any person who, in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing not to report his knowledge or suspicion as soon as it is reasonably practical, after the information came to his attention, to MOKAS. Failure to report in these circumstances is punishable on conviction by a maximum of five (5) years imprisonment or a fine not exceeding 5.000 euro or both of these penalties.

All Money Laundering Compliance Officer's **(hereinafter to be referred as 'MLCO'**) Reports to MOKAS should be sent or delivered at the following address:

Unit for Combating Money Laundering ("MOKAS")

The Law Office of the Republic,

7 Periclous Street, 1st , 2nd & 3rd Floors,

2020 Strovolos, Nicosia, Cyprus

Mailing Address: P.O.Box 23768

1686 Nicosia

Email: mokas@mokas.law.gov.cy

Tel.: +357 22446018

Fax: +357 22317063

2.7 Refraining from performing suspicious transactions before filing a report with MOKAS (Article 70 of the Law)

Article 70 of the Law requires persons engaged in financial or other business to refrain carrying out transactions which they know or suspect to be related with money laundering or terrorist financing before they report their suspicion to MOKAS in accordance with articles 27 and 69 of the Law. As already mentioned above, the obligation to report to MOKAS includes also the attempt to carry such suspicious transactions. Where such a transaction is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, persons carrying on financial or other business shall inform MOKAS immediately afterwards.

2.8 Prohibition of tipping - off (Article 48 of the Law)

It is an offence to make a disclosure to the person who is the subject of a suspicion of money laundering or to a third person that information or other relevant material has been submitted to MOKAS or disclose other relevant data with regard to knowledge or suspicion of money laundering or make a disclosure which may impede or prejudice the search and investigation carried out with regard to ascertaining proceeds or the commitment of a prescribed offence while the person making the disclosure knew or suspected that the above search or investigation was in process. The said offences are punishable with imprisonment up to five (5) years.

2.9 Exemptions from tipping - off (Article 49 of the Law)

Without prejudice to the provisions of article 48, persons carrying financial activities in accordance with article 2 of the Law, may disclose to other persons belonging to the same group operating in countries of the European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined

that it imposes procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive, that information has been disclosed to MOKAS in accordance with article 27 or that a money laundering or terrorist financing investigation is being or may be carried out by the MOKAS.

For the purposes of these Orders, "group" means a group of undertakings, which consists of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries own, directly or indirectly, 20% and above of the voting rights or the share capital of the company. The terms parent company and subsidiary company have the meaning ascribed to them by the International Financial Reporting Standards issued by the International Accounting Standards Board.

Furthermore, it is noted that under article 49 (5) of the Law, the disclosure to the Superintendent of Insurance that a suspicious report or other information have been submitted to MOKAS or disclosing that an investigation is carried out or might be carried out by MOKAS for money laundering or terrorist financing offences, it is not considered as a breach of any contractual or other legal prohibition in the disclosure of information.

2.10 Implementation of these Orders by the branches and subsidiaries of Insurance Companies based in Cyprus and operating outside the European Union

These Orders are applicable to branches and subsidiaries established by Cyprus insurance companies under the approval of the Superintendent of Insurance of Cyprus, in third countries outside the European Union. Cyprus insurance companies should ensure that branches and subsidiaries established in third countries fully comply with the provisions of these Orders with regard to customer identification and due diligence measures and record keeping procedures.

In this regard, insurance companies should forward these Orders, as well as the relevant sections from their risk management and procedures manual for the prevention of money laundering and terrorist financing, to the Board of Directors and Senior Management of their branches and subsidiaries in countries outside the European Union. The MLCO of the Head Office/parent insurance company in

Cyprus, who has the main responsibility for the implementation of these Orders, should ensure that the branches and subsidiaries located in third countries have taken all the necessary measures to comply with these Orders in relation to customer identification, due diligence and record keeping procedures. Where the laws or regulatory requirements of the hosting country where the branches and subsidiaries are situated, differ from the requirements of the Law and these Orders, then the branches and subsidiaries shall apply the stricter requirements of the two, to the extent that the legislation/regulations of the hosting country permit.

Where the legislation/regulations of the third country do not permit the implementation of the requirements of these Orders and the said legislation/regulations do not require the implementation of equivalent measures and procedures, then the MLCO of the insurance company concerned should immediately inform of this fact the Superintendent of Insurance of Cyprus. In addition, the insurance company should take additional measures to effectively manage the enhanced risk of money laundering and terrorist financing which emanates form the above deficiency.

3. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT

3.1 Obligation to establish procedures to prevent money laundering (Article 58 of the Law)

The Law requires all persons carrying on financial or other business, to establish and maintain specific policies and procedures to guard against their business and the financial system in general being used for the purposes of money laundering. In essence these procedures are designed to achieve two purposes: firstly, to facilitate the recognition and reporting of suspicious transactions and, secondly, to ensure through the strict implementation of the "know-your-customer" principle and the maintenance of adequate record keeping procedures, should a customer come under investigation, that the insurance companies and intermediaries are able to provide its part of the audit trail. The Law requires that all persons engaged in financial or other business to establish

appropriate systems and procedures in relation to the following:

a) Customer identification and due diligence.

b) Record keeping.

c) Internal reporting and reporting to MOKAS.

d) Internal control, assessment and management of risk with the purpose of preventing money laundering and terrorist financing.

e) The detailed examination of any transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering or the financing of terrorism, and particularly of the sophisticated, complex and unusually large transactions and all unusual types of transactions that are realised without obvious economic or explicit legal reason.

f) Explicit procedures and standards of recruitment and valuation of new employees' integrity are applied.

g) Employees awareness with regard to the

   i. systems and procedures for the prevention of money laundering and terrorist financing,

   ii. the Law,

   iii. the Orders issued by the competent Supervisory Authority, and

   iv. the European Union's Directives with regard to the prevention of the use of the financial system for the purposes of money laundering and terrorist financing.

h) The regular training of staff to recognise and handle suspicious transactions and activities which may be related to money laundering or terrorist financing offences.

In this regard, training provided by insurance companies/intermediaries to their employees should include the provision of education on the latest developments

in anti money laundering and terrorist financing including the practical methods and trends used by criminals for this purpose.

3.2 When to apply customer identification and due diligence procedures (Article 60 of the Law)

Article 60 of the Law requires persons carrying financial or other business to apply customer identification and due diligence procedures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of transaction;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information previously collected for the customer identification.

According to Article 63(2) of the Law, insurance companies/intermediaries may apply simplified due diligence and customer identification procedures provided that the risk for money laundering and terrorist financing is low and there is no suspicion for money laundering or financing of terrorism, in the cases of sub-paragraphs (a), (b) and (d) above in respect of:

(a) life insurance policies where the annual premium is no more than euro 1.000 or the singe premium is not more than euro 2.500;

(b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

It is noted that insurance companies/intermediaries should establish to their satisfaction that they are dealing with a real person (natural or legal) and obtain sufficient evidence of identity to establish that a prospective policy holder is who he/she claims to be. The verification procedures necessary to establish the

identity of the prospective policyholder should be based on reliable data, documents and information issued or obtained from independent reliable sources, i.e. those data, documents and information that are the most difficult to amend or obtain illicitly. Certified true copies of the identification evidence should always be retained by the insurance companies and/or intermediaries and kept in customers' files. If customers' files are kept at insurance company's' premises then intermediaries are responsible to submit all relevant identification data to the insurance company. However, it must be appreciated that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

3.3 How to exercise customer identification and due diligence (Article 61 of the Law)

Article 61 of the Law provides that the customer identification and due diligence procedures, comprise the following:

(i) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(ii) Identifying the beneficial owner, as described in article 2 of the Law, and taking risk-based and adequate measures to verify his identity based on documents, data or information issued or obtained from an independent, reliable source so that the person carrying on financial or other business is satisfied that knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

The Law (article 2) defines the term beneficial owner as being the natural person or the natural persons who ultimately own or exercise control over a customer.
a) in the case of corporate entities:

- *the natural person or natural persons who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including*

through bearer share holdings a percentage of 10 % plus one share shall be deemed sufficient to meet this criterion;

- *the natural person or natural persons who otherwise exercise control over the management and direction of a legal entity:*

(b) in the case of legal entities, such as foundations and legal arrangements, such as trusts, which administer and distribute funds:

- *where the future beneficiaries have already been determined, the natural person or natural persons who are the beneficiaries of 10 % or more of the property of a legal arrangement or entity;*

- *where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;*

- *the natural person or natural persons who exercise control over 10% or more of the property of a legal arrangement or entity;*

(iii) Obtaining information on the purpose and intended nature of the business relationship;

(iv) Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

It is noted that the Law provides that persons carrying on financial and other business, maintain customer identification and due diligence procedures but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, product or transaction. However, the persons engaged in financial and other business must be able to demonstrate to

the competent supervisory authorities that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

3.3.1 Construction of a customer's business profile

The Insurance Company must be satisfied that it's dealing with a real person and, for this reason, should obtain sufficient evidence of identity to verify that the person is who he claims to be.

The verification of the customer's identification is based on reliable data and information issued or obtained from independent and reliable sources.

A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its verification should be followed.

Without prejudice to the provisions of section 62(2) of the Law, the data and information that are collected before the establishment of the business relationship, with the aim of constructing the customer's economic profile and, as a minimum, include the following :

(a) the purpose and the reason for requesting the establishment of a business relationship;

(b) the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations.

3.3.2 Specific Identification Issues

1. Prospective policyholders permanently residing in Cyprus

The following identification information should be obtained:-

(a) Name of the prospective policyholder;
(b) Residential address;
(c) Telephone and fax numbers;
(d) E-mail address;
(e) Date and place of birth;

(f) Profession or occupation of the customer including the name of employer/business organization;

(g) Annual income

The name used should be verified by reference to a document obtained from a reliable and reputable source which bears a photograph. A current valid full passport, or a national identity card should be requested and the relevant number should be registered. Having been satisfied that the original identification document/s has been presented, insurance companies should obtain a copy.

In addition to the name verification, it is vital that the current permanent address should also be verified by:

- requesting sight of a recent utility bill (e.g. electricity, water, local authority tax bill or/and an insurance company statement (to guard against forged or counterfeit documents care should be taken to check that the documents offered are originals); or

2. Prospective policyholders not permanently residing in Cyprus

For prospective policyholders who are not normally residing in Cyprus, it is important that, verification procedures similar to those applied for clients permanently residing in Cyprus should be carried out and the same information obtained.

In addition, insurance companies and intermediaries are advised, if in any doubt, to seek to verify identity with a reputable financial institution in the client's country of residence.

In addition to the aim of preventing money laundering and terrorist financing, the above information is also essential for implementing the financial sanctions imposed against various persons by the United Nations

and the European Union. In this regard, passport's number, issuing date and country as well as the customer's date of birth should always appear on the copies of documents obtained, so that the insurance company/intermediary would be in a position to verify precisely whether a customer is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union on the basis of a United Nations Security Council's Resolution and a Regulation or a Common Position of the European Union's Council respectively.

3. Corporate clients

Because of the difficulties of identifying beneficial ownership, transactions on behalf of corporate clients (e.g. group policies), before a business relationship is established, when the company is not known, measures should be taken by way of a company search and/or other commercial enquires to ensure that the applicant company has not been, or is not in the process of being dissolved, struck off, wound-up, terminated. In addition, if changes to the company structure of ownership occur subsequently, or suspicions are aroused by a change in the profile of the business carried out by the company, further checks should be made.

In the cases where transactions are made for the benefit of locally or foreign incorporated companies, the insurance company/intermediary should ascertain the following:

(a) Registered number and date of incorporation;

(b) Registered corporate name and trading name used;

(c) Registered office address;

(d) Full addresses of the Head office/principal trading offices;

(e) Telephone numbers, fax numbers and e-mail address;

(f) The members of the board of directors;

(g) The persons that are duly authorised to represent and act on behalf of the company.

(h) The beneficial owners of private companies and public companies that are not listed in a recognised Stock Exchange of the European Union or a third country with equivalent disclosure and transparency requirements.

(i) The registered shareholders where they act as nominees of the beneficial owners.

(j) The business profile of the company in terms of the natural and scale of its activities.

The insurance company/ intermediary should verify the identity of the person(s) authorized to represent the company, the registered shareholder(s) and the beneficial owner(s) and, in addition, obtain the original or certified copies of the following documents relating to a locally incorporated company:

(i) The Certificate of incorporation;
(ii) The Memorandum and Articles of Association;
(iii) A resolution of the Board of Directors conferring authority to any persons to make transactions and represent the company;
(iv) Certificate of Directors and Secretary;
(v) Certificate of registered address;
(vi) Certificate of registered shareholders.
(vii) In the cases where the registered shareholders act as nominees of the beneficial owner(s), a copy of the trust deed/agreement concluded between the nominee and the true beneficiary of the account, by virtue of which the registration of the shares on the nominee's name on behalf the beneficiary has been agreed.

For companies incorporated outside Cyprus, insurance companies/intermediaries should request and obtain documents similar to the above.

- Nominees or agents of third persons

Article 65(1) of the Law provides that persons carrying on financial or other business shall take reasonable measures to obtain adequate documents, data or information for the purpose of establishing the identity of any third person on whose behalf the customer is acting.

As a result of the above, insurance companies/intermediaries should take all necessary measures for the purpose of verifying and establishing the identity of the persons on whose behalf and for their benefit a nominee or agent is acting, that is, to ascertain the identity of the real beneficiaries of a life policy. For this purpose, insurance companies/intermediaries should always obtain a copy of the authorisation agreement that has been concluded between the interested parties.

3.3.3 Renewal of customer identification

Customer identification and due diligence procedures must be applied not only to new customers but also at appropriate times to existing customers, depending on the level of assessed risk of the customer being involved in money laundering or terrorist financing offences.

Insurance companies need to ensure that customer identification records remain up-to-date and relevant throughout the business relationship. In this respect, an insurance company/ intermediary must undertake, on a regular basis, or whenever there are doubts about the veracity of the identification data, reviews of existing records, especially for high-risk customers. If, as a result of these reviews, at any time throughout the business relationship, the insurance company/ intermediary becomes aware that it lacks sufficient information about an existing customer, it should take all necessary action to obtain the missing information and identification data as quickly as possible.

In addition to the requirement for the update of the customer identification data and information on a regular basis or when it is observed that unreliable or

inadequate data and information are being held, insurance companies should check the adequacy of the data and information held with regard to the customer's identity and business/economic profile, whenever one of the following events or incidents occurs:

(1) An individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the business/economic profile of the customer.

(2) There is a material change in the customer's legal status and situation, such as :

(i) Change of director(s)/ secretary;

(ii) Change of registered shareholder(s) and/or beneficial owner(s);

(iii) Change of registered office;

(iv) Change of trustee(s);

(v) Change of corporate name and/or trading name(s) used; and

(vi) Change of the principal trading partners and/or assumption of new major business activities.

(3) There is a material change in the way the account operates, such as :

- Change in the person(s) that are authorised to operate the account(s); and
- Application for the opening of new account(s) or the provision of new insurance product.

If a customer fails or refuses to submit, within a reasonable timeframe, the required data and identification information for the updating of his/her identity and business/economic profile and, as a consequence, the insurance company is unable to comply with the customer identification requirements set out in the Law and this Directive, then the insurance company should terminate the business relationship and close all the accounts of the customer concerned while at the same time it should examine whether it is warranted under the circumstances to submit a report of suspicious transactions/activities to MOKAS.

3.4 Reliance on third parties for customer identification and due diligence

The Law defines as third person a credit or financial institution or auditors or independent legal professional or trust and company service providers situated in the European Economic Area, and who:

(i) are subject to mandatory professional registration, recognized by law and

(ii) are subject to supervision with regard to their compliance with the requirements of the European Union Directive.

Article 67 of the Law permits persons carrying on financial or other business to rely on third parties for the implementation of customer identification and due diligence procedures, as these are prescribed in article 61(1) (a), (b), (c) of the Law.

The Law (article 67) explicitly provides that the ultimate responsibility for performing the above mentioned measures and procedures remains with the insurance company/ intermediary or the other person who carries on the financial or other business which relies on the third person. Consequently, the obligation to apply customer identification and due diligence procedures can not be delegated to the third person.

Furthermore, the Law provides that the third persons could be any person carrying on financial activities or auditors or independent legal professional or trust and company service provides operating in countries outside the European Economic Area which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures and measures for the prevention of money laundering and terrorist financing equivalent to those laid down in the European Union Directive.

The Law provides that, in the case that an insurance company / intermediary chooses to rely on a third person, it must require from the third person to:

(i)make immediately available customer identification data, information and

documents collected in the course of applying customer identification and due diligence procedures in accordance with the requirements of the Law; and

(ii) Immediately forward to the insurance company/ intermediary relevant copies of the customer identification documents, data and information on the customer and the beneficial owner which the third person collected while applying the abovementioned procedures.

All copies of identification documents, data and information obtained by an insurance company/ intermediary should be duly certified by the third person as true copy of the original. It is noted that insurance companies may rely on third parties only at the outset of establishing a business relationship for the purpose of ascertaining and verifying the identity of their customers. Insurance companies and intermediaries, according to the degree of risk may obtain any additional data and information they consider necessary.

Moreover, the insurance company/ intermediary should obtain data and information so as to verify that the third person is subject to professional registration in accordance with the competent law of its country of incorporation and/ or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.

3.5 Timing of implementation of customer identification and due diligence procedures (Article 62 of the Law)

Article 62(1) of the Law requires that the verification of the identity of the customer and the beneficial owner is performed before the establishment of a business relationship or the carrying out of the transaction.

As a rule, insurance companies and intermediaries are expected to seek and obtain satisfactory evidence of identity of their prospective clients prior to the conclusion of a contract.

By derogation to the above, article 62(2)&(**3**) allows the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the

normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

The identification and verification of the identity of the beneficiary under the policy may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under policy.

The Law explicitly requires that in situations where the person carrying on financial or other business is unable to comply with the customer identification and due diligence procedures then it may not carry out a transaction, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider making a report to MOKAS in accordance to articles 27 and 69 of the Law.

3.6 Enhanced due diligence procedures (Article 64 of the Law)

Article 64 of the Law requires persons carrying on financial or other business to apply enhanced customer identification and due diligence measures in the following situations:

3.6.1 Non-face to face customers

Where a customer is not physically present to verify his identity one or more of the following measures are applied:

(i) Obtain from the customer additional documentary evidence, data or information; or

(ii) Take supplementary measures to verify or certify the documents supplied or requiring confirmatory certification by a credit or financial institution covered by the European Union Directive.

(iii) Ensure that the first payment is made through an account which has been opened in the name of the customer by a credit institution which operates in a country of the European Economic Area.

Whenever a customer requests to purchase an insurance product, the insurance company should preferably hold a personal interview during which all information for customer identification should be requested and obtained. It is possible, however, that a customer, especially a non-resident, may request an insurance product through mail, telephone, or the internet without presenting himself for a personal interview. In such a case, insurance companies must follow the established customer identification and due diligence procedures, as applied for customers with whom they come in direct and personal contact and obtain exactly the same information and documents. However, due to the difficulty in matching the customer with the collected identification data, insurance companies should apply enhanced customer identification and due diligence measures as required by the Law and this Directive so as to effectively mitigate the risks associated with such a business relationship.

Practical procedures that can be applied for the purpose of implementing measures (i) and (ii), referred to in article 64(1) of the Law for the purpose of mitigating the higher risk involved in non-face to face customers, are the following:

(i) Direct confirmation of the prospective customer's true name, address and signature from his country of origin;

(ii) Obtaining a reference letter from a third person (as the latter is defined in article 67 of the Law);

(iii) The customer supplies the insurance company with the original customer identification documents e.g. passport, identity card, which are subsequently returned by registered and secured mail;

(iv) Telephone contact with the customer at his residence or office, before the commencement of the insurance policy, on a telephone number which has been verified from an independent source;

(v) Contact with the customer through mail in an address previously verified from independent and reliable sources.

It is pointed out that the same requirements prescribed in article 64(1) (a) of the Law and this Directive are applied for companies or other legal

persons requesting an insurance policy through mail, telephone or internet. Insurance companies should take additional measures for ensuring that the company or legal entity operates at the address of its trading office and carries out legitimate business activities.

3.6.2 Accounts in the name of trusts

The Law requires that insurance companies should establish that a person acting on behalf of a company or a legal arrangement such as trust is appropriately authorized for that purpose and his identity is ascertained and verified.

Trusts do not form a separate legal entity and, therefore, a business relationship is established with the trustees who act on behalf of the trust. Consequently, trustees together with the trust should be considered as the insurance companies' customers. When insurance companies enter into such relationships, they must ascertain the legal substance of the trust, and its name and date of establishment, and verify the identity of the settlers, trustees and true beneficiaries.

Furthermore, insurance companies should ascertain the nature of activities and purpose of establishing the trust as well as the source and origin of funds requesting sight of the relevant extracts from the trust deed as well as obtaining other relevant information from the trustees. All relevant details and information should be recorded and kept in the customers file.

3.6.3 Politically Exposed Persons

The Law (Article 2) defines that politically exposed persons means the natural persons and who are or have been entrusted with prominent public functions in the Republic of Cyprus or any Other Country, and their immediate family members or persons known to be close associates, of such persons.

In respect of transactions or business relationships with politically exposed persons carrying on financial or other business are required to:

(i) have appropriate risk-based procedures to determine whether the

customer or the beneficial owner is a politically exposed person and/or in the case of beneficial owner;

(ii) have Senior Management approval for establishing business relationships with such customers or for the continuation of such a relationship with existing customers who have subsequently become politically exposed persons;

(iii) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(iv) conduct enhanced ongoing monitoring of the business relationship.

Business relationships with individuals holding important public positions in a foreign country and with natural or legal persons closely related to them, may expose an insurance company to enhanced risks, especially, if the potential customer seeking to establish an insurance policy is a PEP, a member of his immediate family or a close associate that is known to be associated with a PEP. Insurance companies should pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering statutes and regulations are not equivalent with international standards. In order to manage effectively such risks, insurance companies should assess which countries with which they maintain business relationships are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the Financial Action Task Force (see Section 3.6.4 of this Directive). With regard to the issue of corruption one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the web-site of Transparency International at www.transparency.org. With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, insurance companies may retrieve information from the country assessment reports prepared by FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) the International Monetary Fund and the World Bank.

For the purpose of this Directive, PEPs, include the following natural

persons:

(i) natural persons who have, or had a prominent public function in a foreign country:

1. heads of State, heads of government, ministers and deputy or assistant ministers;

2. members of parliaments;

3. members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

4. members of courts of auditors or of the boards of central banks;

5. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

6. members of the administrative, management or supervisory bodies of State-owned enterprises.

None of the categories set out above shall be understood as covering middle ranking or more junior officials.

(ii) “Immediate family members ” of PEPs include the following persons:

1. the spouse;

2. any partner considered by national law as equivalent to the spouse;

3. the children and their spouses or partners;

4. the parents.

(iii) Persons known to be “close associates” of a politically exposed person include the following:

1. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a person referred to in subparagraph (i) above.

2. any natural person who has sole beneficial ownership of a legal entity (company) or legal arrangement (trust) which is known to have been set up for the benefit de facto of the person referred to in subparagraph (i) above.

Without prejudice to the application, on a risk sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning described above, for a period of at least one year, insurance companies shall not be obliged to consider such a person as politically exposed.

Insurance companies should adopt, further to the above legal requirements, the following additional 'due diligence' measures, when they have a new policy and/or establish a business relationship with a PEP:

(i) Put in place appropriate risk management procedures to enable them to determine whether a prospective customer is PEP. Such procedures should include, depending on the degree of risk each insurance company faces, the acquisition and installation of a reliable commercial electronic database for PEPs which is available on the market, seeking and obtaining information from the customer himself or from publicly available information which, inter-alia, can be retrieved from the internet. In the case of companies, legal entities and arrangements, the procedures should aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the company constitute PEPs. In case of identifying one of the above as a "Politically Exposed Person", then automatically the account of the company, legal entity or arrangement should be subject to the procedures stipulated in the Law and this Directive.

(ii) The decision for establishing a business relationship with a PEP should be taken by the insurance company's management. When establishing a business relationship with a customer (natural or legal) and subsequently it is ascertained that the person(s) involved are or have become PEPs, then the approval of the insurance company's Management should be given for continuing the operation of the business relationship and/or insurance policy account.

(iii)Before establishing a business relationship with a PEP, the insurance company should obtain adequate documentation to ascertain not only his/her identity but also to assess his/her business reputation (e.g.

references from third parties);

(iv) Insurance Companies should establish the business profile of the policyholder's account by obtaining the information prescribed in Section 3.3 above. The profile of the expected business activity should form the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. Insurance companies should be particularly cautious and most vigilant where their customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks; and

(v) The policyholder's account should be subject to annual review in order to determine whether the specific life insurance policy will continue to be inforce. A note should be prepared summarising the results of the review by the insurance officer. The note should be submitted for consideration and approval to the insurance company's Management and filed in the customer's personal file.

3.6.4 Customers from countries which do not adequately apply FATF's recommendations

The Financial Action Task Force's ("FATF") 40+9 Recommendations constitute today's primary internationally recognised standards for the prevention and detection of money laundering. The Government of Cyprus has formally endorsed FATF's Forty Recommendations and has directly assured the President of the FATF that the competent authorities of Cyprus will take all necessary actions to ensure full compliance and implementation of the Recommendations. In this regard, the Insurance Companies Control Service is committed for the implementation of FATF's 40+9 Recommendations and all its other related initiatives in an effort to reduce the vulnerability of the insurance company system to money laundering and terrorist financing activities.

In this respect, insurance companies are required to apply the following:

1. Exercise additional monitoring procedures and pay special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or they apply inadequately the aforesaid Recommendations.
2. Whenever the above transactions have no apparent economic or visible lawful purpose, their background and purpose should be examined and the findings established in writing. If an insurance company cannot satisfy itself as to the legitimacy of the transaction, then a suspicious transaction report should be filed through the MLCO with MOKAS.

With the aim of implementing the above, the MLCO should obtain and study the country assessment reports prepared by FATF (http://www.fatf-gafi.org), the other regional bodies that have been established and work on the principles of FATF (e.g. Moneyval Committee of the Council of Europe www.coe.int/moneyval), the International Monetary Fund and the World Bank. Based on the said reports, the risk from transactions and business relationships with persons from various countries must be assessed and, when deemed necessary, enhanced due diligence measures should be applied for identifying and monitoring transactions of persons from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing. In this regard, the MLCO should decide on the countries that appear not to adequately apply FATF's Recommendations and for which enhanced due diligence measures should apply for business relationships and transactions originating from those countries.

In addition the Law provides that enhanced due diligence measures should be applied in other situations as well, which by their nature present a higher risk of money laundering or terrorist financing.

3.7 Simplified customer due diligence and identification procedures (Article 63 of the Law)

Article 63(1) of the Law provides that persons carrying out financial or other business activities may apply simplified due diligence and identification processes in the following instances, provided that the risk for money

laundering and terrorist financing is low and there is no suspicion for money laundering or financing of terrorism:

(i). Credit or financial institutions situated in the European Economic Area.

(ii). Credit or financial institutions carrying out one or more of the financial activities as these are defined in article 2 of the Law which is incorporated in a country outside the European Economic Area and which:

- according to a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it imposes requirements equivalent to those laid down in the European Union Directive, and
- is under supervision for compliance with the said requirements.

(iii). Listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or a third country which is subject to disclosure requirements consistent with Community legislation;

(iv). Domestic Public authorities of the countries of the European Economic Area.

It is further provided that in the business relationships mentioned in paragraphs (i) to (iv) above, persons carrying out financial or other business activities, may not apply customer identification procedures on the customer or, where applicable, the beneficial owner, neither collect information in relation to the purpose and intended nature of the business relationship or may not verify the identity of the policyholder and beneficial owner after the establishment of a business relationship or the execution of an occasional transaction. Irrespective of the above, the persons carrying out financial or other business activities are obliged to conduct ongoing monitoring of the business relationships referred to in paragraphs (i) to (iv) above in accordance with the provisions of paragraph (d) of subsection (1) of article 61 and reports to MOKAS cases of or attempts to perform suspicious transactions.

Irrespective of the above, the Law requires that insurance companies and

intermediaries should in any case gather sufficient information to establish whether the customer qualifies for an exemption as mentioned above.

3.8 Powers of MOKAS to order the non-execution or delay in the execution of a transaction (Article 26(2)(c) of the Law)

Article 26(2) (c) of the Law empowers MOKAS to give instructions to financial institutions and professionals for the non-execution or the delay in the execution of a transaction. All the above, are required to promptly comply with such instructions and provide MOKAS with all necessary co-operation. It is noted that, as per the above Article, in such a case no breach of any contractual or other obligation may arise and insurance companies and intermediaries are, therefore, protected from any possible claims from their customers.

3.9 Record Keeping Procedures

Article 68(1) of the Law requires persons carrying financial or other business to retain records and keep for a period of at least five years the following documents:

(i) Copies of the customer identification evidence;

(ii) The relevant evidence and details of all business relationships and transactions, including documents for the recording of transactions in the accounting books; and

(iii) The relevant documents and correspondence with customers and other persons with whom a business relationship is maintained.

The prescribed period of five years commences with the date on which the transactions were completed or the business relationship terminated.

Copies of the customers' identification evidence should be certified by the insurance company's / intermediary's employee who verifies the identity of the customer or the third person on whom the insurance company/

intermediary relies for the purpose of customer identification and due diligence procedure.

Persons carrying on financial or other business must ensure that all the above documents are promptly and without any delay made available to MOKAS and the competent Supervisory Authorities for the purpose of discharging their legal duties.

Moreover, insurance companies and intermediaries must apply appropriate systems which will enable them to promptly identify and inform the Superintendent of Insurance and MOKAS as to whether they maintain or have maintained, during the previous five years, a business relationship with specified natural or legal persons and on the nature of that business relationship.

MOKAS needs to be able to compile a satisfactory audit trail of illicit money and be able to establish the business profile of any account and customer under investigation. To satisfy this requirement, insurance companies and intermediaries must ensure that in the case of a money laundering investigation by MOKAS, they will be able to provide the following information:

(i) The identity of the policy holder(s);

(ii) The identity of the beneficial owner(s);

(iii) The value and volume of premiums or number of policies;

(iv) For selected policy(ies):

  (a) The origin of the funds;

  (b) The type and amount of the currency involved;

  (c) The form in which the funds were placed or withdrawn i.e. cash, cheques, wire transfers etc.;

(d) The identity of the person undertaking the transaction;

(e) The form of instructions and authority.

3.10 Format of records

It is recognized that copies of all documents cannot be retained indefinitely. Prioritization is, therefore, a necessity. Although the Law prescribes a period of retention, where the records relate to on-going investigations, they should be retained until it is confirmed by MOKAS that the case has been closed.

The retention of hard-copy evidence of identity, transactions, business correspondence and other details comprising a customer's business profile creates excessive volume of records to be stored. Therefore, retention may be in other formats other than original documents, such as electronic or other form. The overriding objective is for the insurance companies to be able to retrieve the relevant information without undue delay.

When setting a document retention policy, insurance companies are, therefore, advised to consider both the statutory requirements and the potential needs of MOKAS.

Section 47 of the Law provides that where relevant information is contained in a computer, the information must be presented in a visible and legible form which can be taken away by MOKAS.

3.11 Internal Audit Unit

The Internal Audit Unit, of the insurance company/intermediary or the official designated to perform internal control inspection functions should review, test and evaluate, on a regular basis, the procedures and controls applied for the prevention of money laundering and terrorist financing and verify the level of compliance with the present Orders and the Law. Insurance companies/intermediaries should implement explicit procedures and standards of recruitment so as to ensure that new employees are of high

integrity and honesty.

3.12 Recruitment Procedures

Insurance companies/intermediaries should implement explicit procedures and standards of recruitment so as to ensure that new employees are of high integrity and honesty.

4. INTERNAL REPORTING PROCEDURES

4.1 Appointment of a Money Laundering Compliance Officer ("MLCO")*

Article 69(1) of the Law requires persons carrying on financial and other business to apply the following internal reporting procedures:

(i) Appoint a senior staff member who has the ability , knowledge and the expertise on financial and other business activities, according to each case, known as the MLCO to whom a report is to be made about any information or other matter which comes to the attention of the person handling financial or other business and which, in the opinion of the person handling that business, proves or creates suspicion that another person is engaged in money laundering or terrorist financing;

(ii) Require that any such report be considered in the light of all other relevant information by the MLCO, for the purpose of determining whether

---

* *Note: Where the insurance intermediary is a physical person, he or she will undertake the responsibilities of the Money Laundering Compliance Officer (MLCO) mentioned in these Orders. As far as their training is concerned, they can rely on the assistance provided by the insurance companies they are co-operating with. This assistance can also be provided by the insurance companies to those intermediaries which are very small legal entities without enough resources.*

or not the information or other matter contained in the report proves this fact or creates such suspicion;

(iii) Allow the MLCO to have access to other information, records and details which may be of assistance to him/her and which is available to the person responsible for maintaining the said internal reporting procedures; and

(iv) Secure that the information or other matter contained in the report is transmitted to the Unit for Combating Money Laundering ("MOKAS") where the person who has considered the report under the above procedures ascertains or has reasonable suspicions that another person is engaged in a money laundering offence or terrorist financing or the transaction might be related to such activities.

Furthermore, the Law explicitly provides that the obligation to report to MOKAS includes also the attempt to execute such suspicious transactions.

The person appointed to the post of MLCO should belong to the Management of the insurance company / intermediary so as to command the necessary authority. Where it is deemed necessary due to the volume and/or the geographic spread of the insurance company's / intermediary's operations, insurance companies and intermediaries may appoint Assistant MLCOs by division, district or otherwise for the purpose of assisting the MLCO and passing internal suspicion reports to the Chief MLCO. In the light of the aforesaid, insurance companies and intermediaries should communicate to the Superintendent of Insurance, on a continuous basis, the name and position of the person whom they appoint, from time to time, to act as MLCO.

The Senior Management of insurance company must ensure that MLCO has sufficient resources, including competent staff and technological equipment, for the effective discharge of his/her duties.

The Money Laundering Compliance Officer, the Assistant Money Laundering Compliance Officers and other members of staff who have been assigned with the duty of implementing the adopted procedures for

the prevention of money laundering and terrorist financing, should have complete and timely access to all information concerning customers' identity, transactions' records and other relevant files and information maintained by the insurance company/intermediary so as to be fully facilitated in the effective discharge of their duties.

In addition all employees/intermediaries should be made aware of the person (Money Laundering Compliance Officer) to whom they should report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing activities.

4.2 Duties of the Money Laundering Compliance Officer

The role and responsibilities of the MLCO, including those of his Assistants, should be clearly specified by insurance companies and intermediaries and documented in the risk management and procedures manual for the prevention of money laundering and terrorist financing.

As a minimum, the duties of a MLCO should include the following:

(i) The MLCO has the primary responsibility, together with the insurance company's / intermediary's Senior Management, for establishing appropriate measures, systems and procedures for the due implementation of the Law and the Orders of the Superintendent of Insurance as well as for adherence to all other circulars/recommendations which are issued by the Superintendent of Insurance, from time to time, for the prevention of the use of the insurance company / intermediary system for money laundering and terrorist financing. In this regard, the MLCO has the primary responsibility for the preparation of the insurance company's / intermediary's risk management and procedures manual for the prevention of money laundering and terrorist financing which is submitted through the Senior Management to the Board of Directors for approval.

(ii) The MLCO monitors and assesses whether the policy, procedures

and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the MLCO should apply appropriate monitoring mechanisms (e.g. on-site visits to units/branches) which will provide him/her with all necessary information for assessing the level of compliance of the units /branches of the insurance company / intermediary with the procedures and controls which are in force. In the event that the MLCO identifies shortcomings and/or weaknesses in the application of the require procedures and controls, he/she should give appropriate guidance for the assumption of corrective measures.

(iii) The MLCO receives information from the insurance company's/ intermediary's employees which is considered by the latter to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. A specimen of such an internal report (hereinafter to be referred to as "Internal Money Laundering Suspicion Report") is attached, as "Appendix 1", to these Orders. All such reports should be registered and kept on a separate file.

(iv) The MLCO validates and considers the information received as per paragraph (iii) above by reference to any other relevant information and discusses the circumstances of the case with the reporting employee concerned and, where appropriate, with the employee's superior(s). The evaluation of the information reported to the MLCO should be made on a separate form which should be registered and retained on file. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Internal Evaluation Report") is attached, as "Appendix 2", to these Orders.

(v) If following the evaluation described in paragraph (iv) above, the MLCO decides to notify MOKAS, then he/she should complete a written report and submit it to MOKAS the soonest possible. A specimen of such a report (hereinafter to be referred to as "Money Laundering Compliance Officer's Report to MOKAS) is attached, as "Appendix 3", to these Orders. Reports can be submitted to MOKAS by post or facsimile or by hand. All such reports should be registered and kept on a separate file.

(vi) After the submission of the MLCO's report to the MOKAS, the transactions of the customer(s) involved are monitored by the MLCO.

(vii) If following the evaluation described in paragraph (iv) above, the MLCO decides not to notify MOKAS then he/she should fully explain the reasons for such a decision on the "Money Laundering Compliance Officer's Internal Evaluation Report" which should, as already stated, be registered and retained on file.

(viii) The MLCO maintains a registry with statistical information date of submission of the internal report, date of assessment, date of reporting to MOKAS) in relation to the Internal Money Laundering Suspicious Reports and the MLCO's reports to MOKAS.

(ix) The MLCO acts as a first point of contact with MOKAS, upon commencement of and during an investigation as a result of filing a report to MOKAS under (vi) above.

(x) The MLCO responds to requests from MOKAS and provides all the supplementary information requested and fully co-operates with MOKAS.

(xi) The MLCO ensures that all branches and subsidiaries of the insurance company / intermediary in non-EU countries have taken all necessary measures for achieving full compliance with the provisions of these Orders in relation to customer identification, due diligence and record keeping procedures.

(xii) The MLCO is responsible for the evaluation, on an annual basis, of all risks arising from existing and new customers, new products and updating and amending systems and procedures applied by the insurance company / intermediary for the effective management the aforesaid risks.

(xiii) The MLCO responds to all requests and queries from the Superintendent of Insurance and provides all relevant requested information.

(xiv) The MLCO and the Assistant MLCOs (if applicable) acquire the requisite knowledge and skills for the implementation of appropriate internal procedures for recognising, preventing and reporting transactions/activities suspected to be associated with money laundering

or terrorist financing.

(xv) The MLCO provides advice and guidance to other employees of the insurance company / intermediary on the correct implementation of procedures and controls against money laundering and terrorist financing.

(xvi) The MLCO determines which of the insurance company's/ intermediary's units/branches, staff and employees need further training and education for the purpose of money laundering and terrorist financing prevention and organises appropriate training sessions/seminars. In this regard, the MLCO prepares and applies, in co-operation with other departments of the insurance company / intermediary, an annual staff training program.

(xvii) The MLCO maintains full records of the seminars and other training offered to the insurance company's/ intermediary's employees and assesses the adequacy of the education/training provided.

(xviii) The MLCO assesses the systems and procedures applied by intermediaries on whom the insurance company / intermediary relies for customer identification and due diligence purposes and ensures that these adhere strictly to the insurance companies'/intermediaries' procedures.

4.3 Education and Training of Employees/Intermediaries

The effectiveness of the procedures and recommendations contained in this Directive and other relevant circulars of the Insurance Companies Control Service in relation to the prevention of money laundering and terrorist financing depends on the extent to which insurance company's employees/intermediaries appreciate the seriousness of the background which led to the enactment of the Law and the level of their education with regard to their duties and statutory obligations for countering this serious problem. It is reminded that an employee/intermediary can be personally liable for failure to report information, regarding money laundering and terrorist financing, in accordance with the internal reporting procedures. Consequently, staff of insurance companies must be encouraged to cooperate and report, without delay, anything that comes to their attention

in relation to transactions for which there is a slight suspicion that they are related to money laundering or terrorist financing. In this regard, it is crucial that insurance company establish complete measures to ensure that their staff is fully aware of their responsibilities and duties. In this regard, the MLCO has the responsibility, in cooperation with other competent units of the insurance company (i.e. the Personnel and Training departments etc), to prepare and implement, on an annual basis, an education and training programme for the staff as required by the Law and this Directive. As mentioned above, MLCO is required to evaluate the adequacy of the seminars and the training provided to the staff and maintain detailed data regarding the seminars/programmes carried out, such as:

- the number of lectures/seminars organised,
- their duration,
- the number of employees/intermediaries attending,
- the names and the qualifications of the instructors, and
- whether the lecture/seminar was organised internally or offered by an external organisation or consultants.

The timing and content of the training provided to staff of the various departments of the insurance company should be adjusted according to the needs of each insurance company. Furthermore, the frequency of training can vary depending on to the amendments of legal and/or regulatory requirements, staff duties as well as any other changes in the country's financial system.

The training programme should aim at educating staff on the latest developments in anti-money laundering and terrorist financing including the practical methods and trends used by criminals for this purpose.
The training programme should have a different structure for new staff, customer service staff, compliance staff, staff moving from one department to another or staff dealing with the attraction of new customers. Newly recruited staff should be educated in understanding the importance of preventive policies against money laundering and terrorist

financing and the procedures, measures and controls that the insurance company has in place for that purpose. Customers service staff who deals directly with the public should be trained on the verification of new customers' identity, the exercise of due diligence on an on-going basis, the monitoring of accounts of existing customer and the detection of patterns of unusual and suspicious activity. On-going training should be given at regular intervals so as to ensure that staff is reminded of its duties and responsibilities and kept informed of any new developments.

It is crucial that all members of staff directly involved in the anti-money laundering and terrorist financing preventive system fully understand the need to implement consistently policies and procedures for that purpose. In this regard, insurance companies should promote a culture and understanding among their staff with regard to the importance of the prevention and its key role to the successful implementation of the related policy and procedures.

4.4 Annual Report of the Money Laundering Compliance Officer

The MLCO has also the additional duty of preparing an Annual Report which is a significant tool for assessing the insurance company's level of compliance with its obligations laid down in the Law and the Insurance Company's Control Service Orders for the prevention of money laundering and terrorist financing.

(ii) The MLCO's Annual Report should be prepared two months from the end of each calendar year and should be submitted for consideration to the Board of Directors through the insurance company's Senior Management. In the case of an insurance company operating in Cyprus in the form of a branch, the Annual report should be submitted to the company's Board of Directors through the Senior Management of its country of origin.

(iii) The Board of Directors discuss and assesses the Annual Report. The Senior Management of the insurance company will take all appropriate action as deemed necessary under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

(iv) A copy of the Annual Report which is submitted to the Board of Directors must also be submitted at the same time to the Insurance Companies Control Service.

(v) The MLCO's Annual Report should deal with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, should cover the following:

- Information on changes in the Law and the Insurance Companies Control Service Orders which took place during the year and measures taken and/or procedures introduced for securing compliance with the above changes.
- Information on the number of inspections and reviews performed by the MLCO and the insurance company's Internal Audit Unit and the material deficiencies and weaknesses indentified in the insurance company's anti-money laundering and terrorist financing policies, procedures and controls. In this regard, the report should outline the seriousness of the issue, its risk implications and the recommendations made as well as the action taken for rectifying the situation.

- The number of internal money laundering suspicious reports submitted by the insurance company's employees to the MLCO and possible comments/observations thereon.
- The number of suspicious reports submitted by the MLCO to MOKAS with information of the main reasons for suspicion and highlights of any particular trends.
- The number of suspicious transactions reports which have been investigated by the MLCO and were not submitted to MOKAS.
- Information on circulars and other communication with staff on money laundering and terrorist financing preventive issues.
- Information on the policy, procedures and controls applied by the insurance company in relation to high risk customers as well as the number and countries of origin of high risk policyholders with whom a business relationship is established.

(vi)Information on the training courses/seminars attended by the compliance officer and any educational material received.

(vii)Information on training/education and any educational material provided

to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants.

5. EXAMPLES OF ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING OPERATIONS AND OTHER IMPORTANT ADVICE

The following examples may be indicators of a suspicious transaction report, however it must be noted that the list is not exhaustive.

- **Large Sum of Premiums**

Life insurance companies and intermediaries should be particularly cautious when clients are asking to conclude a single premium life insurance contract with a large sum of premiums paid in cash. It is commonly accepted that in the insurance sector the single premium policies can more easily be used for money laundering purposes. Therefore, life insurance companies and intermediaries are encouraged to be particularly cautious when the single premium is greater that the annual salary of the client and even more cautious in cases of cancellations of those policies before maturity.

- **Return Premiums**

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- a number of proposals entered into by the same insurer/intermediary for small amounts and then cancelled at the same time.
- return premium being credited to an account or person different from the original account/ person
- requests for return premiums in currencies different to the original premium.

- **Overpayment of premiums**

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or business as well as an illegal enterprise. In this method, the launderer may arrange for insurance of legitimate assets and "accidentally", but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums has been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say €1.000 or equivalent)
- the request to refund the excess premium was to a third party
- the assured is in a jurisdiction associated with money laundering and
- where the size or regularity of overpayments is suspicious
- reinstatement of contracts with high sums assured.

- **Additional Indicators of suspicious transactions**

- Application for a policy from a potential client in a distant place where a comparable policy could be provided "closer to home".
- Any request of information or delay in the provision of information to enable verification to be completed.
- The client accepts very unfavorable conditions unrelated to his or her health or age
- Large funds flows through non-resident accounts with intermediary firms
- The client requests an insurance product that has no discernible

purpose and is reluctant to divulge the reason for the investment.

- Insurance policies with values that appear to be inconsistent with the client's insurance needs and means.
- The client conducts a transaction that results in a conspicuous increase of investment contributions
- The applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency
- The applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

➢ **Important advice to insurance companies**

Insurance companies should be extremely cautious in the following cases:

- When designing new products, the insurance companies should take into consideration whether the particular product can be used for money laundering.
- Insurance companies and intermediaries should encourage their clients not to pay their premiums in the form of cash. They should, also, include certain provisions in their contracts, for the payment of extra amounts, especially when those are in cash.
- To avoid any misuse of the claims payment procedure, the insurance companies and intermediaries are advised to make the payments of the relative amounts only through insurance company / intermediary transfers and not make any cash or cheque payments. The name of the insurance company account holder always has to match with the authorized receiver of the money.

APPENDIX 1

INTERNAL MONEY LAUNDERING SUSPICION REPORT

REPORTER

Name: .....Tel

Branch/Dept.....Fax

Position.....

E-mail.....

CUSTOMER

Name:

Address:

Date of birth

Contact/Tel/Fax/E-mail .....Occupation/Employer

Details on employer:

Passport No.....Nationality

ID Card No.....Other ID

INFORMATION/SUSPICION

Brief description of activities/transaction

Reason(s) for suspicion

REPORTER'S SIGNATURE .....**Date**

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

Date received ..... Time received ..... Ref

MOKAS Advised Yes/No Date..... Ref

APPENDIX 2

MONEY LAUNDERING COMPLIANCE OFFICER'S

INTERNAL EVALUATION REPORT

Reference ..... Customer....

Reporter..... Branch/Dept.

ENQUIRIES UNDERTAKEN (Brief description)

DOCUMENTS RESEARCHED/ATTACHED

DETERMINATION/DECISION

FILE REFERENCE

MONEY LAUNDERING
COMPLIANCE OFFICER'S Signature..... ……Date

APPENDIX 3

MONEY LAUNDERING COMPLIANCE OFFICER'S REPORT TO THE UNIT FOR COMBATING MONEY LAUNDERING ("MOKAS")

I. GENERAL INFORMATION

Name of financial institution:

Date when a business relationship started or "one – off" transaction was carried out:

Type of policy(s) and number(s):

II. DETAILS OF NATURAL PERSON(S) AND/OR LEGAL ENTITY(IES) INVOLVED IN THE SUSPICIOUS TRANSACTION(S)

(A) NATURAL PERSONS

Name(s):

Beneficial owner(s) of the policy(ies):

Residential address(es):

Business address(es):

Occupation(s) and Employer(s):

Nationality and passport number(s):

(B) LEGAL ENTITIES

Company's name, country and date of incorporation:

Business address:

Main activities: