Prevention and Suppression of Money Laundering Activities

Directive to the Members of ICPAC

pursuant to Section 59(4) of The Prevention and Suppression of Money Laundering Activities Law of 2007 as amended in 2010, 2012 and 2013

The Institute of Certified Public Accountants of Cyprus

PREFACE

This Directive is issued by the Council of the Institute of Certified Public Accountants of Cyprus (ICPAC), appointed by the Council of Ministers on 7 March 2001 as the Supervisory Authority for auditors, external accountants, tax advisors and trust and company service providers, 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 by Laws L58(I)/2010, L80(I)/2012, L192(I)/2012 and L101(I)/2013 (consolidated hereafter referred to as the "Law").

The Law, in line with Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 and Commission Directive 2006/70/EC of 1 August 2006, constitutes the obligations and responsibilities for implementation by professionals, including auditors, external accountants, tax advisors and trust and company service providers, of measures against money laundering and combating the financing of terrorism.

This Directive deals with the statutory and professional requirements in relation to the avoidance, recognition and reporting of money laundering and terrorist financing activities.

In the preparation of this Directive, consideration was given to the Financial Action Task Force (FATF) Recommendations and the Risk-based Approach Guidance issued by FATF in June 2008 for Accountants and for Trust and Company Service Providers. The International Monetary Fund staff recommendations emanating from their "Risk-based Analysis of Cyprus Anti-money Laundering Regime" report dated 10 October 2012, the "Special Assessment of the Effectiveness of Client Due Diligence Measures in the Banking Sector of Cyprus" report dated 24 April 2013 by the MONEYVAL Committee of the Council of Europe, and Deloitte's "Third Party Anti-Money Laundering (AML) Assessment of the Effective Implementation of Client Due Diligence (CDD) Measures with Regard to Cyprus' Deposits and Loans" report dated 14 June 2013, were also taken into consideration.

The present Directive replaces the "Prevention of Money Laundering and Terrorist Financing" Directive to the members of ICPAC, issued by the Council of the Institute in December 2011.

September 2013

TABLE OF CONTENTS

CHAPTERS

CHAPTER 1

BACKGROUND

1.01 All auditors, external accountants, tax advisors and trust and company service providers, as well as their staff, whether they work in practice or elsewhere, must be aware of The Prevention and Suppression of Money Laundering Activities Law of 2007 L188(I)/2007 as amended in 2010, 2012 and 2013 by Laws L58(I)/2010, L80(I)/2012, L192(I)/2012 and L191(I)/2013 (consolidated hereafter referred to as the "Law"). Individuals who are not aware of the Law, and the senior management of firms which do not apply the necessary procedures, put themselves at risk of criminal prosecution. Failure to comply can result in up to 14 years imprisonment and/or a fine of up to €500.000.

Terminology

1.02 Some of the basic terms that are used throughout this Directive are defined or explained as follows:

Advisory Authority	The Advisory Authority for Combating Money Laundering Offenses and terrorist financing offenses 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 percentage of the shares or voting rights in that legal entity, including through bearer share holdings, a percentage 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	A business, professional or commercial relationship which is connected with the professional activities of persons engaged in financial and other business activities in accordance with the Law, and which is expected, at the time when the contact is established, to have an element of duration.
Client	A person who seeks to form a business relationship or to conduct a single one-off transaction with another person engaged in financial or other business activities in or from the Republic of Cyprus.

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 (see paragraph 3.02).
criminal conduct	See paragraphs 2.22 to 2.24.
EU Directive	(a) Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. (b) Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of "politically exposed person" and the technical criteria for simplified client due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.
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 May 1992 and was adapted by the Protocol which was signed in Brussels on 17 May 1993, as the said agreement is further amended from time to time.

Financial Action Task Force; FATF	An inter-governmental body, the objectives of which are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. It has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism, which form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.
know; knowledge	See paragraph 2.25.
MOKAS	The Unit for Combating Money Laundering (see paragraph 7.23).
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), a Committee of the Council of Europe, is an evaluation and peer pressure mechanism, aiming to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields. MONEYVAL also conducts typologies studies of money laundering and terrorist financing methods, trends and techniques.

person	Any natural or legal person.
politically exposed persons	Natural persons who are or have been entrusted with prominent public functions in the Republic of Cyprus or in another foreign country, and their immediate family members or persons known to be close associates of such persons.
prescribed activities and services	The activities and services referred to in Section 2 of the Law.
property	Movable and immovable property whether situated in the Republic of Cyprus or abroad.
suspect; suspicion	See paragraphs 2.27 to 2.30.
terrorist financing	The provision or collection of funds, by any means, directly or indirectly, with the intention that they shall be used or in the knowledge that they are to 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/HA of 13 June 2002 on combating terrorism (Appendix A).
the Institute; ICPAC	The Council of the Institute of Certified Public Accountants of Cyprus.
the Law	The Prevention and Suppression of Money Laundering Activities Law of 2007 L188(I)/2007 as amended in 2010, 2012 and 2013 by Laws L58(I)/2010, L192(I)/2012, 80(I)/2012 and 101(I)/2013.
third country	A country which is not a member of the European Union or party to the Agreement for the European Economic Area, which was signed at Oporto on 2 May 1992 and was amended by the Protocol which was signed in Brussels on 17 May 1992, as this Agreement is further amended.

unit trust	Any trust established for providing persons who have funds available for investment facilities, the right to participate as beneficiaries under the trust in any profits or income arising from the acquisition, management or disposal of any property.

1.03 The word “firm” is used throughout to include sole practitioner, partnership and company involved in the provision of audit, external accounting, tax advisory and trust and company administration services. References to “partner" include sole practitioners and directors of companies, except where indicated otherwise.

Introduction

1.04 The fight against crime demands that criminals are prevented from legitimising the proceeds of their crime by the process of “money laundering or terrorist financing”. It is a process which can involve many parties, other than the more obvious targets being banks and other financial institutions. Professionals such as auditors, external accountants, tax advisors, providers of trust and company administration services, 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,
- gaming activities,
- company formation agents,
- dealers in precious metals and bullions, and
- antique dealers, car dealers and others selling high value commodities and luxury goods.

1.05 The primary relevant legislation in Cyprus is The Prevention and Suppression of Money Laundering Activities Law of 2007 L188(I)/2007 as amended in 2010 and 2012 by Laws L58(I)/2010 and L192(I)/2012 respectively – the “Law”. The criminal offences which it involves can be summarised as follows:

- Acquiring, possessing or using the proceeds of criminal conduct.
- Concealing or transferring the proceeds of criminal conduct.
- Assisting another person to retain the benefit of criminal conduct.
- Tipping off suspects or others about a money laundering or terrorist financing investigation.
- Failing to report knowledge or suspicion of money laundering or terrorist financing. The failure is punishable on conviction by up to 5 years imprisonment or a fine of up to €50.000, or both of these penalties.

1.06 All auditors, external accountants, tax advisors and trust and company service providers, as well as their staff, whatever the nature of their work, must be aware of the scope of these potential offences. Chapter 2 discusses the last three in more detail.

1.07 Failure to comply with any of the requirements of the Law, by a firm to which they apply, is subject to an administrative fine of up to €200.000 which is imposed by the competent supervisory authority. Where the offence continues, an additional administrative fine of up to €1.000 is imposed for every day that the offence continues. Furthermore, an auditor, external accountant, tax advisor, or trust and company service provider who fails to comply with the requirements of the Law is referred to the Disciplinary Committee of the Institute for disciplinary action. This is irrespective of whether money laundering or terrorist financing has taken place.

1.08 In October 2005 the European Parliament and the Council adopted Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. This brings more professional activities within the scope of the preventive measures against money laundering and terrorist financing as stipulated in the law of member states. Cyprus has harmonised its legislation with the EU Directive.

Scope of this Directive

1.09 All auditors, external accountants, tax advisors and trust and company service providers, as well as their staff, must avoid committing the statutory criminal offences summarised in Chapter 2 of this Directive. Those who carry on the activities and services prescribed in Section 2 of the Law also 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 include a wide range of financial and other activities, but those most likely to be relevant to firms 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 and advice,
- providing safe custody services,
- conducting any other investment business,
- providing any services to clients including audit, accounting/ bookkeeping, tax advice, and trust and company administration.

1.10 Section 2 of the Law under “other activities” prescribes, amongst other, the following:

- Exercise of professional activities by auditors, external accountants and tax advisors, including transactions for the account of their customers in the context of carrying out financial business.

- Any of the services or activities set out in Article 4 of the Law Regulating Companies Providing Administrative Services and Related Matters.

1.11 In determining whether a firm has complied with the requirements of the Law, a relevant directive issued or approved by a supervisory or regulatory body, or in its absence, a directive issued or approved by a trade association or other representative body should be taken into account. The present Directive has been prepared taking account of this fact and to give a practical interpretation of the Law.

1.12 Most services provided by firms are likely to be of use in one way or another to money launderers or terrorist financiers. Firms risk damaging their reputation and business if they become involved in any way with money launderers or terrorist financiers, even unintentionally.

1.13 Firms will appreciate that there are practical benefits in applying standard practice by all their partners and staff and across their entire range of services. Consistency of approach ensures complete coverage of the areas mandated by the Law and avoids difficulties with clients and people who receive or provide services.

1.14 For example, standard procedures to require 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 primary legislation.

Members employed outside the practice

1.15 While this Directive has been prepared primarily with firms and members employed in practice in mind, much of the material, particularly Chapter 2 of the Directive, will also apply to members of the Institute employed elsewhere. Members employed in banking and financial services should refer, where necessary, to the directives published by the Central Bank of Cyprus, the Cyprus Securities and Exchange Commission, the Superintendent of Insurance and the Commissioner of Co-operative Societies. Members employed in other sectors which might be of use to a money launderer or a terrorist financier, may also find that a directive is available from their respective regulator. In the absence of a relevant directive, members should consider the procedures recommended for firms in this Directive, and adapt them for their own circumstances as appropriate.

What is money laundering?

1.16 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, with their "dirty" funds coming to appear "clean".

1.17 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

1.18 There are many methods 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.

1.19 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.

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

1.21 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 accountants to money laundering or terrorist financing

1.22 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 audit and accounting services and a whole range of financial, tax and business advice. Some areas of an accountant'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 Institute

1.23 Supervisory authorities (such as the Institute which is a designated supervisory body under the Law) have specific obligations under the Law to report to the Unit for Combating Money Laundering (MOKAS) any information they obtain which in their opinion is, or may be, indicative of money laundering or terrorist financing.

1.24 Furthermore, the Institute is interested in the measures employed to counter money laundering or terrorist financing, because of the damage which firms and their clients, as well as the reputation of the profession as a whole, can suffer from it. Therefore, there may be occasions when it will be appropriate for action taken in relation to money laundering or terrorist financing by both firms and individuals to be taken into account by the Institute in undertaking its regulatory and disciplinary functions.

1.25 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 of the Institute and of the adequacy of their control systems for guarding against money laundering or terrorist financing.

CHAPTER 2

THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007 AS AMENDED IN 2010 AND 2012 (THE "LAW")

Introduction

2.01 The main purpose of this Law which came into effect on 1 January 2008 and was subsequently amended on 25 June 2010, 27 June 2012, 21 December 2012 and 9 September 2013, 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 which are of direct interest to auditors, external accountants, tax advisors and trust and company service providers, as well as their staff, are given below.

Prescribed offences (Section 3 of the Law)

2.02 The Law has effect in respect to 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 represents proceeds from a predicate offence, is guilty of an offence if he does any of the following:

(a) converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin, or of assisting any person who is involved in the commission of a predicate offence to evade the legal consequences of his actions,
(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 that are being performed for money laundering or terrorist financing offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from having commissioned the said offence.

2.04 Commissioning of the above offences is punishable on conviction by 14 years imprisonment or a fine of up to €500.000 or both of these penalties, in the case of a person who knows that the property is proceeds from a predicate offence, or by 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 person to commit a money laundering offence or terrorist financing, it is in his defense if 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 restriction upon the disclosure of information imposed by a contract.

2.06 In the case of employees of persons whose activities are supervised by one of the Authorities defined in Section 59, the Law recognises that the disclosure may be made to a 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,
(b) terrorist financing offences, including collection of money for financing of persons or organisations 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, whether the predicate offence is subject to the jurisdiction of the Cyprus Courts or not (Section 4(2) of the Law), is of no significance.

Failure to report (Section 27 of the Law)

2.09 Any person, including an auditor, external accountant, tax advisor or trust and company service provider, in practice or elsewhere, 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, commits an offence if he does not 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 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 under the section on money laundering or terrorist financing offences above (paragraph 2.03), 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 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 are carrying out investigations and searches for money laundering or terrorist financing. "Tipping-off" under these circumstances is punishable by imprisonment not exceeding 5 years.

(b) Irrespective of the provisions of Section 48 of the Law, persons who act as professional auditors, external accountants, tax advisors, trust and company service providers, and lawyers, 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 is carrying out or may carry out an investigation for money laundering or terrorist financing offences.

"Third countries" for the purposes of this paragraph means third countries which according to the decision of the Advisory Authority for Suppression of Money Laundering and Terrorist Financing Activities have been specified as imposing procedures and measures for suppression of money laundering and terrorist financing corresponding to the requirements of the EU Directive.

(c) The persons mentioned in paragraph 2.10(b) above may exchange information between them which concerns 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 paragraph 2.10(b) above) and that the persons who exchange information belong to the same professional branch. The information exchanged should be used exclusively for the prevention of money laundering or terrorist financing activities.

(d) The disclosure and exchange of information made in accordance with paragraphs 2.10(b) and 2.10(c) above is not considered as a violation of any contractual or other legal limitation on the 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 a violation of any contractual or other legal limitation on the disclosure of information.

(f) According to Section 48 of the Law and Article 28(6) of the EU Directive, where a firm seeks to dissuade a client from engaging in an illegal activity, this shall not constitute disclosure of information to the client concerned or to any other third party (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 services activities, and (b) those carrying out other activities, including auditors, external accountants, tax advisors, trust and company service providers, and lawyers, for the effective prevention of money laundering and terrorist financing activities, 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 payment 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 the 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 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 insurance contracts, 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 II of the Third Schedule to the Investment Services and Activities and Regulated Markets Law, which are provided in connection with financial instruments which are listed in Part II of the same Schedule, those specified in Article 109 of the Open-Ended Undertakings of Collective Investments in Transferable Securities (UCITS) Law, and those set out in paragraphs 5 and 6 of Article 6 of the Alternative Investment Fund Managers Law.

(15) Life insurance and mediation for the conclusion of life insurance policies.

(16) Without prejudice to the generality of paragraphs (4) and (5), any of the services set out in the Appendix to the Payment Services Law.

(b) Other activities

The professional activities exercised by the following legal or natural persons:

(1) Auditors, external accountants and tax advisors.

(2) Lawyers – when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- opening or management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of trusts, companies and similar structures, and buying and selling of business entities.

(3) Trust and company services providers – if not already covered under points (1) and (2) above – when providing any of the following services to third parties:

- forming companies or other legal persons;
- acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- 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 arrangement;
- acting as, or arranging for another person to act as, a trustee of an express trust or a similar legal arrangement;
- acting as, or arranging for another person to act as, a nominee shareholder for another person.

(4) Real estate agents – when they are involved in transactions for their client concerning the buying and selling of real estate.
(5) Dealers in precious metals or precious stones – when they engage in any cash transaction with a customer equal to or above €15.000.

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 sufficient and appropriate systems or 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:

(a) to facilitate the recognition and reporting of suspicious transactions, and
(b) to ensure through the strict implementation of the procedures of due diligence regarding the client and the maintenance of adequate record keeping procedures, should a client come under investigation by MOKAS, that the firm is able to provide its part of the audit trail, as well as provide the necessary elements regarding the source, origin and destination of the illicit money, and details of the client's identity in its possession.

2.13 The Law requires that all persons carrying out financial or other activities establish and implement systems and procedures in connection with the following:

- Client identification and due diligence procedures.
- Record-keeping procedures in relation to clients' identity and their transactions as specified in Section 68 of the Law.
- Procedures of internal reporting to a competent person (e.g. a 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 per the provisions of Section 69 of the Law.
- Other internal control and risk assessment procedures for the purpose of preventing money laundering and terrorist financing.
- Thorough examination of each transaction which, by its nature, may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing, and in particular complex or unusually large transactions and all other unusual patterns of transactions which are carried out with no apparent economic or visible lawful purpose.
- Measures for making employees aware of all the procedures mentioned in this section to prevent money laundering and terrorist financing and of the legislation and EU Directives relating to money laundering and terrorist financing.

- Provision of regular 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 Institute as the Supervisory Authority for the professional activities of auditors, external accountants and tax advisors, including trust and company service providers. It is clarified that, for trust and company service providers, the Institute has the legal authority for supervising its members as well as their staff in relation to compliance with the avoidance, recognition and reporting of money laundering and terrorist financing activities, unless such members elect to be authorised and licensed under the Law Regulating Companies Providing Administrative Services and Related Matters of 2012 L196(I)/2012.

2.15 The Institute, in its capacity as Supervisory Authority for the purpose of prevention of money laundering and terrorist financing, and for the purpose of achieving the objectives of the Law, is empowered under Section 59(4) of the Law to issue directives to its members in this respect. The purpose of this Directive is to determine the details of the requirements of the Law in respect of business carried on by firms, and the way of implementing the provisions of the Law by the persons under supervision, as well as provide guidance on good business practice in this respect. This Directive highlights the obligation for establishing and implementing procedures and systems for the effective mitigation and prevention of the risk of committing or attempting to commit money laundering and terrorist financing activities.

2.16 The Directive is binding and obligatory as to its adoption by the persons to whom it is addressed. The Institute follows up, supervises and evaluates the adoption of Part VIII of the Law and of this Directive.

2.17 According to Section 59(6) of the Law, the Institute may take all or any of the following measures in case an auditor, external accountant, tax advisor or trust and company service provider fails to comply with the provisions of Part VIII of the Law, or the Institute's directives issued under section 59(4) of the Law, or Regulation No. 1781/2006 of the European Parliament and the Council of the European Union of 15 November 2006 on information on the payer accompanying transfers of funds:

(a) To request the supervised person to take such measures within a specific time as the Institute may decide, for the remedy of the situation.
(b) After giving the supervised person the opportunity to be heard, to impose an administrative fine of up to €200.000. In case the offence continues, to impose an additional fine of up to €1.000 per day for as long as the offence continues. The Institute may, at its discretion, publicise the imposition of an administrative fine.
(c) To amend or suspend or cancel the operation license of the supervised person.

(d) To require the cessation or removal from his/her position, any director, manager or officer, including the Compliance Officer and the heads of internal audit and regulatory compliance, in the event that the breach was due to his/her own fault, willful omission or negligence.

(e) To impose the administrative penalty referred to in (b) above to a director, manager or officer or any other person, in the event that the breach was due to his/her own fault, willful omission or negligence.

2.18 An auditor, external accountant, tax advisor or trust and company service provider who fails to comply with the provisions of Section 59 of the Law and the directives issued by the Institute, is referred to the Institute's Disciplinary Committee.

2.19 Where the Institute has information and believes that a person is involved in money laundering or terrorist financing activities, it has a legal obligation to disclose the relevant information to MOKAS.

2.20 The Institute may exchange information with MOKAS, in the context of its obligations arising from the Law.

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

2.21 Courts in Cyprus may, on application by the investigator, make an order for the disclosure of information by a person, including a firm, 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 7.07 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 which may constitute the subject of a money laundering offence and which are punishable with imprisonment exceeding one year.

2.24 The Law does not impose a duty on firms 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 it occurred in Cyprus. Firms 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 circumstances permit, legal advice should be obtained. 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 an example, they raise the questions:

- Should an accountant 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 an accountant suspect that assets are or represent the proceeds of criminal conduct?

2.28 Suspicion falls far short of proof based on well-founded 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 7.05 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 belief that funds derive from money laundering or terrorist financing, and to matters on which that suspicion or belief is based. If in doubt, firms 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 firm comes to know that property belongs to a person other than its client, it 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 firm comes to know that property belongs not to its client but to a third party:

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

2.33 Paragraph 2.24 shows that “knows” has a wide meaning in this context. Even if it had no actual knowledge, a firm could still be liable to the true owner if it **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 firm and which are the subject of a report to MOKAS, might seek a court order which would direct the firm to disclose information. If the firm 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 obtained before the information is disclosed.

CHAPTER 3

INTERNAL CONTROLS, POLICIES AND PROCEDURES

Responsibilities and accountabilities

3.01 Firms are required to establish and maintain policies, procedures and controls to prevent money laundering or terrorist financing, and to ensure the reporting of any that may be known or suspected.

3.02 Section 69 of the Law requires firms 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. Firms must appoint an "appropriate senior executive with skills, knowledge and expertise in financial or other activities" (referred to in this Directive as the Compliance Officer) to undertake this role.

Recommended procedures for compliance with the Law

3.03 All firms to which the Law applies should have appropriate procedures for:

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

3.04 As good practice, it is recommended for firms to make arrangements to verify, on a regular basis, compliance with policies, procedures and controls relating to the prevention of money laundering or terrorist financing activities. Partners need to satisfy themselves that the requirement of the Law to maintain relevant systems and procedures has been complied with.

3.05 It is important that the procedures and responsibilities for monitoring compliance with and effectiveness of policies and procedures for the prevention of money laundering or terrorist financing are clearly laid down by all firms.

Overseas offices and associated firms

3.06 Where a firm has offices overseas or has associated firms in Cyprus or abroad over which 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, and where these differ from the provisions of the Cyprus Law then the overseas offices and associated firms shall apply the strictest provisions. In case where the implementation of the measures required by the Law is not allowed in the host country, the firm must inform the Institute immediately and must take additional measures in order to mitigate the risk of money laundering and terrorist financing. The firm must notify the policy and procedures implemented for the prevention of money laundering and terrorist financing activities, to its overseas offices and associated firms.

3.07 Irrespective of the above, a senior member of management from a Cyprus incorporated entity of the group (the one with the highest total assets) must be appointed as a coordinator for ensuring the implementation by the firm and its offices and associated firms in Cyprus and overseas, of adequate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing offences.

CHAPTER 4

RISK-BASED APPROACH

The purpose of the risk-based approach

4.01 The Law requires all persons carrying on financial or other business to apply client identification and due diligence procedures, but allows them to determine the extent of such measures on a risk basis. Firms are likely to already have in place policies and procedures to minimise professional, client and legal risks. Procedures against money laundering and terrorist financing may be integrated into existing risk management systems or be controlled separately.

4.02 By adopting a risk-based approach, firms shall apply measures and procedures to prevent or mitigate money laundering and terrorist financing which are commensurate with the risks identified. A risk-based approach allows firms to exercise reasonable business and professional judgement with respect to clients as regards managing potential money laundering and terrorist financing risks. It allows firms to target resources and effort where the risk is greatest and, conversely, reduce requirements where the risk is low. It also allows firms to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

4.03 A risk-based approach:

- recognises that the money laundering or terrorist financing threat varies across clients, countries, services and financial instruments;
- allows firms to differentiate between clients in a way that matches the risk of their particular business;
- allows firms to apply their own approach in the formulation of policies, procedures and controls in response to the firm's particular circumstances and characteristics;
- helps to produce a more cost effective system; and
- promotes the prioritisation of effort and actions of the firm in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the firm.

4.04 In assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by the firm, a risk-based approach involves the following steps:

- identifying and assessing the money laundering and terrorist financing risks emanating from particular clients, services and geographical areas of operation of the firm and its clients;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls;
- documenting, in appropriate manuals and policies, the procedures and controls to ensure their uniform application across the firm.

Risk categories

4.05 In theory, money laundering and terrorist financing risks can be organised into three categories: geographic risk, client risk and service risk. However, in practice these risks may fall into more than one category and should be viewed as inter-related. There is no one single methodology to apply to these risk categories, and their application is merely intended to provide a suggested framework for approaching the management of potential risks.

4.06 Examples of factors that may indicate a higher than normal money laundering or terrorist financing risk are provided in Appendix C. The examples provided are given for assistance in identifying those that may apply in the circumstances of individual firms and client relationships. However, it should be borne in mind that the lists of examples provided is not exhaustive.

Country/Geographic risk

4.07 There is no universally agreed definition that prescribes whether a particular country or geographic area represents a higher risk. It should be borne in mind that lower risk and legitimate commercial enterprises may be located in high risk countries. Nevertheless, clients may be judged to pose a higher than normal risk where they, or their source or destination of funds, are located in a country that poses a higher risk (see Appendix C).

Client risk

4.09 Key factors associated with the main client risk category are:

(a) Factors indicating that the client is attempting to obscure understanding of its business, ownership or the nature of its transactions;
(b) Factors indicating certain transactions, structures, geographical location, international activities or other factors which are not in keeping with the firm's understanding of the client's business or economic situation; or
(c) Client industries, sectors or categories where opportunities for money laundering or terrorist financing are particularly prevalent.

4.10 Clients falling within this category (see Appendix C) may be high risk clients although, after adequate review, the firm may determine that they are pursuing a legitimate purpose. Provided that the economic rationale for the structure and transactions of a client can be made clear, the firm may be able to demonstrate that the client is carrying out legitimate operations for which there is a rational and non-criminal purpose.

Service risk

4.11 An overall risk assessment should also include determining the potential risk presented by the services offered by a firm. There are some categories of service provided by firms which may be used by money launderers for their own purposes, and which are therefore subject to a higher degree of risk (see Appendix C).

4.12 Services which may be provided by firms and which (in some circumstances) risk being used to assist money launderers may result in:

- Misuse of pooled client accounts or safe custody of client money or assets.
- Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures).
- Misuse of introductory services, e.g. to financial institution.

Developing and applying a risk-based approach

4.13 Firms must establish adequate and appropriate policies and procedures for risk assessment and management in order to prevent operations related to money laundering or terrorist financing.

4.14 To develop a risk-based approach it is necessary to review the firm and consider what money laundering and terrorist financing risks might attach to each service type, client type etc. Outlined below is a way to consider this in relation to the services provided by auditors, external accountants, tax advisors or trust and company service providers. It should be noted however that there are other approaches that may be equally or more valid depending on the type of firm concerned.

4.15 Firms should first consider the type of risk presented:

- the firm might be used to launder money or provide the means to launder money.
- the client or its counterparties might be involved in money laundering.

4.16 Consideration of these risk types should enable the firm to draw up a simple matrix of characteristics of the client or service which are considered to present a higher than normal risk, and those which present a normal risk. Some clients may be considered to present a lower than normal risk, through long association and detailed knowledge, or on account of their status (e.g. listed, regulated, or government entities).

4.17 This matrix can then be incorporated into client acceptance procedures, and as the first step of the client due diligence process (see Chapter 5), it allows a money laundering or terrorist financing risk level to be assigned to ensure appropriate, but not excessive, client due diligence work is carried out. Enhanced due diligence should be carried out for those clients that are determined to be higher risk.

4.18 It is important for the approach adopted to incorporate a provision for raising the risk rating from low or normal to high if any information comes to light in conducting the client due diligence that causes concern or suspicion.

4.19 In all cases, firms should gather information about the client ("know your client" information – see Chapter 5), to assist in effective on-going monitoring and allow understanding of:

- who the client is
- where applicable, who owns the client (including ultimate beneficial owners)
- who controls the client
- the purpose and intended nature of the business relationship
- the nature of the client
- the client's source of funds
- the client's business and economic purpose.

4.20 Firms need to set out clear requirements for collecting "know your client" information about the client and for conducting verification of identity, to a depth suitable to the assessment of risk. For those clients that are determined to be higher risk increased levels of "know your client" are required.

4.21 Additional measures and controls for higher risk clients and transactions may include:

- Increased awareness across all departments with a business relationship with the client, including enhanced briefing of client teams.
- Escalation of the approval process for the establishment of a business engagement, or involvement in the client service.

Limitations to the risk-based approach

4.22 There are circumstances in which the application of a risk-based approach will not apply, or may be limited. There are also circumstances in which the application of a risk-based approach may not apply to the initial stages of a requirement or process, but will apply to subsequent stages. The limitations to the risk-based approach are usually the result of legal or regulatory requirements that mandate certain actions to be taken.

4.23 While the identification of potential suspicious transactions can be advanced by a risk-based approach, the reporting of suspicious transactions, once identified, is not risk-based.

4.24 The identification and verification of identity of clients are requirements which must be completed regardless of the risk-based approach. However, in relation to all other client due diligence components, a reasonably implemented risk-based approach may allow for a determination of the extent and quantity of information required, and the mechanisms to be used to meet these minimum standards. Once this determination is made, the obligation to keep records and documents that have been obtained for due diligence purposes, as well as transaction records, is not dependent on risk levels.

4.25 Some form of monitoring is required in order to detect unusual and hence possibly suspicious transactions. Even in the case of lower risk clients, monitoring is needed to verify that transactions match the initial low risk profile and if not, trigger a process for appropriately revising the client's risk rating. Equally, risks for some clients may only become evident once a relationship with a client has begun. This makes appropriate and reasonable monitoring of client transactions an essential component of a properly designed risk-based approach. However within this context it should be understood that not all transactions or clients will be monitored in exactly the same way. Moreover, where there is an actual suspicion of money laundering or terrorist financing, this could be regarded as a higher risk scenario, and enhanced due diligence should be applied regardless of any threshold or exemption.

CHAPTER 5

IDENTIFICATION PROCEDURES

Statutory requirements

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

Introduction – Client due diligence/ Know your client

5.02 In business relationships, the auditor, external accountant, tax advisor or trust and company service provider 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.

5.03 Client due diligence/ Know your client is intended to enable a firm to form a reasonable belief that they know the true identity of each client and, with an appropriate degree of confidence, know the types of business and transactions the client is likely to undertake. It should include procedures to:

(a) Identify and verify the identity of each client on a timely basis.

(b) Identify, where applicable, the beneficial owner, and take reasonable measures to verify the identity of any beneficial owner. The measures which have to be taken to verify the identity of the beneficial owner will vary depending on the risk.

(c) Obtain appropriate additional information to understand the client's circumstances and business, including the expected nature and level of transactions. Relevant client due diligence information should be periodically updated together with its risk assessment. In the event of any change in beneficial ownership or control of the client, or third parties on whose behalf the client acts, reasonable measures should be taken to verify identity.

5.04 Firms should thus identify and verify the identity of their clients in sufficient detail to provide them with reasonable assurance that the information they have is an appropriate and sufficient indication of the true identity.

5.05 Where applicable, the beneficial owners of the client should be identified, including forming an understanding of the ownership and control structure, and taking reasonable measures to verify the identity of such persons. The procedures that need to be carried out can vary, in accordance with the nature and purpose for which the entity exists, and the extent to which the underlying ownership differs from apparent ownership by the use of nominees and complex structures.

5.06 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 firm itself, or merely to ensure that he/she cannot be traced or linked to the proceeds of the crime that the firm 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.

5.07 A firm which is taking over a professional appointment replacing an existing auditor, external accountant, tax advisor, trust and company service provider or other advisor, can come into contact with their predecessor. This can provide evidence for the identity as well as the integrity of the client, and is therefore a valuable procedure in this context.

5.08 Where these procedures do not provide evidence of sufficient quality to satisfy the engagement partner that the identity of the prospective client has been adequately verified, further enquiries may be appropriate. If the engagement partner has doubts as to client identity, he/she may well decline to act.

5.09 It is for each firm to decide what document(s) a prospective client should be required to produce as evidence of identity. A copy of such document(s) should be made and retained. Where this is not possible, the relevant details should be recorded on the prospective client's file. An on-going client due diligence on the client business should be done, including scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the firm'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

5.10 All firms 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 within a reasonable time, then a firm should refrain from providing the requested service or from performing a transaction, without this being considered as a breach of any contractual or other obligation of the firm to its client. In some circumstances, the 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 firm should then seriously consider reporting the case to MOKAS.

5.11 The verification requirements are the same, whatever the means by which the firm intends to provide its 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.

5.12 If a firm suspects that a prospective client is engaged in money laundering or terrorist financing, it 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.

5.13 Section 62(6) of the Law requires identification procedures and client due diligence requirements to be applied not only to all new clients but also to existing clients at appropriate times, depending on the level of risk of involvement in money laundering or financing of terrorism activities.

5.14 If the firm finds out, at any stage of the business relationship with an existing client, that valid or sufficient documentation or information is not available regarding his/her identity and economic profile, the firm must apply all necessary procedures and carry out a due diligence in order to collect the missing documentation and information as quickly as possible, with a view to forming the complete 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 a complete economic profile within a reasonable time, the firm should terminate the business relationship and at the same time it must consider whether under the circumstances it must file a suspicious activity report to MOKAS.

When must identity be verified?

5.15 Information and instructions given by a prospective client may present unusual and unexplained features which could suggest underlying money laundering or terrorist financing activity. Unless the firm withdraws at once in such a case, identity should be verified before it agrees to act, irrespective of the size and nature of the transaction and service to be provided and even if an exemption appears to apply (see paragraphs 5.23 to 5.26).

5.16 According to Section 60 of the Law, persons carrying out financial or other activities must apply verification of identity and client due diligence measures in the following cases:

(a) When they establish a business relationship;
(b) When they carry out occasional transactions amounting to €15.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked (save for company or trust formation or the provision of related services, in which case the verification of identity and client due diligence measures should always be applied regardless of the transaction amount);
(c) When there is suspicion of money laundering or terrorist financing regardless of the amount of the transaction; or
(d) When there are doubts about the veracity or adequacy of the documents, data or information collected in the past for the verification of identity and due diligence of an existing client.

5.17 According to Section 61(1) of the Law, client 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, where applicable, 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 involve understanding 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 monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the data and information held by the firm in connection with the client.

5.18 According to Section 64(1a) of the Law, firms 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) take supplementary measures to verify or certify the documents supplied, or require confirmatory certification by a credit or financial institution covered by the EU Directive;
(b) ensure that the first payment of the operations is carried out through an account opened in the client's name with a credit institution operating in a country within the European Economic Area.

5.19 Once identification procedures have been satisfactorily completed, then as long as records are maintained (see Chapter 6), and some contact is maintained with the client, no further evidence is needed when subsequent transactions are undertaken.

5.20 Firms 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". The Charter was signed on 27 July 1999 by, among others, the European Federation of Accountants (FEE) on behalf of its members one of which is the Institute.

5.21 By way of derogation from the contents of the preceding paragraph, a firm 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 for not interrupting 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.

Applicant for business relationship

5.22 An applicant for business relationship is a person seeking to form a business relationship or carry out a one-off transaction with a person who is carrying out the prescribed activities and services (as defined in Section 2 of the Law) in or from within Cyprus. Thus, for example:

- Clients seeking advice in their own name and on their own behalf are clearly the applicants for business.
- When a person applies for an investment to be registered in the name of another, the latter must be identified through independent source documents, data or other reliable information; in special cases, however, where the investment will be registered in the name of a minor (e.g. a grandchild), it is the person who provides the funds who should be regarded as the applicant for business rather than the registered holder.
- When an intermediary introduces a third party to the firm so that the third party may be given advice, and/or make an investment in his/her own name, then it is that party (not the introducer) who is the firm's applicant for business and therefore whose identity must be verified.
- If an individual claiming to represent a company, partnership, or other legal entity applies for business, then the applicant for business will be the legal entity as such.
- If an applicant for business is or appears to be acting as anything other than as principal, the identity of any person on whose behalf the applicant is acting should be verified.

Identification procedures: Exemptions

5.23 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, firms 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.

5.24 Steps to verify identity are not required in the case of Cyprus credit or financial institutions.

5.25 Verification of identity is not required when there are reasonable grounds for believing that the applicant for business is itself subject to the Law (see paragraph 5.48 below).

5.26 With the exception of company and trust formation or the provision of related services, 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 5.16). However, identification procedures should be undertaken for linked transactions that together exceed this limit.

Reliance on third parties for client identification and due diligence purposes

5.27 The firm may rely on third parties, subject to the third parties' consent, for carrying out all or part of the client identification and due diligence procedures, as these are prescribed in Section 61(1)(a),(b) and (c) of the Law, but should be cautious of such reliance as the firm will remain liable for any compliance failure notwithstanding its reliance on third parties.

5.28 Reliance for this purpose may only be placed on a credit institution, a financial institution, an auditor, an external accountant, a tax advisor, a trust and company service provider or an independent legal professional from a country which is a member of the European Economic Area or a third country that the Advisory Authority has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the EU Directive. The firm must verify that the third party is subject to professional registration in accordance with the competent law of its country of incorporation and/or operation, as well as supervision for the purposes of compliance with prescribed measures for the prevention of money laundering and terrorist financing.

5.29 The firm should obtain immediately from the third party all relevant information and documentation in order that they may satisfy themselves that the information is sufficient. A third party consenting to be relied upon must, if requested, make available to the person relying on it as soon as is reasonably practicable:

- Any information obtained from the client (and any beneficial owner) when applying client due diligence measures; and/or
- Copies of any identification and verification data and other documents on the identity of the client (and any beneficial owner) obtained when applying client due diligence measures.

5.30 Before accepting the client identification data verified by the said third party, the firm should apply the following additional measures/procedures:

(a) assess and evaluate the systems and procedures applied by the third party for the prevention of money laundering and terrorist financing.

(b) satisfy itself based on the assessment of point (a) that the third party implements client identification and due diligence systems and procedures which are in line with the requirements of the Law and this Directive.
(c) maintain a separate file for every such third party, where it stores the assessment report pertaining to point (a) and other relevant information (for example identification details, records of meetings, evidence of the data and information of paragraph 5.28).
(d) take steps to ensure that the third party to be relied upon will provide the required information.
(e) the commencement of the cooperation with the third party and the acceptance of client identification data verified by the third party is subject to approval by the Compliance Officer.

5.31 The firm may rely on third parties only at the outset of establishing a business relationship or the execution of an occasional transaction for the purpose of verifying the identity of their clients. According to the degree of risk, any additional data and information for the purpose of updating the client's economic profile or for the purpose of examining unusual transactions executed through the firm, should be obtained from the natural persons (directors, beneficial owners) who control and manage the activities of the client and have the ultimate responsibility of decision making as regards the management of funds and assets.

5.32 For those occasions where the client is introduced by one of the firm's overseas branch offices or associated firms, the firm could obtain the introducer's written confirmation that it has verified the client's identity and that relevant identification data is retained by the overseas office branch or firm, provided that the group applies common client due diligence and record-keeping procedures and measures against money laundering and terrorist financing, and the effective application of such measures and procedures is supervised at group level by a competent authority.

5.33 Where a firm merges with another firm, or acquires the practice of another firm in whole or in part, it may not be necessary for the identity of clients to be re-verified, provided that satisfactory identification records are available.

Clients from countries whose legislation is ineffective

5.34 Although many countries have enacted, or are enacting, effective legislation against money laundering and terrorist financing, there are some countries where the legislation is considered to be ineffective or deficient. FATF issues the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, known as the "FATF Recommendations". The FATF Recommendations assist in the increase of transparency and enable countries to successfully take action against illicit use of their financial system. Cyprus has officially adopted the FATF Recommendations.

5.35 From time to time FATF issues 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. Firms and in particular their Compliance Officers must regularly consult the country evaluation reports of FATF (www.fatf-gafi.org) as well as those of the MONEYVAL Committee of the Council of Europe (www.coe.int/moneyval).

5.36 When setting up their internal procedures, firms should have regard to the need for additional and continuous monitoring procedures for transactions from countries which appear to have ineffective and deficient anti-money laundering and anti-terrorist financing systems. When considering what additional procedures are required, firms may take into account the FATF and MONEYVAL country evaluation reports with regard to the assessment of any progress made. In respect of transactions with these countries, which do not have an apparent or visible lawful purpose, the background and purpose of such transactions should be examined as extensively as possible, and findings should be documented in writing, and should be available to assist competent authorities.

Identification of individuals

Evidence of identity

5.37 When verifying the identity of an individual, the vital question is "Is the person who he/she claims to be?" and not "What is his/her position and standing?". The identity of an individual comprises his/her name and all other names used, the signature, 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 firm should be recorded.

5.38 In addition to the name(s) used and date of birth, it is important that the current permanent address should be verified as it is an integral part of 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 (to guard against forged or counterfeit documents, care should be taken to check that the documents offered are originals), and
- checking the telephone directory.

5.39 In case where a client or an authorised person provides misleading data and false information in relation to the client's identity or the identity of the ultimate beneficial owner or provides fake identification documents, then in case of conviction, he/she is punished with a maximum of 2 years imprisonment or with a fine not exceeding €100.000 or with both of these penalties.

Transactions that favour anonymity

5.40 In the case of clients' transactions via the internet, phone, fax or other electronic means where the client is not physically present so as to verify the authenticity of his signature or that he is the real owner of the account or that he has been properly authorised to operate the account, the firm applies reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory to the account.

Individuals not resident in Cyprus

5.41 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, firms should confirm the identity and permanent address with a reputable financial institution or professional adviser in the prospective client's home country or normal country of residence.

5.42 Firms should have policies in place or take such measures as may be needed to prevent the misuse of technological developments or new financial products in money laundering or terrorist financing schemes.

5.43 Firms should apply enhanced due diligence procedures in the case of prospective clients who are individuals not resident in Cyprus, who are not seen face to face and who are not covered by one of the exemptions set out in paragraphs 5.25 and 5.26. Possible procedures include:

- A branch office, associated firm or reliable professional adviser in the prospective client's home country could be used to confirm identity or as an agent to check personal verification details.
- Where the firm has no such relationship in the prospective client's country of residence, a copy of the passport authenticated by an attorney or consulate could be obtained.
- 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.

Identification of companies and other organisations

5.44 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 duly authorised to do so and identify and verify the identity of that person.

Companies and partnerships

5.45 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.

5.46 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.

5.47 "Know your client" is an on-going process. If a firm 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.

5.48 According to Section 63(1) of the Law simplified client identification procedures and client due diligence measures may be applied in the following prospective client cases, provided that the money laundering and terrorist financing risk is low and there is no suspicion of money laundering and terrorist financing activities:

- Credit institution or financial organisation which falls within the ambit of the EU Directive.
- 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 it imposes requirements equivalent to those of the EU Directive, and
  (b) it is under supervision for compliance with the said requirements.
- 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 EU legislation.
- The public authorities of the countries of the European Economic Area.

5.49 In the above cases firms should gather sufficient information to establish if the customer qualifies for an exemption as mentioned above. 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.

5.50 According to Section 63(1) of the Law, for the clients mentioned in paragraph 5.48 above, firms may choose not verify the identity of the client or, where applicable, the beneficial owner, nor obtain information on the purpose and intended nature of the business relationship or to carry out client due diligence after the establishment of the business relationship or an isolated transaction.

5.51 The same Section 63(1) of the Law provides that firms are obliged to carry out continuous monitoring of business relationships for the clienst mentioned in paragraph 5.48 above, in accordance with the provisions of Section 61(1)(d), and to report to MOKAS suspicious transaction or the attempt to carry out suspicious transactions.

5.52 Where the applicant for business is an unquoted company, an unincorporated business or a partnership, the firm 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.

5.53 The firm may also make a credit reference agency search or take a reference from a bank or from another professional adviser. Enhanced due diligence should be performed for higher risk categories of clients, business relationships or transactions. Such categories may include non-resident clients and companies that have nominee shareholders or bearer shares.

Trusts (including occupational pension schemes) and nominees

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

5.55 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.

5.56 Where a firm 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 authorized in writing by the trustee.

5.57 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 firm is to give them advice individually.

Clubs, societies and charitable institutions

5.58 Where the applicant is a club, a society or a charitable institution, the firm 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 firm 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

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

Politically Exposed Persons (PEPs)

5.60 In addition to performing the standard client due diligence measures, the firm should put in place appropriate risk based procedures to determine whether a potential client, a client or the beneficial owner is a PEP. Examples of measures that could form part of such risk based procedures include seeking relevant information from the client, referring to publicly available information or having access to commercial electronic databases of PEPs.

5.61 The firm should have senior management approval for establishing a business relationship with a PEP or for the continuation of business relationships with an existing client which has become PEPs.

5.62 The firm should take adequate measures to establish the source of wealth and source of funds of clients and beneficial owners identified as PEPs. It should also conduct enhanced on-going monitoring of the business relationship.

5.63 More attention should be paid when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose laws and regulations for the prevention of money laundering and terrorist financing are not equivalent with international standards.

5.64 In order to effectively manage such risks, the firm should assess the countries of origin of their clients in order to identify the ones that are more vulnerable to corruption or have laws and regulations that do not meet the FATF Recommendations (see paragraphs 5.34 to 5.36).

5.65 With regard to the issue of corruption, a useful source of information is the Transparency International Corruption Perceptions Index which ranks countries and territories based on how corrupt their public sector is perceived to be (www.transparency.org). This index draws on corruption-related data collected by a variety of reputable institutions, and reflects the views of observers from around the world, including experts living and working in the countries and territories evaluated. With regard to the issue of effectiveness of application of the FATF Recommendations, information can be obtained from the MONEYVAL country evaluation reports (see paragraphs 5.34 to 5.36), or relevant reports issued by the International Monetary Fund.

5.66 Enhanced client due diligence measures must also be taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing.

Non-execution or delay in executing a transaction

5.67 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.

CHAPTER 6

RECORD-KEEPING

Statutory requirements

6.01 Sections 58 and 68 of the Law require firms 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 part of the audit evidence procedures that the Law seeks to establish.

6.02 The records prepared and maintained by any firm about 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 firm's compliance with policies and procedures against money laundering and terrorist financing.

6.03 Firms should be aware that they might be called upon to satisfy within a reasonable time frame any enquiries from MOKAS or ICPAC (as the Supervisory Authority) requiring disclosure of information in relation to business relationships during the last five years. For this reason the firms must implement systems and procedures that facilitate the timely response to such possible enquiries.

6.04 The Law requires relevant records to be retained for at least five years from the date when the firm'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 firms through undertaking reviews of existing records, particularly for higher risk clients or business relationships.

6.05 Section 68 of the Law specifies that the records to be 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 a person's identity to be re-obtained.
(b) A record containing evidential material and details relating to all transactions carried out for the account and on behalf of that person, including documents for recording such transactions in the accounting books.
(c) A record containing relevant documents of correspondence with the clients or other persons with whom a business relation is established.

6.06 The prescribed record retention period of at least five years commences with the date on which the relevant business or activities taking place in the course of which transactions were completed, or the end of the business relationship.

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 a 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 the completion of all activities taking place in the course of the last transaction.

Transaction records

6.09 Firms 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 or ICPAC (as the Supervisory Authority). 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 (like passports, identity cards, or driving licences),
- the name and address (or identification code) of its counterparty,
- 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 the 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 Compliance Officer and other relevant 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, firms are therefore advised to consider both the statutory requirements and the potential needs of MOKAS.

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

CHAPTER 7

RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

Recognition of suspicious transactions

7.01 As the types of transactions which may be used by those involved in 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 key to recognition is knowing enough about the client's business so as to recognise that a transaction or series of transactions is unusual.

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

- Is the size of the transaction consistent with the normal activities of the client?
- Is the transaction rational 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 rational 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 firm's client base and range of services and products. A firm 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 internal instructions and guidelines from time to time.

7.05 A list containing examples of what might constitute suspicious transactions/activities related to money laundering or terrorist financing, which can be used as guidance for assisting the firm and its employees in recognising suspicious transactions, can be found in Appendix D.

Reporting of suspicious transactions

7.06 Section 27 of the Law requires that any knowledge or suspicion of money laundering or terrorist financing should be promptly reported to MOKAS. The Law also provides, under Section 26, that such disclosure cannot be treated as a breach of the duty for confidentiality owed by firms to their clients by virtue of the contractual relationship existing between them, and the firms will not accept any responsibility towards the clients involved.

7.07 Section 69 of the Law requires that firms establish internal reporting procedures and identify a senior executive with skills, knowledge and expertise in financial or other activities, as appropriate (hereafter to be referred to as "Compliance Officer") 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, Section 26 of the Law recognises that internal reporting to the Compliance Officer will satisfy the reporting requirement imposed by virtue of Section 27 of the Law, i.e. once the employee reports his/her suspicion to the Compliance Officer then he/she is considered to have fully satisfied his/her statutory obligations under Section 27 of the Law.

7.08 Firms should include in their engagement letters with their clients or their business letters a paragraph which notifies clients of the firm's potential reporting obligations. While this could refer specifically to suspicions of money laundering or terrorist financing, firms may prefer a general form of wording which would extend to other matters where reporting to regulators for instance is required or appropriate. It would also be a useful precaution to include a statement that Cyprus law will govern the provision of the firm's services and that the Cypriot courts will have exclusive jurisdiction over any dispute.

Appointment and role of the Compliance Officer

7.09 In accordance with the provisions of Section 69 of the Law, all firms should proceed with the appointment of a Compliance Officer. The person appointed as Compliance Officer should be sufficiently senior to command the necessary authority.

7.10 Firms should communicate to MOKAS the names and positions of persons whom they appoint to act as Compliance Officers.

7.11 The role and responsibilities of Compliance Officers including those of Chief and Assistants should be clearly specified by the firm and documented in appropriate manuals and/or job descriptions. The Compliance Officer should be allowed direct and timely access to all documents, data and information possessed by the firm and which may assist him/her in carrying out his/her duties.

7.12 As a minimum, the duties of a Compliance Officer should include the following:

(a) To receive from the firm's 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.

(b) To validate and consider the information received as per paragraph (a) 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 Compliance Officer should be recorded and retained on file.

(c) If following the evaluation described in paragraph (b) above, the Compliance Officer decides to notify MOKAS, he/she should complete a written report and submit it to MOKAS the soonest possible. A specimen of such a report can be found in Appendix B. All such reports should be kept on file. The Law stipulates specifically that the obligation for reporting to MOKAS extends to any attempt by somebody to carry out suspicious transactions.

(d) If following the evaluation described in paragraph (b) above, the Compliance Officer decides not to notify MOKAS then he/she should fully document the reasons for such a decision.

(e) The Compliance Officer acts as a first point of contact with MOKAS, upon commencement of and during investigation as a result of filing a report to MOKAS under (c) above.

(f) The Compliance Officer responds to requests from MOKAS and determines whether such requests are directly connected with the case reported and, if so, provides all the supplementary information requested and fully co-operates with MOKAS.

(g) The Compliance Officer provides advice and guidance to other employees of the firm on money laundering matters.

(h) The Compliance Officer acquires the knowledge and skills required which should be used to improve the firm's internal procedures for recognising and reporting money-laundering and terrorist financing suspicions.

(i) The Compliance Officer determines whether the firm's employees need further training and/or knowledge for the purpose of learning to combat money laundering or terrorist financing.

(j) The Compliance Officer is primarily responsible, in consultation with the firm's senior management and Internal Audit Department (if any), towards the Institute in implementing the various Directives issued by it under the Law as well as all other instructions/recommendations issued by the Institute, from time to time, on the prevention of the criminal use of services offered by auditors, external accountants, tax advisors or trust and company service providers for the purpose of money laundering or terrorist financing.

7.13 The Compliance Officer is expected to avoid errors and/or omissions in the course of discharging his/her duties and, most importantly, when validating the reports received on money laundering or terrorist financing suspicions, as a result of which a report to MOKAS may or may not be filed.

7.14 He/she is also expected to act honestly and reasonably and to make his/her determination in good faith. In this connection, it should be emphasised that the Compliance Officer's decision may be subject to the subsequent review of the Institute which, in the course of examining and evaluating the procedures of a firm against money laundering or terrorist financing, and their compliance with the provisions of the Law, is legally empowered to report to MOKAS a firm which, in its opinion, does not comply with the provisions of the Law and forms the opinion that actual money laundering or terrorist financing has been carried out.

Internal reporting procedures and records

7.15 A firm should make the necessary arrangements in order to introduce measures designed to assist the functions of the Compliance Officer and the reporting of suspicious transactions by employees. Firms have an obligation to ensure:

- that they maintain an adequately resourced and independent audit function to test compliance (including sample testing) with procedures, policies and control;
- 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 Compliance Officer.

7.16 Reporting lines should be as short as possible, with the minimum number of people between the person with the suspicion and the Compliance Officer. This ensures speed, confidentiality and accessibility to the Compliance Officer. However, some firms 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 Compliance Officer.

7.17 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 Compliance Officer. On the other hand, the partner should never attempt to prevent a member of staff who remains suspicious from reporting direct to the Compliance Officer. Staff should be made aware that they have a direct route to the Compliance Officer.

7.18 Larger firms may choose to appoint assistant Compliance Officers within departments or branch offices, to enable the validity of the suspicion to be examined before being passed to a central Compliance Officer. In such cases, the role of the assistant Compliance Officers must be clearly specified and documented. All procedures should be documented in appropriate manuals and job descriptions.

7.19 All suspicions reported to the Compliance Officer 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 Compliance Officer and for the report to be prepared jointly. In other firms the initial report should be prepared and sent to the Compliance Officer. The report should include full details of the client and as full statements as possible of the information giving rise to the suspicion.

7.20 The Compliance Officer 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.

7.21 On-going communication between the Compliance Officer and the reporting person, department or branch office is important. The firm may wish to consider advising the reporting person, department or branch office of the Compliance Officer's decision, particularly if the reported suspicions are believed to be without ground. 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 Compliance Officer is informed of all communications between the investigating officer and the firm at all stages of the investigation.

7.22 Records of suspicions which were raised internally with the Compliance Officer 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

7.23 All Compliance Officers' reports to MOKAS should be sent to or delivered at the following address:

Unit for Combating Money Laundering (MOKAS)
Law Office of the Republic
P.O. Box 23768
CY-1686 Nicosia
Cyprus

Tel.: +357 22 446 018, Fax: +357 22 317 063

e-mail: mokas@mokas.law.gov.cy

Contact person:
Mrs Eva Rossidou – Papakyriakou
Senior Council of the Republic, Head of MOKAS

Method of reporting

7.24 The Institute recommends the use of the specimen form attached as Appendix B to this Directive, for the reporting of disclosures. Disclosures can be forwarded by post or by fax. In urgent cases an initial telephone report can be made which will subsequently be confirmed in writing.

7.25 After filing the report, firms 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

7.26 Sufficient information should be disclosed which indicates 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 firm 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 an appropriate court order if necessary.

Constructive trust

7.27 The duty to report suspicious transactions and to avoid "tipping off" can lead to a conflict between the reporting firm's responsibilities under the criminal law, and its obligations under the civil law as a constructive trustee, to a victim of fraud and other crimes.

7.28 A firm's liability as a constructive trustee arises when it comes to know that assets rightfully belong to a person other than its 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.

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

7.30 The tipping off offence prohibits a firm from informing a suspected victim of crime that his assets are at risk, where to do so is likely to prejudice a money laundering or terrorist financing investigation. Given the absolute nature of the prohibition in the criminal law, if a firm makes a disclosure under the money laundering or terrorist financing legislation, and is acting in accordance with the instructions of MOKAS or the investigating officer 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 slight. However, to minimise the liability, the following procedures should be followed:

- When evaluating a suspicious transaction, the Compliance Officer should consider whether there is a constructive trust issue involved. If the Compliance Officer concludes that there is reason to believe that the firm may incur a liability as a constructive trustee, the precise reasons for this belief should be reported to MOKAS immediately by fax, electronic link or modem, 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.

- Unless entirely confident that liability as constructive trustee cannot arise, a firm should take legal advice. In certain cases firms may be advised to apply to the court for directions before reporting their money laundering or terrorist financing suspicions or disposing of any assets. However, it is essential to note that in all cases where:

  (a) a person knows or suspects that another person is engaged in money laundering or terrorist financing; and
  (b) 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. In such cases it will never be appropriate to delay making a disclosure to MOKAS pending an application to the court for directions, and an accountant must report the matter to MOKAS as soon as is reasonably practicable. An accountant in such a position should inform MOKAS of the sensitive nature of his obligations as constructive trustee and he should take legal advice as soon as possible.

Investigation of disclosures

7.31 Following the receipt of a disclosure and the initial research by MOKAS, the information disclosed is allocated to trained financial investigation officers in the office of the Attorney General 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

7.32 In the event of a prosecution, the source of the information provided to MOKAS is protected as far as the rules for the disclosure of evidence allow. Maintaining the integrity of the confidential relationship between law enforcement agencies and firms 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 firm and to maintain the confidence in the disclosure system.

Feedback from the investigating authorities

7.33 MOKAS informs the persons carrying out financial or other activities about the outcome of the investigation of cases they have referred to them in compliance with Sections 27 and 69 of the Law.

CHAPTER 8

EDUCATION AND TRAINING

Statutory requirements

8.01 Section 58 of the Law requires all firms to take appropriate measures to:

- Make employees aware of the policies and procedures they have in place to prevent money laundering or terrorist financing including those of identification, record keeping and internal reporting;
- Make employees aware of the requirements imposed by the Law and all relevant national or EU Directives; and
- Provide employees with on-going training in the recognition and handling of suspicious transactions and activities.

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 a firm's staff 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 and that 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 prompt reports of any knowledge or suspicion of transactions or activities involving money laundering or terrorist financing. It is therefore important that firms introduce comprehensive measures to ensure that their staff is fully aware of their responsibilities.

8.03 All relevant staff should be educated on the importance of the "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, so as 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 For direction in the discharge of their legal obligations, firms should refer to Chapter 7 of this Directive which deals with the recognition and reporting of suspicious transactions.

8.05 In addition to the above, firms are required to put in place screening procedures to ensure high standards when hiring employees and they 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.

8.07 It is also necessary to make arrangements for refresher training at regular intervals so that the firm will ensure that staff do not forget their responsibilities and are kept informed of any new developments in the prevention of money laundering and terrorist financing, including the practical methods used and trends for this purpose.

New professional staff

8.08 A general appreciation of the background on money laundering or terrorist financing, and of the procedures for identifying and reporting any suspicious transactions to the Compliance Officer, should be provided to all new professional staff that will be dealing with clients or their affairs, irrespective of the level of seniority. New staff should be made aware of the importance placed by the firm on the reporting of suspicions and that reporting is an obligation for 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 firm'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 on 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 Compliance Officer, whether or not the funds are accepted or the transaction proceeds. 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 under the Law 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 records.

Compliance Officers

8.12 For larger firms, or those with complex procedures, in-depth training concerning all aspects of the legislation, this Directive and internal policies will be required for the Compliance Officer. In addition, the Compliance Officer 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 Compliance Officer or sole practitioner should have at least the level of knowledge outlined above for partners and managers. When money laundering or terrorist financing becomes an issue, further advice or assistance can be obtained from the Institute.

Refresher training

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

Methods of providing training

8.14 There is no standard preferred way to conduct training for the purposes of prevention of money laundering or terrorist financing. The training should be tailored to meet the needs of a particular firm, depending on its size and nature.

8.15 The Law does not require firms to purchase specific training materials for the purpose of educating relevant staff on the prevention of money laundering or terrorist financing and the recognition and reporting of suspicious transactions.

8.16 Firms 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 1.02)

Articles 1 to 4 of the Council Framework Decision 2002/475/HA

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 organization where committed with the aim of:

   - seriously intimidating a population, or
   - unduly compelling a Government or international organization 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 organization, 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.

APPENDIX B
(Paragraphs 7.12 and 7.24)

Compliance Officer's report to the Unit for Combating Money Laundering (MOKAS)

I. GENERAL INFORMATION

Name of reporting firm _____

Address, telephone and fax numbers _____
_____
_____
_____

Date when business relationship started or one-off transaction was carried out _____

Type of services offered to client _____
_____
_____

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

(A) NATURAL PERSONS

Name _____

Residential address _____
_____
_____

Business address _____
_____
_____

Occupation _____
_____

Date and place of birth _____

Nationality and passport number _____
_____

(B) LEGAL ENTITIES

Company's name, country and date of incorporation _____

Business address _____

Main activities _____

Details of directors and shareholders

	Name	Nationality and passport number	Date of birth	Residential address (if known)	Occupation and employer
Registered shareholder(s)	1.				
	2.				
	3.				
Beneficial shareholder(s) (if different from above)	1.				
	2.				
	3.				
Directors	1.				
	2.				
	3.				

III. FULL DESCRIPTION AND DETAILS OF TRANSACTIONS / ACTIVITY AROUSING SUSPICION

IV. REASONS FOR SUSPICION

V. OTHER INFORMATION

Client's accounts with domestic, international or foreign banks (if known)

Other information the firm wishes to bring to the attention of MOKAS (if any)

COMPLIANCE OFFICER'S signature:

Date:

NB: The above report should be accompanied by photocopies of the following:

1. For natural persons, the relevant pages of clients' passports evidencing identity.
2. For legal entities, certificates of incorporation, directors and shareholders.
3. All documents relating to the suspicious transaction(s)/activity(ies)

APPENDIX C
(Paragraph 4.06)

Examples of factors that may indicate a higher than normal money laundering or terrorist financing risk

The examples below are given for assistance in identifying those that may apply in the circumstances of individual firms and client relationships. It is emphasised however that the lists below are not exhaustive.

(a) Country/Geographic risk (Paragraph 4.07)

Clients may be judged to pose a higher than normal risk where they, or their source or destination of funds, are located in a country that is:

- Subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN). In some circumstances, this would include countries subject to sanctions or measures similar to those issued by bodies such as the UN.
- Identified by credible sources as lacking appropriate laws, regulations and other measures for the prevention and suppression of money laundering and terrorist financing.
- Identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Identified by credible sources as having significant levels of corruption, or other criminal activity.

"Credible sources" refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force (FATF), such sources may include, but are not limited to international bodies such as the International Monetary Fund, and the Egmont Group of Financial Intelligence Units. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

(b) Client risk (Paragraphs 4.09 and 4.10)

<u>Reduced transparency</u>

- Lack of face-to-face introduction of client.
- Subsequent lack of contact, when this would normally be expected.
- Beneficial ownership is unclear.
- Position of intermediaries is unclear.
- Inexplicable changes in ownership.
- Company activities are unclear.
- Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).

- Management appear to be acting according to instructions of unknown or inappropriate person(s).
- Unnecessarily complex client structure.
- Reason for client choosing the firm is unclear, given the firm's size, location or specialisation.
- Frequent or unexplained change of professional adviser(s) or members of management.
- The client is reluctant to provide all the relevant information or the firm has reasonable doubt that the provided information is correct or sufficient.

Transactions or structures out of line with business profile

- Client instructions or funds outside of their personal or business sector profile.
- Individual or classes of transactions that take place outside the established business profile, and expected activities/transaction unclear.
- Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
- Sudden activity from a previously dormant client.
- Client starts or develops an enterprise with unexpected profile or early results.
- Indicators that client does not wish to obtain necessary governmental approvals/filings, etc.
- Clients offer to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.

Higher risk sectors and operational structures

- Entities with a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
- Politically exposed persons.
- Investment in real estate at a higher/lower price than expected.
- Large international payments with no business rationale.
- Unusual financial transactions with unknown source.
- Clients with multijurisdictional operations that do not have adequate centralised corporate oversight.
- Clients incorporated in countries that permit bearer shares.

Categories of clients whose activities may indicate a higher risk

- Clients conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the firm and the location of the client.

- Clients where the structure or nature of the entity or relationship makes it difficult to identify and verify the true owner or controlling interests, such as:
  - Unexplained use of corporate structures, express trusts and nominee shares, and use of bearer shares.
  - Unexplained delegation of authority by the applicant or client through the use of powers of attorney, mixed boards and representative offices.
  - Unexplained relationship between an applicant's beneficial owners and controllers and account signatories.
  - In the case of express trusts, an unexplained relationship between a settlor and beneficiaries with a vested right, other beneficiaries and persons who are the object of a power.
  - In the case of an express trust, an unexplained nature of classes of beneficiaries and classes within an expression of wishes.
- Cash (and cash equivalent) intensive businesses including:
  - Money services businesses (e.g. remittance houses, currency exchange houses, casas de cambio, bureau de change, money transfer agents and bank note traders or other businesses offering money transfer facilities).
  - Casinos, betting and other gambling related activities.
  - Businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions.
- Charities and other "not for profit" organisations which are not subject to monitoring or supervision (especially those operating on a "cross-border" basis).
- Other firms, financial institutions, and other designated non-professional businesses and professions who are not subject to adequate laws and regulations against money laundering and combating of financing terrorism, and who are not adequately supervised.
- Clients that are politically exposed persons.
- Clients where there is no commercial rationale for them buying the products or services that they seek, who request undue levels of secrecy, or where it appears that an "audit trail" has been deliberately broken or unnecessarily layered.

<u>Fraudulent or improperly accounted for transactions</u>

- Over and under invoicing of goods/services.
- Multiple invoicing of the same goods/services.
- Falsely described goods/services or over and under shipments (e.g. false entries on bills of lading).
- Multiple trading of goods/services.

(c) Service risk (Paragraphs 4.11 and 4.12)

<u>Products and services offered by trust and companies service providers</u>

- Shell companies, companies with ownership through nominee shareholding and control through nominee and corporate directors.

- Services where firms, acting as financial intermediaries, actually handle the receipt and transmission of cash proceeds through accounts they actually control in the act of closing a business transaction.
- Other services to conceal improperly beneficial ownership from competent authorities.
- Situations where it is difficult to identify the beneficiaries of trusts. This might include situations where identification is hindered because the beneficiary of a trust is another trust or corporate vehicle, or where the trust deed does not include the names of the settlor, the beneficiaries or the class of beneficiaries.
- Commercial, private, or real property transactions or services with no apparent legitimate business, economic, tax, family governance, or legal reasons.
- Payments received from unassociated or unknown third parties where this would not be a typical method of payment.
- The offer by clients to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Services that inherently have provided more anonymity.
- Trusts which are pensions that may be considered lower risk.

(d) Variables that may impact risk

Some factors that may increase or decrease risk in relation to particular clients, client engagements or practising environments include the following:

- Involvement of financial institutions or other designated non-financial businesses and professions.
- Unexplained urgency of assistance required.
- Sophistication of client, including complexity of control environment.
- Sophistication of transaction/scheme.
- Working environment/structure of firm, e.g. sole practitioner, large firm.
- Role or oversight of another regulator.
- The regularity or duration of the relationship. Long-standing relationships involving frequent client contact throughout the relationship may present less risk.
- The purpose of the relationship and the need for the firm to provide services.
- Clients who have a reputation for probity in the local communities.
- Private companies that are transparent and well known in the public domain.

Additional variables that may increase or decrease the risk posed by a particular client or transaction, applicable for trust and companies service providers, may include:

- The purpose and intended nature of a relationship.
- The type, volume and value of activity expected.

- 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 which 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 firm to treat the client as lower risk.
- The level of regulation or other oversight of a government's regime to which a client is subject. A client that is a financial institution regulated in a country with a satisfactory anti-money laundering regime poses less risk from a money laundering perspective than a client that is unregulated or subject only to minimal anti-money laundering regulation. Additionally, companies and their wholly owned subsidiaries that are publically owned and traded on a recognised exchange generally pose minimal money laundering risks. These companies are usually from countries with an adequate, recognised regulatory scheme, and, therefore, generally pose less risk due to the type of business that they conduct and the wider government's regime to which they are subject.
- The regularity or duration of the relationship. Long standing relationships involving frequent client contact throughout the relationship may present less risk from the money laundering perspective.
- The familiarity with the country, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as a result of a firm's own operations within the country.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or that will increase the complexity or otherwise result in a lack of transparency. The use of such vehicles or structures, without an acceptable explanation, increases the risk.

APPENDIX D
(Paragraph 7.05)

Examples of suspicious transactions/ activities related to money laundering and terrorist financing

(a) Money laundering

1. Transfer of funds between bank accounts established in various countries, through Cyprus, without justified reason.
2. Transfer of funds between companies belonging to the same group, without justified reason.
3. Deposits performed without submission of supporting documentation in an accepted form (e.g. invoice, agreements etc.).
4. Supporting documentation that is submitted in relation to a specific transaction (e.g. an invoice or agreement) is not in the same form that is normally used by the client. For example draft invoices, different from those produced from the system used by the client are submitted.
5. Transactions with no apparent purpose or which are unnecessarily complex.
6. Use of foreign bank accounts or companies or groups of companies with a complicated ownership structure which is not justified based on the needs and economic profile of the client.
7. The transactions or the size of the transactions requested by the client do not comply with the client's usual practice or business activity.
8. Large volume of transactions and/or money deposited or credited into an account, when the nature of the client's business activities would not appear to justify such activity.
9. Frequent settlement of client's obligations in cash.
10. Use of bank accounts other than the client's usual bank accounts, to transfer amounts initially deposited in cash.
11. Any transaction of which the nature, size or frequency appears to be unusual.
12. Instructions of payment to a third person that does not seem to be related with the instructor.
13. Transfer of funds to and from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations (see paragraphs 5.34 to 5.36).
14. A client is reluctant to provide complete information when establishing a business relationship about the nature and purpose of the client's business activities, anticipated account activity, names of officers and directors, or business location.
15. A client is providing minimum or misleading information that is difficult or expensive for the firm to verify.
16. A client provides unusual or suspicious identification documents that cannot be readily verified.
17. A client's home/business telephone is disconnected and the client cannot be reached by the firm and its employees.

18. A client who has been introduced by a foreign financial organisation, or by a third party from countries or geographical areas which do not apply or inadequately apply the FATF Recommendations (see paragraphs 5.34 to 5.36).
19. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
20. Unexplained inconsistencies arising during the process of identifying and verifying the client.
21. Complex trust or nominee network and/or legal structure.

(b) Terrorist financing

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and drug trafficking. Legal fund raising methods used by terrorist groups include:

(a) collection of membership dues and/or subscriptions,
(b) sale of books and other publications,
(c) cultural and social events,
(d) donations,
(e) community solicitations and fund raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non–profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

(a) Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
(b) A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
(c) The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.

(d) The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

(a) Inconsistencies between the apparent sources and amount of funds raised or moved.
(b) A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
(c) A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
(d) Large and unexplained cash transactions by non-profit organisations.
(e) The absence of contributions from donors located within the country of origin of the non-profit organisation.