

Prevention of Money Laundering and Terrorist Financing

Directive to the Members of the CBA



CYPRUS BAR ASSOCIATION

Date of issue:	September2015 July 2014 August 2013
Contact details:	AMLDepartment Cyprus Bar Asasociation Florinis 11, Offices 101 & 202 1065 Nicosia Tel. 22873300 Fax. 22873013 Email: amldep@cybar.org.cy

CYPRUS BAR ASSOCIATION

Prevention of Money Laundering and Terrorist Financing

Directive to the Members of the CBA

by virtue of Section 59(4) of the Prevention and Suppression of Money
Laundering Activities Law of 2007

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

PREFACE

This Directive is issued by the Council of the Cyprus Bar Association appointed by the Council of Ministers on 7 March 2001 as the Supervisory Authority for lawyers in accordance with section 59(4) of the Prevention and Suppression of Money Laundering Activities Law of 2007 (L188(I)/2007) as amended in 2010, 2012 and 2013.

The Directive pertains to the Law 188(I)/2007 and professional requirements in relation to the avoidance, recognition and reporting of money laundering and terrorist financing activities. It is based on the aforementioned Law and creates the obligation and responsibilities for implementation by professionals, including lawyers, auditors and external accountants, of anti-money laundering and anti-terrorist financing measures.

The present Directive will be cited as the Directive for the “Prevention of Money Laundering and Terrorist Financing: Directive to the members of the CBA”, August 2013, 3rd edition, which replaces the members’ Directive “Prevention of Money Laundering and Terrorist Financing, February 2009”, 2nd edition.

August 2013

TABLE OF CONTENTS

	Paragraph
1. BACKGROUND	
Interpretation of basic terms	1.01
Introduction	1.03
What is money laundering?	1.04
Stages of money laundering	1.06
Vulnerability of lawyers to money laundering or terrorist financing	1.09
Responsibilities of the Council of the Cyprus Bar Association	1.10
Scope of this Directive	1.14
Members employed outside practice	1.19
2. THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007	
Introduction	2.01
Prescribed offences	2.02
Money laundering or terrorist financing offences	2.03
Predicate offences including offences of terrorist financing	2.07
Failure to report	2.09
Tipping - off	2.10
Prescribed activities and services	2.11
Procedures to prevent money laundering or terrorist financing	2.12
Supervisory Authorities	2.14
Privileged Information	2.20
Orders for disclosure of information	2.21
Terminology	
Criminal conduct	2.22
Knowledge	2.25
Reasonable excuse	2.26
Suspicion	2.27
Obligations to clients and third parties:	
Client confidentiality	2.31
Constructive trust	2.32
Disclosure of information to third parties	2.34
3. RISK BASED APPROACH FOR CLIENTS	
Introduction	3.01
Identification, recording and evaluation of risks	3.05
Country/Geographic risk	3.07
Client risk	3.08
Service risk	3.09
Controls for Higher Risk Solutions	3.11
Monitoring and improving the effective operation of lawyers' internal procedures.	3.12

4.	INTERNAL CONTROLS, PRINCIPLES AND PROCEDURES	
	Responsibilities and compliance	4.01
	Recommended procedures to comply with the Law	4.03
	Overseas offices and associated firms	4.06
5.	IDENTIFICATION PROCEDURES	
	Statutory requirements	5.01
	Introduction - "Know your client"	5.02
	The basic identification requirement	5.07
	When must an identity be verified?	5.11
	Identification procedures: exemptions	5.17
	Clients from countries whose legislation is ineffective	5.21
	<u>Due Diligence for individuals:</u>	
	Evidence of identity	5.24
	Non-Cypriot residents	5.26
	<u>Due Diligence for legal persons and legal arrangements :</u>	5.29
	Companies and partnerships	5.30
	Information which verifies the identity for legal persons	5.34
	Trusts (including occupational pension schemes) and nominees	5.40
	Information which verifies the identity for legal arrangement	5.41
	Clubs, societies and charitable institutions	5.45
	Local authorities and other public bodies	5.46
	Politically Exposed Persons (PEPs)	5.47
	Non-execution or delay in executing a transaction	5.49
6.	RECORD-KEEPING	
	Statutory requirements	6.01
	Documents verifying evidence of identity	6.05
	Transaction records	6.09
	Format and retrieval of records	6.11
	Due diligence and client identification procedures and record keeping for countries outside the European Economic Area	6.14
	Offence of providing false or misleading evidence or information and false or forged documents	6.18
7.	RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS	
	Recognition of suspicious transactions	7.01
	Reporting of suspicious transactions	7.05
	Appointment and role of the Money Laundering Compliance Officer	7.09
	Internal reporting procedures and records	7.16

External reporting procedures:	
National reporting point for disclosures	7.24
Method of reporting	7.25
Nature of the information to be disclosed	7.27
Constructive trust	7.28
Investigation of disclosures	7.32
Confidentiality of disclosures	7.33
Feedback from the investigating authorities	7.34

8. EDUCATION AND TRAINING

Statutory requirements	8.01
The need for awareness by partners and staff	8.02
Timing and content of training programmes	8.04
New professional staff	8.08
Advisory staff	8.09
Staff who can accept new clients	8.10
Partners and managers	8.11
Money Laundering Compliance Officers	8.12
Refresher training	8.13
Methods of providing training	8.14

APPENDICES

A - Articles 1 to 4 of the Council Framework Decision 2002/475/JHA

1. **BACKGROUND**

In May 1996 domestic legislation was enacted, namely The Prevention and Suppression of Money Laundering Activities Law (61(I)/96) which was adopted in line with various Conventions, the 40 Recommendations of the “Financial Action Task Force on Money Laundering” and the E.U. Council Directives.

The above Law was amended in 1995, 1998, 1999, 2000, 2003 and 2004 to include further international measures or to improve existing measures taken. In 2007 the Law was replaced by the Prevention and Suppression of Money Laundering Activities Law 2007, amending and consolidating the previous Laws, which was further amended in 2010, 2012 and 2013.

Interpretation of basic terms

1.01 As an aid to the use of this Directive, a number of key words and phrases appearing throughout the text, are construed or explained as follows:

Administrative Services	The services provided in section 4 of the Law Regulating Companies providing Administrative Services and Related Matters of 2012 (196(I)/2012)
Advisory Authority	The Advisory Authority for Suppression of Money Laundering and Terrorist Financing which is established under Section 56 of the Law.
Beneficial Owner	The natural person(s) who ultimately own or control a client and/or the natural person on whose behalf a transaction or activity is being conducted. It shall at least include: (a) In the case of corporate entities: (i) The natural person(s) who ultimately own or control a legal entity through direct or indirect ownership or control of a sufficient % of the shares or voting rights in that legal entity, including through bearer share holdings, a % of 10% plus one share be deemed sufficient to meet this criterion; (ii) The natural person(s) who otherwise exercise control over the management 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:
 - (i) Where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 10% or more of the property of a legal arrangement or entity;
 - (ii) 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;
 - (iii) The natural person(s) who exercise control over 10% or more of the property of a legal arrangement or entity.

Business relationship	The business, professional or commercial relationship which is connected to the activities of persons who carry out financial or other activities, and which was expected, at the time of conclusion of the contact, to have some duration.
Client	A person who seeks to form a business relationship or to carry out a single one-off transaction with another person who carries out a financial or other activity in or from the Republic.
Compliance Officer	A senior executive with skills, knowledge and expertise in financial or other activities, appointed under section 69(1)(a) of the Law as a firm's central point of contact in order to handle the reported suspicions of their partners and staff regarding money laundering or terrorist financing.
Criminal conduct	See paragraphs 2.22 to 2.24.
EU Directive	Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 in connection with the prevention of money laundering and terrorist financing activities.
European Economic Area Country	A Member State of the European Union or other State which is a contracting party in

	the agreement for the European Economic Area which was signed in Porto on 2 nd May 1992 and was adapted by the Protocol which was signed in Brussels on 17 th May 1993 as the said agreement is further amended from time to time.
know; knowledge	See paragraph 2.25.
Lawyer	<ul style="list-style-type: none"> i) A lawyer and/or a limited liability company (LLC) according to the Advocates Law, Cap. 2 ii) A general partnership or limited partnership whose general partners are lawyers or a limited liability company (LLC) and
Lawyers' Limited Liability Company	See sections 6C and 6D of the Advocates Law, Cap. 2.
MLCO	A firm's Money Laundering Compliance Officer (see paragraph 4.02).
MOKAS	The Unit for Combating Money Laundering at the Attorney General's office (see paragraph 7.23).
Person	The term "person" includes any individual and any company, partnership, association, society, institution or body of persons, corporate or unincorporated.
Politically Exposed Persons	Individuals who are or have been entrusted with prominent public functions in the Republic or in another country and their immediate family members, or persons known to be close associates of such persons.
Prescribed activities and services	The engaging in one or more of the activities and services listed in Section 2 of the Law.
Privileged Information	See section 44 of 188(I)/2007.
Suspect; suspicion	See paragraphs 2.27 to 2.30.
Terrorist financing	The disposition or collection of funds, by any means, directly or indirectly, with the objective or in the knowledge that they shall be used, in full or in part, in order to carry

out any of the offences within the meaning of Articles 1 to 4 of the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (Appendix A).

the Council	The Council of the Cyprus Bar Association.
the Law	The Prevention and Suppression of Money Laundering Activities Law of 2007 (188(I)/2007)
Unit trust	The Trust which is created for the purpose of or resulting in the provision to persons who have funds available for investment facilities of the right to participate as beneficiaries under the trust in profits or income which accrue from the acquisition, management or disposal of any property.

- 1.02 The word “firm”, used in this Directive, includes:
- (i) a lawyer and or a limited liability company (LLC) according to the Advocates Law, Cap 2
 - (ii) a general partnership or limited partnership whose general partners are lawyers or a limited liability company (LLC) and
 - (iii) a subsidiary company, owned directly or indirectly, by any of the above, provided that these activities also include trust services and services to third parties as specified in the Law.

Likewise, references to “partner” include sole practitioners and directors of companies, except where otherwise indicated.

Introduction

- 1.03 The fight against crime demands that criminals are prevented from legitimising the proceeds of their crime through the process of “money laundering or terrorist financing”. It is a process which can involve many persons outside the more obvious targets which are the banks and other financial institutions. Professionals such as accountants and lawyers are at risk because their services could be of value to the successful money launderer or terrorist financier. But the launderer or terrorist financier often seeks to involve many other often unwitting accomplices, such as:

- stockbrokers and securities houses;
- insurance companies and insurance brokers;
- financial intermediaries;
- surveyors and estate agents;
- persons involved in gaming activities;
- company formation agents;
- dealers in precious metals and bullions;
- antique dealers, car dealers and others selling high value

commodities and luxury goods;

- Lawyers.

What is money laundering?

- 1.04 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of funds. Their “dirty” funds come to appear “clean”.
- 1.05 Money laundering is a global phenomenon that affects all countries in varying degrees. By its very nature, it is a hidden activity and, therefore, the scale of the problem and the amount of criminal money being generated either locally or globally each year is impossible to measure accurately. However, failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime a more attractive proposition.

Stages of money laundering

- 1.06 There is no one method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a car or jewellery) to passing money through a complex international web of legitimate businesses and “shell” companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). Initially, however, in the case of drug trafficking and some other serious crimes such as robbery, the proceeds usually take the form of cash which needs to enter the financial system by some means. Street level purchases of drugs are almost always made with cash.
- 1.07 Despite the variety of methods employed, the laundering process is typically accomplished in three stages. These three stages may comprise numerous transactions by the launderers, that could raise suspicions of underlying criminal activity:
- Placement – the physical disposal of the initial proceeds derived from illegal activity.
 - Layering – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. Such transactions are often channelled via shell companies or companies with nominee shareholders and/or nominee directors.

- Integration – the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may partly overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organisations.

- 1.08 Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where his activities are therefore more susceptible to be recognised, specifically:
- entry of cash into the financial system;
 - cross-border flows of funds; and
 - Transfers within and from the financial system.

Vulnerability of lawyers to money laundering or terrorist financing

- 1.09 Money launderers or terrorist financiers are plausible people and their business activities will often be difficult to distinguish from those of the legitimate client. Like the legitimate client, the launderer or terrorist financier will need legal services and a whole range of legal advice. Some areas of a lawyer's work may be more vulnerable than others to the involvement of money launderers or terrorist financiers, but it would be dangerous to regard any area as immune.

Responsibilities of the Council of the Cyprus Bar Association

- 1.10 Supervisory authorities (such as the Association as the designated supervisory body under the Law) have specific obligations under the Law to report to MOKAS any information they obtain which, in their opinion is, or may be, indicative of money laundering or terrorist financing and report to the Attorney General law firms which do not comply with the provisions of the Law.
- 1.11 Further, the Association has an interest in measures employed to counter money laundering or terrorist financing because of the damage which lawyers and their clients can suffer from it, as well as the reputation of the profession as a whole. Therefore, there may be occasions when it will be appropriate for action taken in relation to money laundering or terrorist financing by both lawyers and individuals to be taken into account by the Association in undertaking both its regulatory and disciplinary functions.
- 1.12 Failure to report money laundering or terrorist financing, or failure to have adequate policies and procedures to guard against being used for money laundering or terrorist financing, may call into question the integrity of and the due care and diligence used by the firm or individual member involved.

Compliance with this Directive is likely to be an important point of reference in any assessment of the conduct of individual members and of the adequacy of systems of control to guard against money laundering or terrorist financing.

1.13

Failure to comply with any of the provisions of the Law or with the Directive, the Council of the Cyprus Bar Association may take all or any of the following measures:

- (i) To require the supervised person to take such measures within a specified time frame in order to remedy the situation
- (ii) To impose an administrative fine of up to €200.000 having first given the opportunity to the supervised person to be heard, and in the case the failure continues, to impose an administrative fine of up to €1.000 for each day the failure continues;
- (iii) To amend or suspend or revoke the license of operation of the supervised person.
- (iv) To require the dismissal or removal from their position of any director, manager or officer including the Compliance Officer and the Head of the Internal Audit and Compliance Units whenever it is established that the failure to comply was due to their fault, intentional omission or negligence.
- (v) To impose an administrative fine referred to in sub-paragraph (ii) of the present paragraph to a director, manager or officer or to any other person whenever it is established that the failure to comply was due to their fault, intentional omission or negligence.

Scope of this Directive

1.14

This Directive has been drawn up to give a practical interpretation of the Law. Particularly, persons who carry on the activities and services prescribed in Section 2 of the Law have a legal obligation to implement the measures to prevent money laundering and terrorist financing set out in Part VIII of the Law. Activities and services prescribed under Section 2 of the Law are defined to include a wide range of financial and other activities, but those most likely to be relevant to lawyers are:

- providing services relating to the issue of securities,
- providing advice or services on capital structure, industrial strategy, mergers or the purchase of undertakings,
- undertaking portfolio management,
- providing safe custody services,
- conducting any other investment business, and
- providing any services to clients including carrying out audit activities, accounting/bookkeeping services and providing tax advice.

- 1.15 Most services provided by firms are likely to be of use in one way or another to money launderers or terrorist financiers. Firms risk damage to their reputation and business if they become involved in any way with money launderers or terrorist financiers, even unintentionally.
- 1.16 Firms should appreciate that there are practical benefits in applying standard practice to all of their partners and staff and across their entire range of services. Consistency of approach ensures complete coverage of the areas where the Law is mandatory and avoids difficulties with clients and people who receive or provide services.
- 1.17 For example, standard procedures requiring partners and staff to report any suspicion of money laundering or terrorist financing in the course of their work not only ensure that the requirements of the Law are met whenever they apply, but also give protection to individuals against breaching the disclosure provisions of the primary legislation.
- 1.18 All those who carry out the activities and services described in Section 60 of the Law have also the legal obligation to apply measures to prevent the concealment activities set out in Part VIII of the Laws. It is clarified that these guidance notes do not cover all professional activities of lawyers but only those set out in the aforementioned Section.

Members employed outside practice

- 1.19 While this Directive has been prepared primarily with lawyers in mind, most of the material, and in particular Part II of the Directive, also applies to members employed outside practice. Members employed in banking and financial services should refer, where necessary, to the directive produced by the Central Bank of Cyprus, the Cyprus Securities and Exchange Commission, the Superintendent of Insurance and the Commissioner of the Authority for the Supervision and Development of Co-operative Societies. Members employed in other sectors that might be of use to a money launderer or a terrorist financier may also find that a directive is available from their regulator. In the absence of a suitable directive, members should consider the procedures recommended for lawyers in this Directive, and adapt them as appropriate.

2. **THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007**

Introduction

- 2.01 The main purpose of this Law, which came into effect on 1st January 2008, is to define and criminalise the laundering of the proceeds generated from all serious criminal offences or terrorist financing activities, and provides for the confiscation of such proceeds aiming at depriving criminals from the profits of their crimes. The major provisions of the Law are as follows:

Prescribed offences (Section 3 of the Law)

- 2.02 The Law has effect in respect of offences which are referred to as "prescribed offences" and which comprise of:
- (a) laundering offences; and
 - (b) predicate offences.

Money laundering or terrorist financing offences (Section 4 of the Law)

- 2.03 Under the Law, every person who **knows, or ought to have known** that any kind of property constitutes proceeds from a prescribed offence is guilty of an offence if he carries out any of the following:
- (a) converts or transfers or moves such property, for the purpose of concealing or disguising its illicit origin, or assists any person who is involved in the commission of a predicate offence to evade the legal consequences of his actions;
 - (b) conceals or disguises the true nature, source, location, disposition, movement and rights with respect to property or ownership of this property;
 - (c) acquires, possesses or uses such property;
 - (d) participates in, associates 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; or
 - (e) provides information with respect to investigations performed in relation to laundering offences, for the purpose of enabling the person who has gained profit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence.

- 2.04 Commitment of the above offences is punishable by fourteen (14) years' imprisonment or by a fine of up to €500.000 or by both of these penalties, in the case of a person who knows that the property constitutes proceeds from a predicate offence, or by five (5) years' imprisonment or a fine of up to €50.000 or both of these penalties, in the case of a person who ought to have known.
- 2.05 Under Section 26 of the Law, in criminal proceedings against a person in respect of assisting another to commit a laundering offence or terrorist financing, it is a defence for the defendant to prove that he intended to disclose to 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 Section 26 of the Law, any such disclosure should not be treated as a breach of any contractual restriction upon the disclosure of information.
- 2.06 In the case of employees or persons whose activities are supervised by one of the Authorities set out in Section 59, the Law recognizes that the disclosure may be made to a Money Laundering Compliance Officer in accordance with established internal procedures and such disclosure shall have the same effect as a disclosure made to MOKAS.

Predicate offences including offences of terrorist financing (Section 5 of the Law)

- 2.07 Predicate offences are:
- (a) the criminal offences as a result of which proceeds or assets were derived which may constitute offences of money laundering and which are punishable with imprisonment exceeding one year; (including tax crimes related to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum penalty of more than one year).
 - (b) terrorist financing offences, including collection of money for financing of persons or organizations connected with terrorism; and
 - (c) Offences of drug trafficking as described in Section 2 of the Law.
- 2.08 For the purposes of money laundering or terrorist financing offences it does not matter whether the predicate offence is subject to the jurisdiction of the Cypriot Courts or not (Section 4(2) of the Law).

Failure to report (Section 27 of the Law)

- 2.09 It is an offence for any person, including a lawyer 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 to MOKAS, as soon as it is reasonably practical after the information came to his attention. 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 or both of these penalties.

Tipping – off (Section 48 of the Law)

- 2.10
- (a) Further to the offence (paragraph 2.03), under the section on money laundering or terrorist financing offences above, it is also an offence for any person to make a disclosure, either to the person who is the subject of a suspicion or any third party that information or other relevant documentation on money laundering or terrorist financing has been transmitted to MOKAS or that a report of suspicious transactions or activities has been submitted or that the authorities carry out investigations and searches for money laundering or terrorist financing. "Tipping-off" under these circumstances is punishable by imprisonment not exceeding five (5) years.
 - (b) Irrespective of the provisions of Section 48, persons who exercise professional activities of auditors, external accountants and independent legal advisors may make known to other persons that belong to the same group in countries of the European Economic Area or in third countries (as defined below), information transmitted to MOKAS in accordance with Section 27 of the Law or that MOKAS carries out or may carry out an investigation for money laundering or terrorist financing offences.

For the purposes of this paragraph, "third countries" means third countries which, according to the decision of the Advisory Authority for the Suppression of Money Laundering and Terrorist Financing Activities, have been designated to impose procedures and measures for suppression of money laundering and terrorist financing equivalent to the requirements of the EU Directive.
 - (c) Persons mentioned in paragraph 2.10(b) above may exchange between them information concerning the same client and the same transaction in which two or more persons are involved, on condition that they are in countries of the European Economic Area or in third countries (as defined in the previous paragraph) and that the persons who exchange information belong to the same professional field. The information so exchanged is used exclusively for the prevention of money laundering or terrorist financing activities.
 - (d) The disclosure and exchange of information made under 2.10(b) and 2.10(c) above is not considered as violation of contractual or other legal restriction pertaining to disclosure of information.
 - (e) The disclosure to the competent Supervisory Authorities by persons who carry out financial and other activities, that information has been communicated to MOKAS, in accordance with Section 27 of the Law, or that MOKAS investigates or may investigate offences of money laundering or terrorist financing activities does not constitute violation of any contractual or other legal restriction pertaining to disclosure of information.
 - (f) According to Section 28(6) of the EU Directive, where a firm seeks to dissuade a client from engaging in an illegal activity, this shall not constitute a disclosure to the client concerned or to other third persons (tipping-off).

Prescribed activities and services (Section 2 of the Law)

2.11 The Law recognises the important role of (a) those carrying out financial activities, and (b) those carrying out other activities, including accountants, auditors and lawyers, for the effective prevention of money laundering activities and terrorist financing, and places additional administrative requirements on all institutions, including firms engaged in the activities and services listed below:

(a) Financial Services

- (1) Acceptance of deposits from the public.**
- (2) Lending money to the public.**
- (3) Finance leasing, including hire purchase financing.**
- (4) Money transmission services.**
- (5) Issue and administration of means of payment (e.g. credit cards, travellers' cheques, bankers' drafts and electronic means).**
- (6) Guarantees and commitments.**
- (7) Trading on one's own account or on account of another person in:**
 - (i) Stocks or money market securities including cheques, bills of exchange, bonds and certificates of deposits,**
 - (ii) foreign exchange,**
 - (iii) financial futures and options,**
 - (iv) exchange and interest rate instruments, and**
 - (v) transferable instruments.**
- (8) Participation in bond issues and provision of related Services.**
- (9) Consultancy services to enterprises concerning their capital structure, industrial strategy and related issues and consultancy services as well as services in the areas of mergers and acquisitions of businesses.**
- (10) Money broking.**
- (11) Investment services, including dealing in and arranging the dealing in investments, managing investments, giving investment advice and establishing and operating collective investment schemes. For the purposes of this section, the term "investment" includes long term life insurance policies, whether or not associated with investment schemes.**
- (12) Safe custody services.**
- (13) Custody trustee services in relation to stocks.**
- (14) Any of the services specified in Parts I and III of the Third Schedule to the Investment Services and Activities and Regulated Markets Law, and which are provided in connection with financial instruments listed in Part III of the same Schedule and those specified in Sections 41 and 100 of the Open-Ended Undertakings of Collective Investments in Transferable Securities (UCITS) and other Related Issues Law.**
- (15) Mediation for the conclusion of life insurance policies.**

(b) Other Activities

- (1) Exercise of professional activities by auditors, external accountants and tax advisors, including transactions on behalf of their clients in the context of carrying out financial activities.
- (2) Exercise of professional activities on behalf of lawyers, with the exception of privileged information, when they participate, either:
 - (i) by assisting in the planning or execution of transactions for their clients concerning:
 - the purchase and sale of real estate or business entities;
 - the managing of client money, securities or other assets;
 - the opening or management of bank, savings or securities accounts;
 - the organisation or contributions necessary for the creation, operation or management of companies; and
 - the creation, operation or management of trust companies, businesses and similar structures;
 - (ii) by acting on behalf and for the account of their clients in any financial or real estate transactions.
- (3) Dealings in real estate transactions, conducted by real estate agents.
- (4) Trading in goods or commodities such as precious stones or metals, provided the payment is made in cash and in an amount equal or greater than €15.000.
- (5) The following administrative services provided to third parties:
 - (i) forming companies or other legal persons;
 - (ii) acting as director or secretary of a company, a partner of a partnership, or a holder of a similar position in relation to other legal persons or legal mechanisms so that another person may carry out such duties;
 - (iii) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or legal mechanism;
 - (iv) acting as a trustee of an express trust or a relevant legal mechanism so that another person carries out such duties;
 - (v) acting as nominee shareholder for another person or a legal mechanism so that another person carries out such duties.
- (6) any of the services or activities specified in Article 4 of the Law regulating companies providing administrative services and related matters as amended or replaced.

Procedures to prevent Money Laundering or Terrorist Financing (Section 58 of the Law)

- 2.12 The Law requires all persons carrying on financial or other activities, as defined above, to establish and maintain specific policies and procedures to guard against their business and the wider financial sector in general, being used for the purposes of money laundering or terrorist financing. In essence, these procedures are designed to achieve two targets: firstly, to facilitate the recognition and reporting of suspicious transactions, and secondly, to ensure, through the strict implementation of the “Know your Client” principle and the implementation of adequate record keeping procedures that the lawyer is able to provide his part of the audit trail, should a client come under investigation.
- 2.13 The Law requires all persons to establish systems and procedures in connection with the following:
- Client identification;
 - Record-keeping procedures in relation to clients’ identity and their transactions;
 - Procedures of internal reporting to a competent person (e.g. a Money Laundering Compliance Officer) appointed to receive and consider information that give rise to knowledge or suspicion that a client is engaged in money laundering or terrorist financing activities and to MOKAS as provided by the Law;
 - Other internal control and communication procedures for the purpose of preventing money laundering and terrorist financing;
 - Measures for making employees aware of all the above procedures to prevent money laundering and terrorist financing and of the relevant legislation; and
 - Provision of training to their employees in the recognition and handling of transactions suspected to be associated with money laundering or terrorist financing.

Supervisory Authorities (Section 59 of the Law)

- 2.14 On 7 March 2001, the Council of Ministers designated the Council of the Cyprus Bar Association as the Supervisory Authority for lawyers.
- 2.15 For the purpose of preventing money laundering and terrorist financing and for the purpose of accomplishing the objects of the Law, the Council of the Association, under section 59(2)(b) is the Supervisory Authority for the following persons:
- (i) a lawyer and or a limited liability company (LLC) according to the Advocates Law, Cap 2
 - (ii) a general partnership or limited partnership whose general partners are lawyers or a limited liability company (LLC) and
 - (iii) a subsidiary company, owned directly or indirectly, by any of the above, provided that these activities also include trust services and services to third parties as specified in the Law.

- Under section 59(4), the Council of the Cyprus Bar Association is authorized to issue directives to the above persons. The purpose of this Directive issued by the Association as the Supervisory Authority of the legal profession is to give detailed instructions regarding the requirements of the Law in respect of business carried out by firms and to indicate good business practice.
- 2.16 The Directive is binding and obligatory as to its adoption by the persons to whom it is addressed. The Association follows up, evaluates and supervises the adoption of Part VIII of the Law and of the Directive issued.
- 2.17 According to Section 59(6) of the Law, the Association may take all or any of the following measures in case a lawyer fails to comply with the provisions of Part VIII of the Law or its directives issued under section 59(4) of the Law or Regulation (EC) No. 1781/2006 of the European Parliament and the Council of the European Union of 15th November 2006 on information regarding the payer accompanying money transfers:
- (i) To require the supervised person to take such measures within a specified time frame in order to remedy the situation
 - (ii) To impose an administrative fine of up to €200.000 having first given the opportunity to the supervised person to be heard, and in the case the failure continues, to impose an administrative fine of up to €1.000 for each day the failure continues;
 - (iii) To amend or suspend or revoke the license of operation of the supervised person.
 - (iv) To require the dismissal or removal from their position of any director, manager or officer including the Compliance Officer and the Head of the Internal Audit and Compliance Units whenever it is established that the failure to comply was due to their fault, intentional omission or negligence.
- To impose an administrative fine referred to in sub-paragraph (ii) of the present paragraph to a director, manager or officer or to any other person whenever it is established that the failure to comply was due to their fault, intentional omission or negligence.
- 2.18 A person falling within its supervision, who fails to comply with the provisions of Section 59 of the Law and the directives issued by the Association, is referred to the Disciplinary Body which decides accordingly.
- 2.19 Where a Supervisory Authority has information and believes that a person falling within its supervision is involved in money laundering or terrorist financing offences, it has a legal obligation to disclose the relevant information to MOKAS.

“Privileged Information” (Section 44 of the Law)

2.20 Under Section 44 of the Law “privileged information” means:

(a) The communication between a lawyer and a client for the purposes of providing legal advice or for the provision of professional services relating to any legal proceedings, whether initiated or not, the disclosure of which, in any legal proceedings, is protected by the privilege of confidentiality in accordance with the legislation in force.

Provided that the communication between a lawyer and a client for the purpose of committing a prescribed offence does not constitute privileged information.

(b) Any other information which is not admitted before a Court for reasons of safeguarding the public interest in accordance with the legislation in force.

Orders for disclosure of information (Section 45 of the Law)

2.21 Courts in Cyprus may, on application by the investigator, issue an order for the disclosure of information by a person, including a lawyer, who appears to the Court to be in possession of the information to which the application relates. Such an order applies irrespective of any legal or other provision which creates an obligation for the maintenance of secrecy or imposes any constraints on the disclosure of information. As already stated under “tipping-off”, a person who makes any disclosure which is likely to obstruct or prejudice an investigation into the commitment of a money laundering or terrorist financing offence, knowing or suspecting that the investigation is taking place, is guilty of an offence.

Terminology

Criminal conduct

2.22 The term criminal conduct (predicate offence) in the Law refers to the original offence, e.g. drug trafficking, the proceeds of which are involved in actual or suspected money laundering or terrorist financing. It includes any conduct, wherever it takes place, which would constitute an indictable offence if committed in Cyprus. In general, such offences are those which are serious enough to be tried in Court. There will be criminal conduct, which can give rise to money laundering or terrorist financing offences in Cyprus, even if the conduct was not criminal in the country where it actually occurred. See paragraph 7.05 as to the reporting requirement under the Law.

2.23 Offences indictable in Cyprus are all criminal offences from which proceeds or assets were derived, and which are punishable with imprisonment exceeding one year.

2.24 The Law does not impose on lawyers the duty to look into the criminal law of any other country in which the criminal conduct may have occurred. The basis for determining whether assets derive from criminal conduct is that the activity

from which the assets are generated would be an indictable criminal offence if occurred in Cyprus. Lawyers would not be expected to know the exact nature of the criminal activity concerned, or that particular assets are definitely those arising from the crime.

Knowledge

- 2.25 The term “knowledge” is not strictly defined in the Law but it may include situations such as:
- actual knowledge,
 - shutting one’s mind to the obvious,
 - deliberately refraining from making enquiries, the results of which one might not care to have,
 - knowledge of circumstances which would indicate the facts to an honest and reasonable person, and
 - knowledge of circumstances which would put an honest and reasonable person on enquiry, but not mere neglect to ascertain what could have been found out by making reasonable enquiries.

Reasonable excuse

- 2.26 The legal interpretation of the defence of reasonable excuse is covered by Section 26 of the Law. If you find yourself in breach of the Law inadvertently, or under duress, the situation should be corrected by reporting the matter as soon as is reasonably possible.

Suspicion

- 2.27 The words suspect and suspicion appear many times in the legislation. As examples, they raise the questions:
- Should a lawyer suspect that a person has engaged in or benefited from criminal conduct, even if he/she does not know the exact nature of the criminal offence?
 - Should a lawyer suspect that assets are or represent the proceeds of criminal conduct?
- 2.28 Suspicion falls far short of proof based on firm evidence, but must be built on some factual foundation. There must be a degree of satisfaction, even if it does not amount to belief. This means that speculation as to whether a possible situation does in fact exist does not by itself amount to suspicion.
- 2.29 A particular sector or business may be subject to a greater degree of inherent risk of money laundering or terrorist financing than another sector. The nature of the business practices in a particular entity may raise the overall risk of fraudulent, illegal or unauthorised transactions. However, an assessment that there is a higher than normal risk of money laundering or terrorist financing **is not** the same as suspecting money laundering or terrorist financing.
- 2.30 Paragraphs 7.01 to 7.04 of this Directive contain some guidance on how to recognise whether a transaction is suspicious.

Obligations to clients and third parties

Client confidentiality

- 2.31 The legislation protects those reporting suspicions of money laundering or terrorist financing from claims in respect of any alleged breach of client confidentiality. This ensures that no action can be taken against the reporter even where the suspicions are later proved to be ill founded. However, the protection extends only to disclosure of the suspicion or opinion that funds derive from money laundering or terrorist financing, and to matters on which that suspicion or opinion is based. If in doubt, lawyers should insist on the law enforcement agencies obtaining a Court order before disclosing information beyond that contained in their initial report.

Constructive trust

- 2.32 A number of concerns have been raised about possible conflicts between the civil and criminal law in the area of constructive trusteeship, as a result of the duty to report suspicious transactions. Where a lawyer comes to know that property belongs to a person other than his client, he can become a constructive trustee of that property and, therefore, accountable for it to its true owner. This is most likely to arise in two cases when the lawyer comes to know that property belongs not to his client but to a third party:

- The lawyer receives property and deals with it in a way which he knows to be inconsistent with the rights of the true owner. The fact that the lawyer was acting with the consent of the law enforcement agencies would be no defence to a claim by the true owner.
- Even though the lawyer does not himself receive the property, he acts in a way which he knows will assist others to defraud the true owner of his property.

- 2.33 Paragraph 2.25 shows that the term “knows” has a wide meaning in this context. Even if he had no actual knowledge, a lawyer could still be liable to the true owner if he **should have known** that his rights were being or might be infringed. Further guidance on reporting procedures in cases which could involve constructive trusteeship is given in paragraphs 7.27 to 7.30.

Disclosure of information to third parties

- 2.34 A third party claiming to be entitled to assets which are or have been in the hands of a lawyer and which are the subject of a report to MOKAS, might seek a Court order which would direct the lawyer to disclose information. If the lawyer believes that disclosure of information to the third party could prejudice a money laundering or terrorist financing investigation by the law enforcement agencies, the tipping off offence could arise. Legal advice should be taken before the information is disclosed.

3. RISK BASED APPROACH FOR CLIENTS

- 3.01 Potential money laundering and terrorist financing risks faced by lawyers will vary according to many factors including the activities undertaken by lawyers, the type and identity of client and the nature of the client relationship and its origin. These criteria are not exhaustive, are not intended to be prescriptive and should be applied in a manner that is well- considered.
- 3.02 Identification of the ML risks and TF risks associated with certain clients or categories of clients, and certain types of work will allow lawyers to determine and implement reasonable and proportionate measures and controls to mitigate these risks.
- 3.03 It is recognised that no control system is able to detect and prevent all cases of money laundering or terrorist financing. But, the lawyer should implement appropriate measures and procedures on risk-based approach so that his efforts are concentrated on areas that are most in need of addressing the risks of money laundering and terrorist financing
- 3.04 A risk-based approach involves specific measures and procedures in assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by lawyers.

Such measures and procedures are:

- (a) Identifying and assessing the money laundering and terrorist financing risks emanating from particular customers, financial instruments, services, and geographical areas.
- (b) Documenting the policies, measures, procedures and controls to ensure their uniform application.
- (c) Managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- (d) Continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

Identification, recording and evaluation of risks

- 3.05 The starting point for the application of the risk-based approach system is the identification, recording and evaluation of risk faced by lawyers. The identification, recording and evaluation of risk that the lawyers face presupposes the finding of answers to the following questions:
- (a) What risk is posed by the lawyers' customers? For example:
 - (i) complexity of ownership structure of legal persons,
 - (ii) companies with bearer shares,
 - (iii) companies incorporated in offshore centres,
 - (iv) politically exposed persons,
 - (v) customers engaged in transactions which involves significant amounts of cash,
 - (vi) customers from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking;

- (b) What risk is posed by a customer's behaviour? For example:
- (i) customer transactions where there is no apparent legal financial/commercial rationale,
 - (ii) situations where the origin of wealth and/or source of funds cannot be easily verified,
 - (iii) unwillingness of customers to provide information on the beneficial owners of a legal person;
- (c) How did the customer communicate the lawyers? For example:
- (i) non-face to face customer,
 - (ii) customer introduced by a third person;
- (d) What risk is posed by the services and financial instruments provided to the customer? For example:
- (i) services that allow payments to third persons,
 - (ii) large cash deposits or withdrawals.

3.06 The most commonly used risk criteria are: country or geographic risk; client risk; and risk associated with the particular service offered. These criteria, however, should not be considered in isolation. There is no single methodology to apply these risk categories, and the application of these risk categories is merely intended to provide a suggested framework for approaching the management of potential risks.

Country/Geographic Risk

3.07 There is no universally agreed definition that prescribes whether a particular country or geographic area represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks, such as the domicile of the client, the location of the transaction and the source of the funding. Countries that pose a higher risk include:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the UN.
- Countries identified by credible sources as generally lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as being a location from which funds or support are provided to terrorist organizations.
- Countries identified by credible sources as having significant levels of corruption or other criminal activity.

Client Risk

3.08 Determining the potential money laundering or terrorist financing risks posed by a client, or category of clients, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a lawyer should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment.

Categories of clients whose activities may indicate a higher risk include:

- PEPs are considered as higher risk clients – If a lawyer is advising a client that is a PEP, or where a PEP is the beneficial owner of the client, then a lawyer will need to carry out appropriate enhanced CDD.
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances.
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely fashion the true beneficial owner or controlling interests, such as the unexplained use of legal persons or legal arrangements, nominee shares or bearer shares.
- Clients that are cash (and cash equivalent) intensive businesses including:
 - Money services businesses (e.g. remittance houses, currency exchange houses etc.)
 - Casinos, betting and other gambling related activities.
 - Businesses that while not normally cash intensive generate substantial amounts of cash.
- Where clients that are cash intensive businesses are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations this may mitigate the risks.
- Charities and other “not for profit” organisations that are not subject to monitoring or supervision by designated competent authorities..
- Clients using financial intermediaries, financial institutions or lawyers that are not subject to adequate AML/CFT laws and measures and that are not adequately supervised by competent authorities.
- Clients having convictions for proceeds generating crimes who instruct the lawyer to undertake specific activities on their behalf.
- Clients who have no address, or multiple addresses without legitimate reasons.
- Clients who change their settlement or execution instructions without appropriate explanation.

Service Risk

3.09 An overall risk assessment should also include determining the potential risks presented by the services offered by a lawyer. When determining the risks associated with provision of services related to specified activities, consideration should be given to such factors as:

- Services where lawyers, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they actually control in the act of closing a business transaction.
- Transfer of real estate between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- Payments received from unassociated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- Transactions where it is readily apparent to the lawyer that there is inadequate consideration, such as when the client does not identify legitimate reasons for the amount of the consideration.
- Administrative arrangements concerning estates where the deceased was known to the lawyer as being a person who had been convicted of proceeds generating crimes.
- Clients who offer to pay extraordinary fees for services which would not ordinarily warrant such a premium. However, bona fide and appropriate contingency fee arrangements, where a lawyer may receive a significant premium for a successful representation, should not be considered a risk factor.
- The source of funds and the source of wealth – The source of funds is the activity that generates the funds for a client, while the source of wealth describes the activities that have generated the total net worth of a client.
- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile may indicate that a client not otherwise seen as higher risk should be treated as such. Conversely, low levels of assets or low value transactions involving a client that would otherwise appear to be higher risk might allow for a lawyer to treat the client as lower risk.
- Situations where it is difficult to identify the beneficiaries of trusts; this might include a discretionary trust that gives the trustee discretionary power to name the beneficiary within a class of beneficiaries and distribute accordingly the assets held in trust, and when a trust is set up for the purpose of managing shares in a company that can make it more difficult to determine the beneficiaries of assets managed by the trust.
- Services that deliberately have provided or purposely depend upon more anonymity in the client identity or participants than is normal under the circumstances and experience of the lawyer.

3.10 On implementing appropriate measures and procedures on a risk-based approach, and on implementing the customer identification and due diligence procedures, the lawyer and particularly the compliance officer, consults data, information and reports [e.g. customers from countries which inadequately apply Financial Action Task Force's (FATF), country assessment reports] that are published in following relevant international organisations:

(a) FATF - www.fatf-gafi.org

(b) the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) - www.coe.int/moneyval

(c) the EU Common Foreign & Security Policy (CFSP)-

http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm

(d) the UN Security Council Sanctions Committees -

www.un.org/sc/committees/

(e) the International Money Laundering Information Network (IMOLIN) - www.imolin.org

(f) the International Monetary Fund (IMF) – www.imf.org.

Controls for Higher Risk Solutions

3.11 Lawyers should implement appropriate measures and controls to mitigate the potential ML & TF risks with respect to those clients that as the result of the lawyer or firm risk-based approach, are determined to be higher risk. Paramount among these measures is the requirement to train legal professionals and appropriate staff to identify and detect changes. These measures and controls may include:

- General training on ML methods and risks relevant to lawyers.
- Targeted training for increased awareness by the lawyers providing specified activities to higher risk clients or to lawyers undertaking higher risk work.
- Increased levels of CDD or enhanced DD for higher risk situations.
- Escalation or additional review by the lawyer or within a firm at the establishment of a relationship.
- Periodic review of the services offered by the lawyer and/or firm to determine whether the risk of ML & TF occurring has increased.
- Reviewing client relationships from time to time to determine whether the risk of ML & TF occurring has increased.
- The same measures and controls may often address more than one of the risk criteria identified and it is not necessarily expected that a lawyer establish specific controls targeting each risk criterion.

Monitoring and improving the effective operation of lawyers' internal procedures

3.12 Lawyers need to have suitable means of assessing, on a regular basis that their risk mitigation procedures and controls are working effectively. For that purpose, aspects the lawyer will need to consider are the following:

- Appropriate procedures to identify changes in customer's business profile;
- Reviewing ways in which new products and services may be used by criminals for money laundering or terrorist financing purposes, and how these ways may change;
- Procedures for assessing the adequacy of staff training and awareness;
- Introducing effective compliance monitoring arrangements (such as internal audit inspection and reviews by the compliance unit);
- Appropriate technology-based and people-based systems;
- Appropriate management information systems;
- Reporting and accountability by responsible officials to the Board of Directors and Senior Management;
- Effectiveness of liaison with the Cyprus Bar Association and MOKAS.

4. **INTERNAL CONTROLS, POLICIES AND PROCEDURES**

Responsibilities and accountabilities

4.01 Lawyers are required to establish and maintain policies, procedures and control systems to prevent money laundering or terrorist financing, and to ensure the reporting of any cases that may be known or suspected.

4.02 Section 69 of the Law requires lawyers to establish a central point of contact in order to handle the reported suspicions of their partners and staff regarding money laundering or terrorist financing. Lawyers must appoint an “appropriate person” (referred to in this Directive as the Money Laundering Compliance Officer or MLCO) to undertake this role.

Recommended procedures to comply with the Law

4.03 All lawyers to which the Law applies should have appropriate procedures for:

- identifying clients (see Part 5 of this Directive),
- record-keeping (see Part 6 of this Directive),
- recognising and reporting suspicions of money laundering or terrorist financing (see Part 7 of this Directive), and
- the education and training of partners and staff (see Part 8 of this Directive).

4.04 As good practice, lawyers are recommended to make arrangements to verify, on a regular basis, compliance with policies, procedures and control systems relating to anti-money laundering or anti-terrorist financing activities. Lawyers need to satisfy themselves that the requirement in the Law to maintain such procedures has been fulfilled.

4.05 It is important that the procedures and responsibilities for monitoring compliance with and effectiveness of anti-money laundering or anti-terrorist financing policies and procedures are clearly laid down by all lawyers.

Overseas offices and associated firms

4.06 Where a lawyer has overseas offices or associated firms, where control can be exercised, it is prudent to adopt a “group policy”. This should require all overseas offices and associated firms to ensure that verification of identity and record-keeping are undertaken at least to the standards required under the Cyprus law. Reporting procedures and other requirements of the money laundering or terrorist financing legislation in the host country must nevertheless be adhered to in accordance with local laws and procedures.

5. IDENTIFICATION PROCEDURES

Statutory requirements

- 5.01 The Law requires all persons carrying out financial business to apply client identification procedures in accordance with Sections 58 and 61 to 65. The essence of these requirements is that, except where the Law states that client identification need not be made, a firm must verify the identity of a prospective client.

Introduction – “Know your Client”

- 5.02 In business relationships, the lawyer will need to obtain a good working knowledge of a client’s business and financial background as well as information on the purpose and intended nature of the business relationship in order to provide an effective service. This will provide evidence of identity at an early stage in the relationship.
- 5.03 The “Know your Client” process is vital for the prevention of money laundering or terrorist financing and underpins all other activities. If a client has established a business relationship under a false identity, he/she may be doing so for the purpose of defrauding the lawyer himself, or merely to ensure that he/she cannot be traced or linked to the proceeds of the crime that the lawyer is being used to launder. A false name, address or date of birth will usually mean that the law enforcement agencies cannot trace the client if he/she is needed for interview in connection with an investigation.
- 5.04 A lawyer, who is taking over a professional appointment, replacing an existing lawyer, may be in communication with the latter. This may provide evidence of both the identity and integrity of the client, and is a valuable procedure in this context.
- 5.05 Where a partner, a trusted member of staff, a respected client of long standing or another reliable source introduces a new client, a lawyer should not overlook the need for normal client acceptance procedures.
- 5.06 A lawyer should require from a prospective client to produce documents as evidence of identity. A copy of such document(s) should be taken and retained.. An on-going client due diligence on the business should be done, including scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the lawyer’s knowledge of the client, their business and risk profile and, where necessary, the source of funds. Records kept must be reviewed and updated.

The basic identification requirement

- 5.07 All lawyers should seek satisfactory evidence of identity of those for whom they provide services (a process referred to in this Directive as verification of identity). If satisfactory evidence of identity has not been obtained in a reasonable time, then “the business relationship or one-off transaction in

question shall not proceed any further". This means that the lawyer should refrain from providing the requested service or performing the transaction. In some circumstances, failure by a client to provide satisfactory evidence of identity may, in itself, lead to a suspicion that he/she is engaging in money laundering. The lawyer should then seriously consider reporting the case to MOKAS.

5.08 It is for lawyers themselves to discharge their obligation under the Law to verify identity. The few occasions when it is reasonable to rely on others to undertake the procedures or to confirm identity include:

- Occasions where the client is introduced by one of the lawyer's overseas branch offices or associated firms. For these, the lawyer should obtain the introducer's written confirmation that it has verified the client's identity and that relevant identification data is retained by the overseas branch office or firm.
- Occasions where a lawyer merges with another firm, or acquires the practice of another firm, in whole or in part, and where it is not necessary for the identity of clients to be re-verified, provided that satisfactory identification records are available.

5.09 The verification requirements are the same, whatever the means by which the lawyer intends to provide his services to the client. Thus, the requirements are no less where all advice is to be given by post, by telephone or even through the internet.

- 5.10
- (a) If a lawyer suspects that a prospective client is engaged in money laundering or terrorist financing, he may well decline to act but has a legal obligation to file a suspicious activity report to MOKAS. In that event it will be unnecessary to complete identification procedures. Moreover, nothing must be communicated to the prospective client (or to any other person) which might prejudice an investigation or proposed investigation by the law enforcement agencies.
 - (b) Section 62(6) of the Law requires adoption of the same procedures for verification of identity and the measures of due diligence as to the new and existing clients, at the appropriate time, regard being had to the degree of the risk of being involved in money laundering or terrorist financing.
 - (c) If the lawyer finds out, at any stage of the business relationship with an existing client, that valid or sufficient documentation or information are absent regarding his/her identity and economic profile, the lawyer is obliged to act for the adoption of all procedures and due diligence in order to collect the missing documentation and information as early as possible with a view to forming an economic profile of the client. If the client fails or refuses to produce the necessary documentation and information regarding his/her identity for the establishment of his economic profile within a reasonable time, the lawyer should terminate the business relationship and, at the same time, he must consider whether, under the circumstances, he must file a suspicious activity report to MOKAS.

When must identity be verified?

- 5.11 According to Section 60 of the Law, persons carrying out financial or other activities adopt the identification procedures and the measures of due diligence as to the client in the following cases:
- (a) When they establish business relationships,
 - (b) When they carry out once off transactions amounting to €15.000 or more, whether or not the transaction is carried out in a single operation or in several operations which appear to be linked,
 - (c) When there is suspicion of money laundering or terrorist financing regardless of the amount of the transaction,
 - (d) When there are doubts about the veracity or adequacy of the documents, data or information collected earlier for the identification of an existing client.
- 5.12 According to Section 61(1) of the Law, client identification procedures and due diligence measures shall comprise:-
- (a) identifying the client and verifying the client's identity on the basis of documents, data or information obtained from a reliable and independent source;
 - (b) Identifying the beneficial owner and taking risk-based and adequate measures to verify his/her identity on the basis of documents, data or information issued by or received from a reliable and independent source; As regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the client;
 - (c) Obtaining information on the purpose and intended nature of the business relationship;
 - (d) Conducting on-going supervision 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 data and information held by the lawyer in connection with the client.
- 5.13 According to Section 64(1)(a) of the Law, lawyers should apply one or more of the following enhanced due diligence measures, in addition to those stated above, when the client has not been physically present for identification purposes:-
- (a) ensuring that the client's identity is established by additional documents, data or information;
 - (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution;
 - (c) effecting the first payment in the context of the transactions through an account that has been opened in the client's name in a credit institution operating in a country within the European Economic Area.

- 5.14 Once identification procedures have been satisfactorily completed, then as long as records are maintained in accordance with Part 6 of the Directive and some contact is maintained with the client, no further evidence is needed when subsequent transactions are undertaken.
- 5.15 Lawyers should verify the identity of the client and the beneficial owner before the establishment of a business relationship or the carrying out of a transaction. This applies whatever type of business may be involved. It is an obligation which arises under the Law and the “Charter of the European Professional Associations in support of the fight against organised crime”.
- 5.16 By way of derogation from the provisions of this paragraph, lawyers may allow the verification of the identity of the client and the beneficial owner to be completed during the establishment of a business relationship if this is necessary in order 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.

Identification procedures: Exemptions

- 5.17 The obligation to maintain procedures for obtaining evidence of identity is general, but there are a number of exemptions when some of the requirements can be waived. However, lawyers should realise that exemptions can be difficult to apply and may cause additional administrative problems. They may think it more prudent to carry out their own identification procedures for all new clients. It is also important to remember that no exemption applies in the case of any one-off transaction which is known or suspected to involve money laundering or terrorist financing.
- 5.18 Steps to verify identity are not required in the case of Cypriot credit or financial institutions.
- 5.19 Verification of identity is not required when there are reasonable grounds for believing that the applicant for business relationship is himself subject to the Law
- 5.20 Verification of identity is not normally needed in the case of a single one-off transaction when payment by, or to, the applicant is less than €15.000 (see paragraph 5.11). This exception does not apply to company or trust formation.

Clients from countries whose legislation is ineffective

- 5.21 Although many countries have enacted, or are enacting, effective anti-money laundering and anti-terrorist financing legislation, there are some countries where the legislation is considered to be ineffective or deficient. The 40 Recommendations of the Financial Action Task Force (FATF) provide the international standard for combating money laundering and terrorist financing. The Government of the Republic of Cyprus has officially adopted the said Recommendations.

- 5.22 The Financial Action Task Force issues, from time to time, guidance on countries considered to be at risk from criminal money. Special attention should be given to business relationships and transactions with any person or body from such countries. The MLCOs are requested to consult the FATF country evaluations (<http://www.fatf-gafi.org>) and the Moneyval Committee of the Council of Europe (www.coe.int/moneyval).
- 5.23 When formulating their internal procedures, lawyers should have regard to the need for additional and continuous supervision procedures for transactions from countries which appear to have ineffective and deficient systems of anti-money laundering and anti-terrorist financing. When considering what additional procedures are required, lawyers may take into account the FATF assessment of the progress that has been made, if any. In respect of transactions from these countries which do not have an apparent or visible lawful purpose, the background and purpose of such transactions should, as far as possible, be examined, and written findings should be available to assist competent authorities.

Due Diligence for individuals

Evidence of identity

- 5.24 When verifying the identity of an individual, the vital question is “Is the person who he/she claims to be?” not “What is his/her position and standing? The identity of an individual comprises his/her name and all other names used the date of birth, the address at which the person can be located and his /her profession or occupation. An official document bearing a photograph of the person should also be obtained. However, photographic evidence of identity is only of value to identify clients who are seen face to face. It is neither safe nor reasonable to require a prospective client to send a passport through the post. Any subsequent changes to the client’s name or address that are notified to the lawyer should be recorded.
- 5.25 In addition to the name(s) used and the date of birth, it is important that the current permanent address should be verified as it is an integral part of the identity. Some of the best means of verifying addresses are:
- a face to face home visit to the applicant for business,
 - making a credit reference agency search,
 - requesting sight of a recent utility bill, local authority tax bill, bank or co-operative society statement (not more than 3 months old) (to guard against forged or counterfeit documents, care should be taken to check that the documents offered are originals), and
 - checking the telephone directory.

Non Cyprus residents

- 5.26 For those prospective clients who are not normally resident in Cyprus but who make face to face contact, a passport or national identity card will normally be available. In addition to recording the passport or identity card number and place of issue, lawyers should confirm identity and permanent address with a

- reputable financial institution or professional advisor in the prospective client's home country or normal country of residence.
- 5.27 Lawyers should have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
- 5.28 Where the client has not been physically present for identification purposes, lawyers must take measures such as:
- (a) Supplementary measures to verify or certify the documents supplied by i.e. attorney or consulate, or requiring confirmatory certification by a credit or financial institution which is subject to equivalent AML rules/standards.
 - (b) Ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.
 - (c) Verification details covering true name or names used, current permanent address and verification of signature could be checked with a reputable credit or financial institution or professional advisor in the prospective client's home country.

Due Diligence for legal persons and legal arrangements

- 5.29 Because of possible difficulties of identifying beneficial ownership and the complexity of their organisations and structures, legal entities and trusts are among the most likely vehicles for money laundering or terrorist financing, particularly when fronted by a legitimate trading company. Particular care should be taken to verify the legal existence of the prospective client and to ensure that any person purporting to act on its behalf is authorised to do so and identify and verify the identity of that person.

Companies and partnerships

- 5.30 In the case of any corporate or other entity, the principal requirement is to identify and take reasonable measures to understand the ownership and control structure, duly identifying the beneficial owners of the clients. Enquiries should be made to confirm that the entity exists for a legitimate trading or economic purpose and that the controlling principals can be identified
- 5.31 Before a business relationship is established, a company search and/or other commercial enquiries should be made to ensure that, if the applicant is a company, it has not been, or is not in the process of being dissolved, struck off, wound up or terminated.
- 5.32 "Know your Client" is an on-going process. If a lawyer becomes aware of changes to the client's structure or ownership, or if suspicions are aroused by a change in the nature of the business transacted, further checks should be made to ascertain the reason for the changes.

5.33 In this context, lawyers are required to:

(a) Identify the customer and verify its identity. The type of information needed to perform this function would be:

(i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

(iii) The address of the registered office, and, if different, a principal place of business.

(b) Identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons.

Information which verifies the identity for legal persons:

5.34 (i.i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person; and

(i.ii) to the extent that there is doubt under (i.i) as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

(i.iii) Where no natural person is identified under (i.i) or (i.ii) above, lawyers should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior manager.

5.35 According to Section 63(1) of the Law no further steps to verify identity over and above normal commercial practice and due diligence procedures will

usually be required where the prospective client is:

- A credit institution or financial organisation which falls within the ambit of the EU Directive;
- A credit institution or financial organisation which operates in a country outside the European Economic Area which:

(a) in accordance with the decision of the Advisory Authority for the suppression of crimes of money laundering proceeds from illegal activities and terrorist financing, it imposes requirements equivalent to those of the EU Directive, and

(b) it is supervised as regards compliance with the said requirement.

- A company quoted on a recognised stock exchange and whose titles are accepted for dealing in a regulated market of the European Economic Area or in a third country which is subject to the declaration requirements which comply with the Community legislation.
- The Public Authorities of the countries of the European Economic Area.

5.36 The evidence for accepting that the prospective client falls into one of these categories should be recorded. Moreover, evidence that any individual representing the company has the necessary authority to do so should be sought and retained.

5.37 Where the applicant is an unquoted company, an unincorporated business or a partnership, the lawyer should identify the principal directors/partners and beneficial shareholders in line with the requirements for individual clients. In addition, the following documents should normally be obtained:

- for established businesses, a copy of the latest report and accounts (audited where applicable),
- a copy of the certificate of incorporation/certificate of trade or equivalent, and
- a copy of the company's Memorandum and Articles of Association and other certificates issued by the Registrar of Companies.

5.38 The lawyer may also make a credit reference agency search or take a reference from a bank or from another professional advisor. Enhanced due diligence should be performed for higher risk categories of client, business relationship or transaction. Such categories may include a non-resident client, private banking and companies that have nominee shareholders or shares in bearer form.

5.39 Where the customer or the owner of the controlling interest is a company listed on a stock Exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

5.40 ***Trusts (including occupational pension schemes) and nominees***

Where a lawyer is asked to act as trustees or nominees, the identity of all major parties should be verified. These include the trustees, the settlor and the principal beneficiaries.

5.41 Information which verifies the identity for legal arrangements:

(i) Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);

5.42 (ii) Other types of legal arrangements – the identity of persons in equivalent or similar positions.

Trust and nominee accounts are a popular vehicle for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder. Particular care needs to be exercised when the accounts are set up in countries with strict bank secrecy or confidentiality rules. Trusts created in jurisdictions without equivalent money laundering or terrorist financing procedures in place will warrant additional enquiries.

5.43

Where a lawyer receives money on behalf of a trust, it is important to ensure that the source of the receipt is properly identified, that the nature of the transaction is understood, and that payments are made only in accordance with the terms of the trust and are properly authorised in writing by the trustee.

5.44

In the case of occupational pension schemes, the identity of the principal employer should be verified, and also (by inspecting the scheme's trust documents) that of the trustees. There is no need to verify the identity of those who are to receive scheme benefits, unless the lawyer is to give them advice individually.

Clubs, societies and charitable institutions

5.45 Where the applicant is a club, a society or a charitable institution, the lawyer should examine and find out the purpose of its operation and ensure its legality requesting the provision of its constitution and the Certificate of Registration issued by the relevant Government Authority. In addition, the lawyer should verify the identity of all signatories in accordance with the established procedure of verifying the identity of natural persons.

Local authorities and other public bodies

5.46 Where the applicant for business is a local authority or other public body, the lawyer should obtain a copy of the resolution authorising the undertaking of the relevant transaction. Evidence that the individual dealing with the lawyer has the relevant authority to act should also be sought and retained.

Politically Exposed Persons(PEPs)

- 5.47 Lawyers should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. The requirements for all types of PEP should also apply to family members or close associates of such PEPs.
- 5.48 Lawyers are required, in relation to politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:
- (a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person. Examples of measures that could form part of such risk management systems include seeking relevant information from the client, referring to publicly available information or having access to commercial electronic databases of PEPs.
 - (b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
 - (c) conduct enhanced on-going monitoring of the business relationship.
 - (d) establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs.
 - (e) conduct enhanced on-going monitoring on the business relationship.

Without prejudice to the above paragraph, the lawyer and particularly the compliance officer should put in place appropriate risk management procedures to enable him to determine whether a prospective customer is a politically exposed person. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for politically exposed persons, seeking and obtaining information from the customer himself or from publicly available information.

In the case of legal entities and arrangements, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute politically exposed persons. In case of identifying one of the above as a politically exposed person, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in the Law and the present Directive.

Non-execution or delay in executing a transaction

In case where a firm does not execute or delays in executing a transaction on behalf of a client, this shall not constitute breach of any contractual or other obligation of the firm towards its client, if it is due to the fact that satisfactory information in relation to the involved parties, the nature, the economic or the trading purpose of the transaction is not obtained or if there are suspicions that the money credited in the account or the transaction are possibly related to

money laundering or terrorist financing activities or to any other criminal offence.

6. **RECORD-KEEPING**

Statutory requirements

- 6.01 The Law requires, under Sections 58 and 68, lawyers to retain records concerning client identification and details of transactions for use as evidence in any possible investigation into money laundering or terrorist financing. This is an essential constituent of the audit trail procedures that the Law seeks to establish.
- 6.02 The records prepared and maintained by any lawyer on its client relationships and transactions should be such that:
- requirements of the legislation and the Directive are fully met, and
 - competent third parties will be able to assess the lawyer's observance of anti-money laundering and anti-terrorist financing principles and procedures.
- 6.03 Lawyers should be aware that they might be called upon to satisfy, within a reasonable time, any enquiries by MOKAS or relating to Court orders requiring disclosure of information.
- 6.04 The most important single feature of the Law in this area is that it requires relevant records to be retained for at least five years from the date when the lawyer's relationship with the client was terminated or a transaction was completed. Documents, data or information collected under the Client Due Diligence process should be kept up-to-date by the lawyers, through reviews of existing records, particularly for higher risk categories of clients or business relationships.

Documents verifying evidence of identity

- 6.05 The Law specifies, under Section 68, that, where evidence of a person's identity is required, the records retained must include the following:
- (a) A record that indicates the nature of a client's identity obtained in accordance with the procedures provided in the Law and which comprises either a copy of the evidence or which provides sufficient information to enable details as to the client's identity to be re-obtained.
 - (b) A record containing details relating to all transactions carried out for the account and on behalf of that person.
- 6.06 The prescribed record retention period is at least five years commencing with the date on which the relevant activity or all transactions taking place in the course of this activity were completed.
- 6.07 In accordance with the Law, the date when the relationship with the client has ended is the date of:
- (a) the carrying out of an one-off transaction or the last in the series of one-off transactions;
 - (b) the termination of the business relationship;

- (c) if the business relationship has not formally ended, the date on which the last transaction was carried out.

6.08 Where formalities to end a business relationship have not been undertaken, but a period of five years has elapsed since the date when the last transaction was carried out, then the five year retention period commences on the date of completion of all activities taking place in the course of the last transaction.

Transaction records

6.09 Lawyers should maintain, for at least five years after the business relationship has ended, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from MOKAS. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved) so as to provide, if necessary, evidence for prosecution of criminal activity.

6.10 For each transaction, consideration should be given to retaining a record of:

- the name and address of its client and copies or records of official identification documents (such as passports, identity cards, or driving licences);
- the name and address (or identification code) of its counter party;
- the form of instruction or authority;
- the account details from which any funds were paid;
- the form and destination of payment made by the business to the client; and
- business correspondence.

Format and retrieval of records

6.11 It is recognised that the retention of hard-copy evidence creates excessive volume of records to be stored. Therefore, retention may be in formats other than original documents, such as electronic or other form. The overriding objective is for the firms to be able to retrieve the relevant information without undue delay and in a cost effective manner. The MLCO and other appropriate staff should have timely access to client identification data and other Client Due Diligence information, transaction records and other relevant information.

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

6.13 Section 47 of the Law requires that where relevant information is contained in a computer, the information must be presented in a visible and legible form which can be handed over to MOKAS.

Due diligence and client identification procedures and record keeping for countries outside the European Economic Area

6.14 Firms which have branches and subsidiary companies established in third countries outside the European Economic Area, must apply in those branches and subsidiary companies measures and procedures for due

diligence, client identification and record keeping, equivalent to those provided for in this Directive and in the directives issued by the relevant competent Supervisory Authorities.

- 6.15 Where the measures and procedures required by the legislation of the third country and the directives of the Supervisory Authority of the third country differ from those provided for in this Directive and in the directives of the competent Supervisory Authority of Cyprus, then the branch and/or the subsidiary company established in the third country, must apply the stricter requirements of the two.
- 6.16 In the event the legislation of the third country does not allow the application of equivalent measures as provided above, a firm which maintains a branch and/or a subsidiary company in the third country, is required:
- (i) to inform the competent Supervisory Authority immediately, and
 - (ii) to take additional measures in order to mitigate the risk of money laundering or terrorist financing.
- 6.17 Firms must notify their branches and subsidiary companies established in third countries of the policy and procedures they apply according to Section 58 of the Law for the prevention of money laundering and terrorist financing offences.

Offence of providing false or misleading evidence or information and false or forged documents

- 6.18 In the event that a client of a firm, or a person who is authorised to act on behalf of the client, or a third party according to Section 67(2)(a) of the Law, on whom the firm relies for the performance of the procedures for client identification and due diligence measures, knowingly provides false or misleading evidence or information for the identity of the client or of the ultimate beneficial owner or provides false or forged identification documents, is guilty of an offence and, in case of conviction, is subject to imprisonment not exceeding 2 years or to a pecuniary penalty of up to €100.000 or to both of these penalties.

7. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

Recognition of suspicious transactions

7.01 As the types of transactions which may be used by those exercising money laundering or terrorist financing are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a client's known, legitimate business or personal activities or with the normal business for that type of client. Therefore, the first key to recognition is knowing enough about the client's business to recognise that a transaction, or series of transactions, is unusual.

7.02 Questions that a lawyer might consider when determining whether an established client's transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the client?
- Is the transaction reasonable in the context of the client's business or personal activities?
- Has the pattern of transactions conducted by the client changed?

7.03 Warning signs which can indicate that an established client's transactions might be suspicious include:

- The size of the transaction (or transactions when aggregated) is inconsistent with the normal activities of the client.
- The transaction is complex, unusual or of unusual pattern with no apparent or visible economic or lawful purpose.
- The transaction is not reasonable in the context of the client's business or personal activities.
- The pattern of transactions conducted by the client has changed.
- The transaction is international in nature and the client has no obvious reason for conducting business with the other country involved.

7.04 Sufficient guidance must be given to staff to enable them to recognise suspicious transactions. The type of situations giving rise to suspicions will depend on a lawyer's client base and range of services and products. A lawyer might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating, from time to time, internal instructions and guidelines.

Reporting of suspicious transactions

7.05 The Law requires, under Section 27, that a person having any knowledge or suspicion that another person is involved in a money laundering or terrorist financing offence and who has become aware of the information on which the knowledge or reasonable suspicion is based in the course of his occupation, profession or business, commits an offence in case he does not promptly disclose such information to MOKAS as soon as reasonably practicable. Failure to disclose information which the lawyer has become aware of and which is privileged information does not constitute an offence. The Law also provides, under Section 26, that such a disclosure cannot be treated as a breach of the duty of confidentiality owed by lawyers to their clients by virtue of the contractual

relationship existing between them and the lawyers will not accept any responsibility towards the clients involved.

- 7.06 The Law also recognises, under Section 26, that, in certain instances, the suspicions may arise after the transaction or service has been completed and, therefore, allows subsequent disclosure provided that such disclosure is made on the concerned person's initiative and as soon as it is reasonable for him/her to make such disclosure.
- 7.07 The Law requires, under Section 69, that firms establish internal reporting procedures and that they identify a person (hereinafter to be referred to as "the Money Laundering Compliance Officer" ("MLCO")) to whom employees should report their knowledge or suspicion of transactions or activities involving money laundering or terrorist financing. In case of a firm's employees, the Law recognises, under Section 26, that internal reporting to the MLCO will satisfy the reporting requirement imposed by virtue of Section 27 i.e. once the employee has reported his/her suspicion to the MLCO he/she is considered to have fully satisfied his/her statutory requirements, under Section 27.
- 7.08 Some lawyers may wish to include in their client agreements, or in the terms of their business letters, a passage which places clients on notice of potential reporting obligations. While this could refer specifically to suspicions of money laundering or terrorist financing, lawyers may prefer a generalised form of wording which would extend to other matters where reporting to regulators etc. is required or necessary. It is also a useful precaution to include a statement that Cyprus law will govern the provision of the lawyer's services and that the Cypriot Courts will have exclusive jurisdiction over any dispute.

Appointment and role of the Money Laundering Compliance Officer (MLCO)

- 7.09 In accordance with the provisions of Section 69 of the Law, all lawyers should proceed with the appointment of a Money Laundering Compliance Officer. The MLCO should belong to the management of the firm so as to command the necessary authority.
- 7.10 Where it is deemed necessary due to the volume of the services/activities, assistants of the MLCO are appointed for the purpose of assisting the MLCO and passing internal suspicion reports to him.
- 7.11 The Firm communicates to the Cyprus Bar Association the names and positions of persons it appoints, as MLCO and assistants of the MLCO.
- 7.12 As a minimum, the MLCO's duties include the following:
- (a) To design, the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing.
 - (b) To develop and establish the firm's anti-money laundering policy, the customers' acceptance policy and risk management and procedures manual regarding money laundering and terrorist financing. (The Manual). The said manual has to be submitted to the Board of Directors/senior management for consideration and approval and includes, inter alia, the

details referred to in paragraph 7.13. The role and responsibilities of the MLCO should be clearly specified and documented in the manual. The MLCO should be allowed direct and timely access to all documents, data and information possessed by the lawyer and which may assist him/her in carrying out his/her duties. The manual is assessed on a periodic basis and reviewed when deficiencies are found or when there is a need to adapt the firm's procedures for the effective management of the risks emanating from money laundering and terrorist financing. Any reviews of the manual will receive the approval of the Board of Directors/senior management. The manual is communicated to all employees and especially those who handle, monitor or control in any way the customer transactions and are responsible for implementing the policies, procedures and controls adopted.

- (c) To receive from the employees information which is considered by the latter to be knowledge of money laundering or terrorist financing activities or which is cause for suspicion connected with money laundering or terrorist financing.
- (d) To validate and consider the information received as per paragraph (c) above by reference to any other relevant information and discuss 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 recorded and retained on file.
- (e) If following the evaluation described in paragraph (d) above, the MLCO decides to notify MOKAS, then he/she should submit a report online through the system "goAML Professional Edition". The Law stipulates specifically that the obligation for reporting to MOKAS extends to any attempt by somebody to carry out suspicious transactions.
- (f) If following the evaluation described in paragraph (d) above, the MLCO decides not to notify MOKAS, then he/she should fully document the reasons for such a decision.
- (g) To act as a first point of contact with MOKAS, for example upon commencement of and during investigation as a result of filing a report to MOKAS under (e) above.
- (h) To respond to requests and queries from MOKAS and the Cyprus Bar Association.
- (i) To provide advice and guidance to other employees on money laundering and terrorist financing matters.
- (j) To acquire the knowledge and skills required, which should be used to improve the firm's internal procedures for recognizing and reporting

money laundering and terrorist financing suspicions.

- (k) To provide ongoing training and education to employees for the purpose of preventing money laundering and terrorist financing and organize appropriate training sessions/seminars.
- (l) To receive training, guidance and education in relation to compliance, at least 6 hours per year.
- (m) To ensure the preparation and maintenance of the lists of customers categorized as low – medium – high risk, which contains, inter alia, the names of customers, their account number and the date of commencement of the business relationship. Moreover, to ensure the updating of the said lists with all new or existing customers, in the light of additional information obtained.
- (n) To detect, record and evaluate at least on an annual basis, all risks arising from existing and new customers and updates and amends the systems and procedures applied by the firm for the effective management of the aforesaid risks.
- (o) To evaluate the systems and procedures applied by a 3rd person on whom the firm relies for customer identification and due diligence purposes and approves the cooperation with the 3rd person.
- (p) To ensure that the branches of the firm that operate in countries outside the EEA have taken all necessary measures for achieving full compliance with the provisions of the present Directive, in relation to customer identification, due diligence and record keeping procedures.
- (q) To prepare annual report as per paragraphs 7.14 & 7.15 below.

7.13 The Manual covers, inter alia, the lawyer's ML policy, the customer acceptance policy, the duties and responsibilities of the MLCO, Board of Directors and employees, the procedures followed for entering into business relationships, for the execution of individual transactions, for account opening and customer due diligence procedures, including the documents and information required for the establishment of the business relationship and trade execution procedures of record keeping, for on-going monitoring of accounts and transactions, for detecting and reporting unusual and suspicious transactions, for risk assessment of the lawyers' operations, for the overall education/training program of the lawyer.

- 7.14 (a) The Annual Report is significant tool for assessing the firm's level of compliance with its obligations laid down in the Law and the present Directive.
- (b) The Annual Report is submitted to the Board within two months from the end of each calendar year for approval.
- (c) After its approval by the Board, the Annual Report together with its minutes of the meeting, during which the Annual Report has been discussed and approved, should be ready at any time to be inspected or submitted to the Cyprus Bar Association upon request by the Cyprus Bar Association. The said minutes include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.
- 7.15 The Annual Report deals with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, covers the following:
- (a) Information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the present Directive which took place during the year under review.
- (b) Information on the inspections and reviews performed by the MLCO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Lawyer applies for the prevention of money laundering and terrorist financing. In this regard, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation.
- (c) The number of internal suspicion reports submitted by the employees to the MLCO.
- (d) The number of Reports submitted by the MLCO to MOKAS.
- (e) Information on the policy, measures, practices, procedures and controls applied by the Lawyer in relation to high risk customers as well as the number and country of origin of high risk customers with whom a business relationship is established or an occasional transaction has been executed.
- (f) Information on the systems and procedures applied by the Lawyer for the ongoing monitoring of customer accounts and transactions.
- (g) Information on the measures taken for the compliance of branches and subsidiaries, with the requirements of the present Directive in relation to customer identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements.
- (h) Information on the training courses/seminars attended by the MLCO.
- (i) Information on training/education provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the 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.

(j) Information on the recommended next year's training program.

(k) Information on the structure and staffing of the department of the compliance officer for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

Internal reporting procedures and records

- 7.16 A lawyer should make the necessary arrangements in order to introduce appropriate measures designed to assist the functions of the Money Laundering Compliance Officer and the reporting of suspicious transactions by employees. Lawyers have an obligation to ensure:
- that they maintain an adequately resourced and independent audit function to test compliance (including sample testing) with procedures, principles and internal control systems;
 - that all their employees know to whom they should be reporting money laundering or terrorist financing knowledge or suspicion; and
 - that there is a clear reporting chain under which money laundering or terrorist financing knowledge or suspicion is passed without delay to the Money Laundering Compliance Officer.
- 7.17 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the MLCO. This ensures speed, confidentiality and accessibility to the MLCO. However, some lawyers may choose to require that unusual or suspicious activities or transactions be drawn initially to the attention of an appropriate partner to ensure that there are no known facts that will negate the suspicion before further reporting to the MLCO.
- 7.18 Such partners should also be aware of their own legal obligations. An additional fact which the partner supplies may negate the suspicion in the mind of the person making the initial report, but not in the mind of the partner. The firm's procedures should then require the partner to report to the MLCO. On the other hand, the partner should never attempt to prevent a member of staff who remains suspicious from reporting direct to the MLCO. Staff should be made aware that they have a direct route to the MLCO.
- 7.19 Larger firms may choose to appoint assistant MLCOs within departments or branch offices, to enable the validity of the suspicion to be examined before being passed to a central MLCO. In such cases, the role of the assistant MLCO must be clearly specified and documented. All procedures should be documented in appropriate manuals and job descriptions.
- 7.20 All suspicions reported to the MLCO should be documented (in urgent cases this may follow an initial discussion by telephone). In some firms it may be possible for the person with the suspicion to discuss it with the MLCO and for the report to be prepared jointly. In other firms the initial report should be prepared and sent to the MLCO. The report should include full details of the client and as full a statement as possible of the information giving rise to the suspicion.
- 7.21 The MLCO should acknowledge receipt of the report and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. to avoid "tipping off". All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to MOKAS, should be documented. This information may be required to supplement the initial report or as evidence of good practice and due diligence if, at some future date, there is an investigation and the suspicions are confirmed.

- 7.22 On-going communication between the MLCO and the reporting person, department or branch office is important. The lawyer may wish to consider advising the reporting person, department or branch office of the MLCO's decision, particularly if the reported suspicions are believed to be groundless. Likewise, at the end of an investigation, consideration should be given to advising all members of staff concerned of the outcome. It is particularly important that the MLCO is informed of all communications between the investigating officer and the lawyer at all stages of the investigation.
- 7.23 Records of suspicions which were raised internally with the MLCO, but not disclosed to the law enforcement agencies, should be retained for five years from the date of the transaction.

External reporting procedures

National reporting point for disclosures

- 7.24 All Money Laundering Compliance Officers' Reports to MOKAS are submitted online through a system called "goAML Professional Edition".

For more information on the new online reporting method, please contact MOKAS.

Method of reporting

- 7.25 The Association recommends the use of the standard form attached as Appendix B to this Directive, for the reporting of disclosures, but this is not mandatory. Disclosures can be forwarded by post or by facsimile message. In urgent cases, an initial telephone report can be made and subsequently confirmed in writing.
- 7.26 After filing of the report, lawyers should adhere to any instructions given to them by MOKAS and, in particular, as to whether or not to continue a transaction or continue providing the requested service or terminate the business relationship.

Nature of the information to be disclosed

- 7.27 Sufficient information should be disclosed, indicating the nature of and reason for the suspicion. If a particular offence is suspected, this should be stated to enable the report to be passed to the correct agency for investigation with the minimum of delay. Where the lawyer has additional relevant evidence that could be made available, the nature of this evidence might be indicated to enable the law enforcement agencies to obtain a production order, if necessary.

Constructive trust

- 7.28 The duty to report suspicious transactions and to avoid "tipping off" can lead to a conflict between the reporting lawyer's responsibilities under the criminal law and his obligations, under civil law, as a constructive trustee, towards a victim of fraud and other crimes.
- 7.29 A lawyer's responsibility as a constructive trustee arises when he comes to know that assets rightfully belong to a person other than his client. The firm then takes on the obligation of constructive trustee for the true owner. If the assets are dealt

with in a way which is inconsistent with the rights of the true owner, the civil law treats the firm as though it were a trustee for the assets, and holds the firm liable to make good the loss suffered. Having a suspicion which it considers necessary to report under the money laundering and terrorist financing legislation could be taken as indicating that it knows or should know that the assets belong to a third party.

7.30 In the normal course of events, a lawyer would not dispose of assets to a third party knowing himself to be in breach of trust. The concern in relation to money laundering or terrorist financing is that the lawyer will have reported his suspicion to MOKAS. He will, therefore, have no option but to act on the client's instruction, because by refusing to hand over the assets he might alert the perpetrator of, e.g. a fraud, and in doing so commit a tipping off offence under the money laundering and terrorist financing legislation.

7.31 The tipping off offence prohibits a lawyer from informing a suspected victim of crime that his assets are at risk, where to do so is likely to prejudice the investigation of a concealment offence. Given the absolute nature of the prohibition in the criminal law, if a lawyer makes a disclosure under the money laundering or terrorist financing legislation, and is acting in accordance with MOKAS or the investigating officer's instructions in disposing of the assets, some would regard the risk of the firm being held liable by a civil Court as constructive trustee to be minimal. However, to minimise the liability, the following procedures should be followed:

- When evaluating a suspicious transaction, the MLCO should consider whether there is a constructive trust issue involved. If the MLCO concludes that there is reason to believe that the lawyer may incur a liability as a constructive trustee, the precise reasons for this belief should be reported to MOKAS immediately, along with the other matters giving rise to suspicion that the assets relate to the proceeds of crime. The constructive trust aspects should be set out clearly in the "reason for suspicion" section of the standard reporting form, with "Potential Constructive Trust Issue" marked clearly at the top of this section. Neither the client nor any third party should be tipped off.
- On receipt of the report, MOKAS will evaluate the information and "fast track" the report to the appropriate investigator who will determine whether the "consent" to undertake the transaction can be issued.
- Where a suspicious transaction report has previously been made to MOKAS, and a potential constructive trust issue comes to light subsequently, MOKAS (or the designated investigator) should be provided with an immediate further report indicating the reasons why a constructive trust situation is believed to have arisen.
- It is essential to note that in all cases where the information or other matter on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, there is an obligation to disclose the information or other matter to MOKAS as soon as is reasonably practicable after it comes to his attention. Failure to make such a disclosure is a serious criminal offence.

Investigation of disclosures

- 7.32 Following receipt of a disclosure and initial research by MOKAS, the information disclosed is allocated to trained financial investigation officers of MOKAS for further investigation. Members should be aware that if they were to disclose money laundering or terrorist financing suspicions to any other person, this could amount to a breach of client confidentiality.

Confidentiality of disclosures

- 7.33 It is understood that in the event of a prosecution, the source of information supplied to MOKAS is protected as far as the disclosure of evidence rules allow so. Maintaining the integrity of the confidential relationship between law enforcement agencies and lawyers is considered by MOKAS to be of paramount importance. The origins of financial disclosures are not revealed because of the need to protect the disclosing lawyer and to maintain confidence in the disclosure system.

Feedback from the investigating authorities

- 7.34 MOKAS has stated that in cases of disclosure, it will make every effort to give feedback about the outcome. However, this does not prohibit the disclosing firm from contacting the case's investigator directly.

8. EDUCATION AND TRAINING

Statutory requirements

8.01 The Law requires, under Section 58, all lawyers to take appropriate measures to make employees aware of:

- principles and procedures maintained to prevent money laundering or terrorist financing including those relating to identification, record keeping and internal reporting, and
- the requirements imposed by the Law,

and, also, to provide such employees with training in the recognition and handling of suspicious transactions.

The need for awareness by partners and staff

8.02 The effectiveness of the procedures and recommendations contained in the various Directives on the subject of money laundering or terrorist financing depends on the extent to which the staff of law firms appreciates the serious nature of the background against which the Law has been enacted and are fully aware of their responsibilities. Staff must also be aware of their own personal statutory obligations. They can be personally liable for failure to report information in accordance with internal procedures. All staff must, therefore, be encouraged to co-operate and to provide a prompt report of any knowledge or suspicion of transactions or activities involving money laundering or terrorist financing. It is, therefore, important that lawyers introduce comprehensive measures to ensure that their staff is fully aware of their responsibilities.

8.03 All relevant staff should be educated in the importance of “Know your Client” requirements for money laundering or terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the client but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that client at the outset, in order to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a client’s transactions or circumstances that might constitute criminal activity.

Timing and content of training programmes

8.04 As a means of assistance in the discharge of their legal obligations, lawyers should refer to Part 7 of this Directive, which deals with the recognition, and reporting of suspicious transactions.

8.05 In addition to the above, lawyers are required to put in place strict screening procedures to ensure high standards when hiring employees and are expected to establish a programme of continuous training for all levels of their staff.

8.06 The timing, content and methods of training for the various levels/types of staff should be tailored to meet the needs of the particular firm, depending on the size and nature of the organisation and its available time and resources.

8.07 It will also be necessary to make arrangements for refresher training at regular intervals, to ensure that staff do not forget their responsibilities.

New professional staff

8.08 A general appreciation of the background to money laundering or terrorist financing, and of the procedures for reporting any suspicious transactions to the MLCO, should be provided to all new professional staff that will be dealing with clients or their affairs, irrespective of the level of seniority. They should be made aware of the importance placed by the firm on the reporting of suspicions and that reporting is an obligation on them as individuals.

Advisory staff

8.09 Members of staff who deal directly with clients are likely to be the first point of contact with potential money launderers or terrorist financiers, and their efforts are therefore vital to the lawyer's reporting system. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction or activity is deemed to be suspicious.

Staff who can accept new clients

8.10 Those members of staff who are in a position to accept new clients must receive the training recommended for advisory staff. In addition, the need to verify the identity of the client must be understood, and training should be given in the firm's client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction or provide a service in connection with a suspicious activity may need to be reported to the MLCO, whether or not the funds are accepted or the transaction proceeded with. They must also know what procedures to follow in these circumstances.

Partners and managers

8.11 A higher level of instruction covering all aspects of money laundering or terrorist financing procedures should be provided to those with the responsibility for supervising or managing staff. This will include:

- the offences and penalties arising from the legislation for non-reporting and for assisting money launderers or terrorist financiers;
- the recognition of a valid Court order requiring information, and the circumstances when information should be declined without such an order;
- internal reporting procedures; and
- the requirements for verification of identity and the retention of documents.

Money Laundering Compliance Officers

- 8.12 For larger firms, or those with complex procedures, in-depth training concerning all aspects of the legislation, the Directive and internal policies will be required for the MLCO. In addition, the MLCO will require extensive initial and on-going instruction on the validation and reporting of suspicious transactions, on the feedback arrangements and on new trends and patterns of criminal activity. For small firms, the MLCO or sole practitioner should have at least the level of knowledge identified above for partners and managers. When money laundering or terrorist financing becomes an issue, further advice or assistance is available from the Association.

Refresher training

- 8.13 It will also be necessary to make arrangements for refresher training at regular intervals, to ensure that staffs do not forget their responsibilities. Some lawyers may wish to provide such training on an annual basis; others may choose a shorter or longer period or may wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

Methods of providing training

- 8.14 There is no standard preferred way to conduct training for money laundering or terrorist financing purposes. The training should be tailored to meet the needs of the particular firm, depending on its size and nature.
- 8.15 The Law does not require lawyers to purchase specific training materials for the purpose of educating relevant staff in money laundering or terrorist financing prevention and the recognition and reporting of suspicious transactions.
- 8.16 Lawyers should establish on-going employee training to ensure that employees are kept informed of new developments, including information on current money laundering and terrorist financing techniques, methods and trends.

APPENDIX A **(Paragraph 1.01)**

Articles 1 to 4 of the Council Framework Decision of 13 June 2002 on combating terrorism

Article 1

Terrorist offences and fundamental rights and principles

1. Each Member State shall take the necessary measures to ensure that the intentional acts referred to below in points (a) to (i), as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation where committed with the aim of:
 - seriously intimidating a population, or
 - unduly compelling a Government or international organisation to perform or abstain from performing any act, or
 - seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation,shall be deemed to be terrorist offences:
 - (a) attacks upon a person's life which may cause death;
 - (b) attacks upon the physical integrity of a person;
 - (c) kidnapping or hostage taking;
 - (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
 - (e) seizure of aircraft, ships or other means of public or goods transport;
 - (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons;
 - (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;
 - (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;
 - (i) threatening to commit any of the acts listed in (a) to (h).

2. This Framework Decision shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.

Article 2

Offences relating to a terrorist group

1. For the purposes of this Framework Decision, "terrorist group" shall mean: a structured group of more than two persons, established over a period of time and acting in concert to commit terrorist offences. "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

2. Each Member State shall take the necessary measures to ensure that the following intentional acts are punishable:
 - (a) directing a terrorist group;
 - (b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Article 3

Offences linked to terrorist activities

Each Member State shall take the necessary measures to ensure that terrorist-linked offences include the following acts:

- (a) aggravated theft with a view to committing one of the acts listed in Article 1(1);
- (b) extortion with a view to the perpetration of one of the acts listed in Article 1(1);
- (c) drawing up false administrative documents with a view to committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

Article 4

Inciting, aiding or abetting, and attempting

1. Each Member State shall take the necessary measures to ensure that inciting or aiding or abetting an offence referred to in Article 1(1), Articles 2 or 3 is made punishable.
2. Each Member State shall take the necessary measures to ensure that attempting to commit an offence referred to in Article 1(1) and Article 3, with the exception of possession as provided for in Article 1(1)(f) and the offence referred to in Article 1(1)(i), is made punishable.

